Regeringens proposition 2025/26:303

En ny lag för ökad motståndskraft hos kritiska verksamhetsutövare

Prop. 2025/26:303

Regeringen överlämnar denna proposition till riksdagen.

Stockholm den 9 juli 2026

Pål Jonson

Carl-Oskar Bohlin
(Försvarsdepartementet)

Propositionens huvudsakliga innehåll

Europaparlamentet och rådet antog 2022 ett direktiv om åtgärder för ökad motståndskraft hos kritiska entiteter som tillhandahåller samhällsviktiga tjänster inom EU, det så kallade CER-direktivet. I syfte att genomföra direktivet i svensk rätt föreslår regeringen att det ska införas en ny lag om motståndskraft hos kritiska verksamhetsutövare.

Den nya lagen innebär att offentliga och enskilda verksamhetsutövare som tillhandahåller samhällsviktiga tjänster inom vissa utpekade sektorer och som identifieras som kritiska verksamhetsutövare ska vidta åtgärder för ökad motståndskraft samt rapportera vissa incidenter. Den nya lagen innehåller också bestämmelser om tillsyn och ingripandemöjligheter när det gäller verksamhetsutövare som inte följer lagens bestämmelser.

Därutöver föreslås ändringar i säkerhetsskyddslagen som innebär att högre sanktionsavgifter kan beslutas med stöd av den lagen när det gäller enskilda verksamhetsutövare.

Den nya lagen och övriga lagändringar föreslås träda i kraft den 1 januari 2027.

Innehållsförteckning

1 Förslag till riksdagsbeslut 5

2 Lagtext 6
2.1 Förslag till lag om motståndskraft hos kritiska verksamhetsutövare 6
2.2 Förslag till lag om ändring i lagen (1998:620) om belastningsregister 13
2.3 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400) 15
2.4 Förslag till lag om ändring i säkerhetsskyddslagen (2018:585) 17
2.5 Förslag till lag om ändring i cybersäkerhetslagen (2025:1506) 18

3 Ärendet och dess beredning 20

4 CER-direktivets bakgrund och kopplingen till NIS 2-direktivet 21
4.1 Arbetet med skydd av kritisk infrastruktur har pågått under lång tid 21
4.2 CER-direktivets innehåll i stort 21
4.3 NIS 2-direktivets innehåll i stort 24

5 En ny lag om motståndskraft hos kritiska verksamhetsutövare 26
5.1 CER-direktivet bör genomföras genom en ny lag och vissa uttryck i lagen bör definieras 26
5.2 Uppdelning i enskilda och offentliga verksamhetsutövare 30
5.3 Vilka bör räknas som offentliga och enskilda verksamhetsutövare? 32
5.4 Undantag från tillämpningsområdet 38
5.4.1 Undantag kopplat till bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur 38
5.4.2 Undantag på grund av krav i andra författningar 42
5.4.3 Undantag för viss säkerhetskänslig verksamhet och brottsbekämpande verksamhet 47
5.4.4 Undantag för säkerhetsskyddsklassificerade uppgifter 54

6 Identifiering av kritiska verksamhetsutövare utifrån bland annat en nationell riskbedömning 57
6.1 Den myndighet som regeringen pekar ut bör genomföra riskbedömningen 57
6.2 Uttrycket samhällsviktig tjänst bör definieras i lagen och styra vilka som kan identifieras 59
6.3 Krav för att identifieras som kritisk verksamhetsutövare 64

6.4 Beslutet om identifiering och reglering om när skyldigheter enligt lagen bör gälla ... 72
6.5 En kritisk verksamhetsutövare bör räknas som en väsentlig verksamhetsutövare enligt cybersäkerhetslagen ... 76

7 Kritiska verksamhetsutövare av särskild europeisk betydelse ... 81
7.1 Anmälningsskyldighet ... 81
7.2 Medverkan till genomförande av rådgivande uppdrag ... 84

8 Riskbedömning, åtgärder för motståndskraft och incidentrapportering ... 88
8.1 Kritiska verksamhetsutövares riskbedömning ... 88
8.2 Åtgärder för motståndskraft ... 95
8.3 Incidentrapportering ... 107

9 Bakgrundskontroll och befattningsanalys ... 114
9.1 Skyldigheten att genomföra bakgrundskontroll ... 114
9.2 Befattningsanalysen bör utgöra grunden för vilka som ska genomgå bakgrundskontroll ... 128
9.3 Registerkontroll och förnyad bakgrundskontroll ... 132
9.4 Krav på dokumentation och bevarande ... 139
9.5 Bakgrundskontroller inför deltagande i viss samverkan enligt direktivet ... 140
9.6 Utbyte av uppgifter ur belastningsregistret mellan medlemsstater ... 143

10 Tillsyn ... 146
10.1 Tillsynsmyndigheterna ska pekas ut i förordning ... 146
10.2 Tillsynsmyndighetens befogenheter ... 149

11 Ingripanden ... 154
11.1 En reglering liknande den som gäller NIS 2-direktivet bör införas ... 154
11.2 Vilka överträdelser bör kunna leda till ingripanden? ... 154
11.3 Vilka möjligheter till ingripande bör finnas? ... 156
11.4 Förelägganden vid behov ... 160
11.5 Sanktionsavgifter ... 161
11.5.1 När bör en sanktionsavgift få tas ut? ... 161
11.5.2 Sanktionsavgiftens storlek ... 164
11.5.3 Omständigheter att särskilt beakta vid bestämmande av sanktionsavgiftens storlek ... 166
11.5.4 Förfarandet vid beslut om sanktionsavgift ... 169

12 Överklagande ... 171

13 Sekretess och personuppgiftsbehandling ... 172
13.1 Ändrad reglering i offentlighets- och sekretesslagen ... 172
13.2 Ingen ytterligare reglering om personuppgiftsbehandling behövs ... 186

14 Ändringar i säkerhetsskyddslagen ... 188

15 Ikraftträdande- och övergångsbestämmelser ... 191

16 Konsekvenser av förslagen 192
16.1 Konsekvenser för motståndskraften hos kritiska verksamhetsutövare och samhällsekonomin 192
16.2 Ekonomiska konsekvenser för den offentliga sektorn 195
16.3 Konsekvenser för enskilda 198
16.4 Konsekvenser för den kommunala självstyrelsen 202
16.5 Övriga konsekvenser 204
17 Författningskommentar 204
17.1 Förslaget till lag om motståndskraft hos kritiska verksamhetsutövare 204
17.2 Förslaget till lag om ändring i lagen (1998:620) om belastningsregister 227
17.3 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400) 228
17.4 Förslaget till lag om ändring i säkerhetsskyddslagen (2018:585) 229
17.5 Förslaget till lag om ändring i cybersäkerhetslagen (2025:1506) 230
Bilaga 1 Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG 232
Bilaga 2 Sammanfattning av betänkandet Motståndskraft i samhällsviktiga tjänster (SOU 2024:64) 267
Bilaga 3 Betänkandets lagförslag 275
Bilaga 4 Förteckning över remissinstanserna 294
Bilaga 5 Lagrådsremissens lagförslag 296
Bilaga 6 Lagrådets yttrande 310
Utdrag ur protokoll vid regeringssammanträde den 9 juli 2026 326

1 Förslag till riksdagsbeslut

Regeringens förslag:

1. Riksdagen antar regeringens förslag till lag om motståndskraft hos kritiska verksamhetsutövare.
2. Riksdagen antar regeringens förslag till lag om ändring i lagen (1998:620) om belastningsregister.
3. Riksdagen antar regeringens förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400).
4. Riksdagen antar regeringens förslag till lag om ändring i säkerhetsskyddslagen (2018:585).
5. Riksdagen antar regeringens förslag till lag om ändring i cybersäkerhetslagen (2025:1506).

2 Lagtext

Regeringen har följande förslag till lagtext.

2.1 Förslag till lag om motståndskraft hos kritiska verksamhetsutövare

Härigenom föreskrivs[1] följande.

1 kap. Inledande bestämmelser

Lagens tillämpningsområde och syfte

1 § Denna lag gäller för verksamhetsutövare som har identifierats som kritiska med stöd av lagen (kritiska verksamhetsutövare). Syftet med lagen är att stärka kritiska verksamhetsutövares motståndskraft och förmåga att tillhandahålla samhällsviktiga tjänster.

Bestämmelserna i lagen genomför delvis Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG, i den ursprungliga lydelsen (här benämnt CER-direktivet).

Uttryck i lagen

2 § I denna lag betyder

1. *enskild verksamhetsutövare*: en kritisk verksamhetsutövare som inte är en offentlig verksamhetsutövare,
2. *incident*: en händelse som kan medföra en betydande störning eller som medför en störning i den kritiska verksamhetsutövarens tillhandahållande av en samhällsviktig tjänst,
3. *kritisk infrastruktur*: en tillgång, en anläggning, utrustning, ett nätverk eller ett system, eller en del av en tillgång, en anläggning, utrustning, ett nätverk eller ett system, som krävs för tillhandahållandet av en samhällsviktig tjänst,
4. *motståndskraft*: förmågan att förebygga, skydda mot, reagera på, stå emot, begränsa konsekvenserna av, absorbera, anpassa sig till och återhämta sig från en incident,
5. *offentlig verksamhetsutövare*: en kritisk verksamhetsutövare som är
   a) en statlig myndighet, eller
   b) en region, en kommun eller ett kommunalförbund,
6. *samhällsviktig tjänst*: en tjänst som är avgörande för upprätthållandet av centrala samhällsfunktioner, ekonomisk verksamhet, folkhälsa, allmän säkerhet eller för skyddet av miljön och som omfattas av bilagan till CER-direktivet.

[1] Jfr Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG, i den ursprungliga lydelsen.

Undantag från lagens tillämpningsområde

3 § Om det i lag eller annan författning finns bestämmelser som innehåller krav på åtgärder för motståndskraft ska de bestämmelserna gälla om verkan av kraven minst motsvarar verkan av skyldigheterna enligt denna lag med beaktande av bestämmelsernas omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till kraven i bestämmelserna.

4 § För en verksamhetsutövare som har identifierats som kritisk inom någon eller några av sektorerna bankverksamhet, finansmarknadsinfrastruktur eller digital infrastruktur i bilagan till CER-direktivet gäller inte skyldigheterna enligt denna lag för den delen av verksamheten.

5 § Denna lag gäller inte för en statlig myndighet som till övervägande del bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen (2018:585) eller som till övervägande del bedriver brottsbekämpande verksamhet.

För en enskild verksamhetsutövare som bedriver enbart säkerhetskänslig verksamhet enligt säkerhetsskyddslagen eller som erbjuder tjänster enbart till sådana statliga myndigheter som avses i första stycket gäller inte skyldigheterna enligt denna lag.

För andra kritiska verksamhetsutövare som till någon del bedriver sådan verksamhet eller erbjuder sådana tjänster som avses i första eller andra stycket gäller inte skyldigheterna enligt denna lag för den delen av verksamheten.

6 § Skyldigheterna att lämna uppgifter enligt denna lag gäller inte uppgifter som är säkerhetsskyddsklassificerade enligt 1 kap. 2 § säkerhetsskyddslagen (2018:585).

7 § Denna lag gäller inte för regeringen, Regeringskansliet, utlandsmyndigheter, kommittéväsendet, myndigheter under riksdagen, domstolar och inte heller för nämnder som utövar rättskipning.

Lagen gäller inte heller för förbundsfullmäktige eller förbundsdirektion i ett kommunalförbund eller för kommunfullmäktige eller regionfullmäktige.

Uppdrag enligt CER-direktivet

8 § Den myndighet som regeringen bestämmer ska göra en nationell riskbedömning och vara gemensam kontaktpunkt enligt artiklarna 5 och 9 i CER-direktivet.

Bemyndigande

9 § Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om vad som utgör en incident enligt 2 § 2.

2 kap. Identifiering av kritiska verksamhetsutövare

1 § Den eller de myndigheter som regeringen bestämmer ska i enskilda fall besluta om identifiering av kritiska verksamhetsutövare.

2 § För att identifieras som kritisk verksamhetsutövare enligt 1 § krävs att

1. verksamhetsutövaren tillhandahåller en eller flera samhällsviktiga tjänster,

2. verksamhetsutövaren

a) omfattas av någon av kategorierna i bilagan till CER-direktivet, eller

b) är en statlig myndighet som regeringen i övrigt bestämmer ska kunna omfattas av lagen,

3. verksamhetsutövaren bedriver verksamhet i och har kritisk infrastruktur belägen i Sverige, och

4. en incident skulle få en betydande störande effekt för

a) verksamhetsutövarens tillhandahållande av en eller flera samhällsviktiga tjänster, eller

b) tillhandahållandet av andra samhällsviktiga tjänster som är beroende av den eller de samhällsviktiga tjänster som verksamhetsutövaren tillhandahåller.

3 § En myndighet som avses i 1 § ska så snart det kan ske besluta att en verksamhetsutövare som inte längre uppfyller kraven enligt 2 § inte ska omfattas av lagen.

Ett beslut enligt första stycket gäller omedelbart.

4 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om vad som utgör en betydande störande effekt enligt 2 § 4.

3 kap. Skyldigheter för kritiska verksamhetsutövare

Anmälningsskyldighet

1 § En kritisk verksamhetsutövare som tillhandahåller en samhällsviktig tjänst till eller i minst sex medlemsstater inom Europeiska unionen ska så snart det kan ske anmäla detta till den eller de myndigheter som regeringen bestämmer.

Riskbedömning

2 § En kritisk verksamhetsutövare ska göra en riskbedömning.

Riskbedömningen ska dokumenteras och innehålla en redogörelse för alla relevanta risker för en incident.

Riskbedömningen ska uppdateras vid behov och minst vart fjärde år.

Åtgärder för motståndskraft

3 § En kritisk verksamhetsutövare ska vidta lämpliga och proportionella tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa sin motståndskraft (åtgärder för motståndskraft). Åtgärderna för motståndskraft ska vidtas på grundval av verksamhetsutövarens riskbedömning och annan relevant information samt inkludera åtgärder som är nödvändiga för att

1. förhindra att incidenter inträffar,

2. säkerställa ett tillfredsställande fysiskt skydd av lokaler och kritisk infrastruktur,
3. reagera på, stå emot och begränsa konsekvenserna av incidenter,
4. återhämta sig från incidenter,
5. säkerställa en ändamålsenlig hantering av personalsäkerhet, inbegripet åtgärder enligt 4–7 §§, och
6. öka kunskapen och medvetenheten om åtgärderna för motståndskraft hos berörd personal.

Verksamhetsutövaren ska upprätta och följa en plan för motståndskraft som beskriver de åtgärder som har vidtagits eller ska vidtas enligt första stycket.

4 § En kritisk verksamhetsutövare ska göra en analys av vilka befattningar som ska omfattas av krav på bakgrundskontroll enligt 5 § (befattningsanalys).

Befattningsanalysen ska dokumenteras och innehålla uppgifter om sådana befattningar där deltagandet i verksamheten innebär möjlighet att orsaka mer än ringa störning i den kritiska verksamhetsutövarens tillhandahållande av en eller flera samhällsviktiga tjänster.

Befattningsanalysen ska uppdateras vid behov och minst en gång om året.

5 § En kritisk verksamhetsutövare ska säkerställa att en person som deltar i eller ska delta i verksamheten, i den mån det följer av verksamhetsutövarens befattningsanalys, har genomgått en bakgrundskontroll.

En bakgrundskontroll innebär att den person som kontrollen avser ska
1. styrka sin identitet, och
2. genomgå en registerkontroll enligt 6 §.

En förnyad bakgrundskontroll ska göras när det finns skäl för det, och senast två år efter den senaste kontrollen.

6 § En person som avses i 5 § ska på begäran av den kritiska verksamhetsutövaren visa upp ett utdrag ur det register som förs enligt lagen (1998:620) om belastningsregister.

Utdraget får inte vara äldre än sex månader.

7 § Vid en bakgrundskontroll ska den kritiska verksamhetsutövaren anteckna om den person som kontrollen avser har styrkt sin identitet och visat upp ett sådant utdrag som avses i 6 §. Någon annan dokumentation av kontrollen får inte göras.

Anteckningar enligt första stycket ska bevaras i två år från den dag då bakgrundskontrollen avslutades.

8 § En kritisk verksamhetsutövare ska utse en kontaktpunkt för tillsynsmyndigheten.

Incidentrapportering

9 § En kritisk verksamhetsutövare ska till den myndighet som regeringen bestämmer anmäla sådana incidenter som medför eller kan

medföra en betydande störning i den kritiska verksamhetsutövarens tillhandahållande av en samhällsviktig tjänst.

En incidentanmälan enligt första stycket ska lämnas så snart det kan ske, dock senast 24 timmar efter det att verksamhetsutövaren har fått kännedom om incidenten. Senast en månad efter incidentanmälan ska verksamhetsutövaren lämna en rapport om incidenten till samma myndighet.

När skyldigheterna inträder

10 § En kritisk verksamhetsutövares skyldigheter enligt 2 § börjar gälla nio månader efter det att denne har fått del av ett sådant beslut som avses i 2 kap. 1 §. Skyldigheterna enligt 3–9 §§ börjar gälla tio månader efter det att verksamhetsutövaren har fått del av beslutet.

Bakgrundskontroller inför deltagande i samverkan enligt CER-direktivet

11 § Regeringen eller den myndighet som regeringen bestämmer får genomföra bakgrundskontroller enligt 5 § av personer som föreslås delta i ett rådgivande uppdrag eller företräda Sverige i gruppen för kritiska entiteters motståndskraft enligt artiklarna 18 och 19 i CER-direktivet.

Bemyndigande

12 § Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om riskbedömning enligt 2 §, åtgärder för motståndskraft enligt 3–8 §§ och incidentrapportering enligt 9 §.

4 kap. Tillsyn

Tillsynsmyndigheten och tillsynsmyndighetens uppdrag

1 § Den eller de myndigheter som regeringen bestämmer ska vara tillsynsmyndighet.

2 § En tillsynsmyndighet ska

1. utöva tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs,
2. utöva tillsyn över att sådana rättsakter följs som har antagits med stöd av artikel 13.6 i CER-direktivet, och
3. inom ramen för sin tillsyn medverka till att rådgivande uppdrag genomförs i enlighet med artikel 18 i CER-direktivet.

Tillsynsmyndighetens befogenheter

3 § Den som står under tillsyn ska på begäran tillhandahålla en tillsynsmyndighet de uppgifter eller handlingar som behövs för tillsynen.

4 § En tillsynsmyndighet har i den omfattning det behövs för tillsynen rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamhet som omfattas av tillsynen.

5 § En tillsynsmyndighet får besluta att förelägga den som står under tillsyn att tillhandahålla uppgifter eller handlingar eller ge tillträde enligt 3 och 4 §§.

Ett föreläggande får förenas med vite. Ett vitesföreläggande får även riktas mot staten.

6 § En tillsynsmyndighet får begära handräckning av Kronofogdemyndigheten för de tillsynsåtgärder som avses i 3 och 4 §§. Vid handräckning gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande.

5 kap. Ingripanden

När och hur tillsynsmyndigheten ska ingripa

1 § En tillsynsmyndighet ska ingripa om en kritisk verksamhetsutövare har åsidosatt sina skyldigheter enligt 3 kap. 1–9 §§ eller enligt föreskrifter som har meddelats i anslutning till de paragraferna eller enligt sådana rättsakter som har antagits med stöd av artikel 13.6 i CER-direktivet.

Ett ingripande sker genom ett beslut om föreläggande enligt 2 §, ett beslut om sanktionsavgift enligt 3 § eller, om det inte finns skäl att ingripa mot en överträdelse på något annat sätt, genom att besluta om anmärkning.

Tillsynsmyndigheten får avstå från ett ingripande om överträdelsen är ringa eller ursäktlig, eller om det annars med hänsyn till omständigheterna vore oskäligt att ingripa.

Förelägganden

2 § En tillsynsmyndighet får besluta de förelägganden som behövs för att en kritisk verksamhetsutövare ska uppfylla skyldigheterna som avses i 1 § första stycket.

Ett föreläggande får förenas med vite. Ett vitesföreläggande får även riktas mot staten.

Sanktionsavgift

3 § En tillsynsmyndighet får besluta att ta ut en sanktionsavgift av en kritisk verksamhetsutövare till följd av en överträdelse av de skyldigheter som avses i 1 § första stycket.

4 § Sanktionsavgiften ska bestämmas till lägst 5 000 kronor och till högst

1. det högsta av 2 procent av en enskild verksamhetsutövares totala globala årsomsättning under närmast föregående räkenskapsår, och ett belopp i kronor motsvarande 10 000 000 euro, eller
2. 10 000 000 kronor för en offentlig verksamhetsutövare.

5 § När sanktionsavgiftens storlek bestäms ska särskild hänsyn tas till

1. den skada eller risk för skada som har uppstått till följd av överträdelsen,

2. om den kritiska verksamhetsutövaren tidigare har gjort sig skyldig till en överträdelse, och

3. den ekonomiska fördel som överträdelsen har inneburit för verksamhetsutövaren.

6 § En sanktionsavgift får inte beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

7 § En sanktionsavgift får beslutas endast om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

8 § En sanktionsavgift ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas i rätt tid, ska tillsynsmyndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m.

Sanktionsavgiften tillfaller staten.

9 § En sanktionsavgift faller bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

6 kap. Överklagande

1 § Beslut enligt denna lag får överklagas till allmän förvaltningsdomstol. När ett sådant beslut överklagas är den beslutande myndigheten motpart i domstolen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Denna lag träder i kraft den 1 januari 2027.

2.2 Förslag till lag om ändring i lagen (1998:620) om belastningsregister

Härigenom föreskrivs[1] att 9 och 12 a §§ lagen (1998:620) om belastningsregister ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
9 §[2]	
En enskild har rätt att på begäran skriftligen få ta del av samtliga uppgifter ur registret om sig själv. Om sådana uppgifter finns har den enskilde även rätt att få sådan skriftlig information som anges i 4 kap. 3 § första stycket 1–8 brottsdatalagen (2018:1177). Uppgifterna ska på begäran lämnas ut utan avgift en gång per kalenderår.	
En enskild som behöver ett registerutdrag om sig själv har rätt att få ett begränsat utdrag ur registret	
1. för att kunna ta till vara sin rätt i ett främmande land eller få tillstånd att resa in, bosätta sig eller arbeta där,	
2. enligt bestämmelser i skollagen (2010:800),	
3. enligt bestämmelser i lagen (2018:1219) om försäkringsdistribution,	
4. enligt bestämmelser i lagen (2007:171) om registerkontroll av personal vid vissa boenden som tar emot barn,	
5. enligt bestämmelser i lagen (2010:479) om registerkontroll av personal som utför vissa insatser åt barn med funktionshinder,	
6. enligt bestämmelser i lagen (2013:852) om registerkontroll av personer som ska arbeta med barn,	
7. enligt bestämmelser i lagen (2026:43) om registerkontroll vid arbete i hemmet åt äldre personer eller vuxna personer med funktionsnedsättning, *eller*	7. enligt bestämmelser i lagen (2026:43) om registerkontroll vid arbete i hemmet åt äldre personer eller vuxna personer med funktionsnedsättning,
8. enligt bestämmelser i lagen (2026:44) om registerkontroll vid anställning till ledande befattningar i kommuner.	8. enligt bestämmelser i lagen (2026:44) om registerkontroll vid anställning till ledande befattningar i kommuner, *eller*
	9. enligt bestämmelser i lagen (2026:000) om motståndskraft hos kritiska verksamhetsutövare.
Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om vilka uppgifter ett sådant utdrag som avses i andra stycket 1–3 ska innehålla.	
Regeringen får meddela föreskrifter om vilka uppgifter ett sådant utdrag som avses i andra stycket 4–*8* ska innehålla.	Regeringen får meddela föreskrifter om vilka uppgifter ett sådant utdrag som avses i andra stycket 4–*9* ska innehålla.

[1] Jfr Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG, i den ursprungliga lydelsen.
[2] Senaste lydelse 2026:46.

En begäran om uppgifter ur registret ska vara skriftlig. Polismyndigheten ska säkerställa att begäran görs av en behörig person.

12 a §[3]

Uppgifter ur registret får efter en begäran som sker med stöd av rådets rambeslut 2009/315/RIF av den 26 februari 2009 om organisationen av medlemsstaternas utbyte av uppgifter ur kriminalregistret och uppgifternas innehåll lämnas ut till en myndighet i en annan medlemsstat i Europeiska unionen för något annat ändamål än att användas i ett brottmålsförfarande om motsvarande rätt att få del av uppgifterna finns för en svensk myndighet.

En uppgift som har förts in i registret med stöd av 4 a § får dock inte lämnas ut om Polismyndigheten har underrättats av en behörig myndighet i den stat som har överfört uppgiften om att uppgiften har gallrats i den staten.

Uppgifter ur registret får lämnas ut till en annan medlemsstat i Europeiska unionen om begäran görs med stöd av Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG, i den ursprungliga lydelsen. Detta gäller även om motsvarande rätt att få del av uppgifterna saknas för en svensk myndighet.

Denna lag träder i kraft den 1 januari 2027.

[3] Senaste lydelse 2022:735.

2.3 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs[1] i fråga om offentlighets- och sekretesslagen (2009:400)

dels att 18 kap. 8 b § ska ha följande lydelse,

dels att det ska införas en ny paragraf, 15 kap. 3 d §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	15 kap.
	3 d §
	Sekretessen enligt 1 a § hindrar inte att Myndigheten för civilt försvar i egenskap av en sådan gemensam kontaktpunkt som avses i 1 kap. 8 § lagen (2026:000) om motståndskraft hos kritiska verksamhetsutövare lämnar en uppgift till en tillsynsmyndighet enligt samma lag, om uppgiften behövs för att tillsynsmyndigheten ska kunna fullgöra sitt uppdrag.
	Sekretessen hindrar inte heller att en sådan tillsynsmyndighet som avses i första stycket lämnar en uppgift till Myndigheten för civilt försvar, om uppgiften behövs för att Myndigheten för civilt försvar ska kunna fullgöra sitt uppdrag som sådan gemensam kontaktpunkt som avses i första stycket.
	En uppgift enligt första eller andra stycket får lämnas endast om intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.
	18 kap.
	8 b §[2]
Sekretess gäller för uppgift i en incidentrapport enligt cybersäkerhetslagen (2025:1506) och för uppgift om vilka åtgärder som en verksamhetsutövare har vidtagit till	Sekretess gäller för uppgift i en incidentrapport enligt cybersäkerhetslagen (2025:1506) *och lagen (2026:000) om motståndskraft hos kritiska verksamhets-*

[1] Jfr Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG, i den ursprungliga lydelsen.

[2] Senaste lydelse 2025:1508.

följd av incidenten, om det inte står klart att uppgiften kan röjas utan att den rapporterande verksamhetsutövarens framtida verksamhet skadas eller syftet med vidtagen åtgärd motverkas.	*utövare samt* för uppgift om vilka åtgärder som en verksamhetsutövare har vidtagit till följd av incidenten, om det inte står klart att uppgiften kan röjas utan att den rapporterande verksamhetsutövarens framtida verksamhet skadas eller syftet med vidtagen åtgärd motverkas.

För uppgift i en allmän handling gäller sekretessen i högst fyrtio år.

Denna lag träder i kraft den 1 januari 2027.

2.4 Förslag till lag om ändring i säkerhetsskyddslagen (2018:585)

Härigenom föreskrivs att 7 kap. 4 § säkerhetsskyddslagen (2018:585) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
7 kap.	
4 §[1]	
En sanktionsavgift ska bestämmas till lägst 25 000 kronor och högst *50 000 000 kronor*. Sanktionsavgiften för en statlig myndighet, kommun eller region ska dock bestämmas till högst 10 000 000 kronor.	En sanktionsavgift ska bestämmas till lägst 25 000 kronor och högst *till det högsta av 2 procent av verksamhetsutövarens totala globala årsomsättning under närmast föregående räkenskapsår och 120 000 000 kronor*. Sanktionsavgiften för en statlig myndighet, kommun eller region ska dock bestämmas till högst 10 000 000 kronor.

1. Denna lag träder i kraft den 1 januari 2027.
2. Äldre bestämmelser gäller fortfarande för överträdelser som har ägt rum före ikraftträdandet.

[1] Senaste lydelse 2021:952.

2.5 Förslag till lag om ändring i cybersäkerhetslagen (2025:1506)

Härigenom föreskrivs[1] i fråga om cybersäkerhetslagen (2025:1506)

dels att 1 kap. 9 § ska ha följande lydelse,

dels att det ska införas en ny paragraf, 1 kap. 8 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 kap.
	8 a §
	Lagen gäller också för en verksamhetsutövare som har identifierats som en kritisk verksamhetsutövare enligt 2 kap. 1 § lagen (2026:000) om motståndskraft hos kritiska verksamhetsutövare.
	9 §
Som väsentlig verksamhetsutövare räknas	
1. en verksamhetsutövare som är en statlig myndighet,	
2. en verksamhetsutövare som är större än ett medelstort företag och som	
a) är en kommun eller en region,	
b) i övrigt omfattas av bilaga 1 till NIS 2-direktivet i den ursprungliga lydelsen men inte av 7 § 2 eller 3, eller	
c) är en enskild utbildningsanordnare med tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina,	
3. en verksamhetsutövare som avses i 6 § och som storleksmässigt motsvarar eller är större än ett medelstort företag,	
4. en verksamhetsutövare som avses i 7 § 2 eller 3,	
5. en verksamhetsutövare som är en kvalificerad tillhandahållare av betrodda tjänster*, och*	5. en verksamhetsutövare som är en kvalificerad tillhandahållare av betrodda tjänster*,*
6. en verksamhetsutövare som räknas som väsentlig enligt föreskrifter som har meddelats med stöd av 15 § andra stycket.	6. en verksamhetsutövare som räknas som väsentlig enligt föreskrifter som har meddelats med stöd av 15 § andra stycket*, och*
	7. en verksamhetsutövare som avses i 8 a §.
Verksamhetsutövare som inte är väsentliga är viktiga verksamhetsutövare.	

[1] Jfr Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148, i den ursprungliga lydelsen.

3 Ärendet och dess beredning

Europaparlamentet och rådet antog den 14 december 2022 direktivet (EU) 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (CER-direktivet), se *bilaga 1*. Samma dag antogs direktivet (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet). Medlemsländerna skulle senast den 17 oktober 2024 ha antagit de nationella bestämmelser som krävs för att genomföra direktiven.

Regeringen beslutade den 23 februari 2023 att ge en särskild utredare i uppdrag att föreslå hur direktiven ska genomföras i svensk rätt (dir. 2023:30). Utredningen antog namnet Utredningen om genomförande av NIS2- och CER-direktiven (Fö 2023:01). I mars 2024 överlämnade utredningen sitt delbetänkande Nya regler om cybersäkerhet (SOU 2024:18) som behandlar genomförandet av NIS 2-direktivet. En ny lag som är en del av genomförandet av NIS 2-direktivet, cybersäkerhetslagen (2025:1506), trädde i kraft den 15 januari 2026 (se vidare prop. 2025/26:28).

Utredningen överlämnade i september 2024 sitt slutbetänkande Motståndskraft i samhällsviktiga tjänster (SOU 2024:64) som behandlar genomförandet av CER-direktivet samt vissa frågor som avser samordningen mellan kraven i direktiven. I slutbetänkandet föreslås bland annat ändringar i offentlighets- och sekretesslagen (2009:400) kopplat till genomförandet av NIS 2-direktivet som delvis behandlas i ovan nämnda proposition.

En sammanfattning av slutbetänkandet finns i *bilaga 2* och slutbetänkandets lagförslag finns i *bilaga 3*. Slutbetänkandet har remissbehandlats. En förteckning över remissinstanserna finns i *bilaga 4*. Remissvaren finns tillgängliga på regeringens webbplats (regeringen.se) och i lagstiftningsärendet (Fö2024/01550).

Lagrådet

Regeringen beslutade den 21 maj 2026 att inhämta Lagrådets yttrande över de lagförslag som finns i *bilaga 5*. Lagrådets yttrande finns i *bilaga 6*. Regeringen följer delvis Lagrådets synpunkter och förslag, som behandlas i avsnitt 5.1, 5.4.1–5.4.3, 6.1, 6.3, 6.4, 7.1, 7.2, 8.1–9.1, 11.3–11.5.3 och 13.1 samt i författningskommentaren (avsnitt 17). I förhållande till lagrådsremissen görs dessutom vissa språkliga och redaktionella ändringar.

4 CER-direktivets bakgrund och kopplingen till NIS 2-direktivet

4.1 Arbetet med skydd av kritisk infrastruktur har pågått under lång tid

Arbetet gällande skydd av kritisk infrastruktur har pågått under lång tid. Före 2022 har arbetet på EU-nivå framför allt bedrivits inom ramen för det europeiska programmet för skydd av kritisk infrastruktur (EPCIP). Målet med arbetet inom EPCIP är att förbättra skyddet av kritisk infrastruktur inom EU. En av de viktigaste delarna i programmet var rådets direktiv 2008/114/EG av den 8 december 2008 om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna (härefter rådets direktiv). Genom artikel 27 i Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (CER-direktivet) upphävdes rådets direktiv. Rådets direktiv upphörde att gälla den 18 oktober 2024.

Rådets direktiv omfattade energi- och transportsektorerna och gick huvudsakligen ut på att EU:s medlemsstater skulle identifiera och utse europeisk kritisk infrastruktur. Med uttrycket kritisk infrastruktur avsågs, enligt artikel 2 a i direktivet, anläggningar, system eller delar av dessa belägna i medlemsstaterna som är nödvändiga för att upprätthålla centrala samhällsfunktioner, hälsa, säkerhet, trygghet och människors ekonomiska eller sociala välfärd och där driftsstörning eller förstörelse av dessa skulle få betydande konsekvenser i en medlemsstat till följd av att man inte lyckas upprätthålla dessa funktioner. Med uttrycket europeisk kritisk infrastruktur avsågs, enligt artikel 2 b i samma direktiv, i medlemsstaterna belägen kritisk infrastruktur vars driftsstörning eller förstörelse skulle få betydande konsekvenser för minst två medlemsstater. Konsekvensernas omfattning bedömdes utifrån sektorsövergripande kriterier. Detta inbegrep verkningar till följd av tvärsektoriella beroenden av andra typer av infrastruktur.

Myndigheten för civilt försvar (MCF), tidigare Myndigheten för samhällsskydd och beredskap, är utpekad nationell kontaktpunkt för arbetet med EPCIP-frågorna i Sverige. Trafikverket, Affärsverket svenska kraftnät och Statens energimyndighet ska identifiera och redovisa eventuell kritisk infrastruktur till MCF. MCF ska i egenskap av kontaktpunkt samordna frågor kring skydd av kritisk infrastruktur i Sverige med andra medlemsstater och med EU-kommissionen.

4.2 CER-direktivets innehåll i stort

I skäl 1 till CER-direktivet konstateras att som tillhandahållare av samhällsviktiga tjänster spelar kritiska entiteter en oumbärlig roll när det gäller att upprätthålla viktiga samhällsfunktioner eller central ekonomisk verksamhet på den inre marknaden, i en unionsekonomi som i allt högre grad kännetecknas av ömsesidigt beroende. Det är därför enligt direktivet

mycket viktigt att det inrättas en unionsram som syftar dels till att stärka kritiska entiteters motståndskraft på den inre marknaden genom att fastställa harmoniserade minimiregler, dels till att bistå entiteterna genom enhetligt och särskilt stöd och tillsynsåtgärder. I direktivet anges också att en utvärdering av rådets direktiv visat att skyddsåtgärder som enbart gäller enskilda tillgångar inte är tillräckliga för att förhindra alla störningar från att uppstå (skäl 2). Med uttrycket kritisk entitet avses i CER-direktivet en offentlig eller privat entitet som har identifierats av en medlemsstat i enlighet med artikel 6 som tillhörande en av de kategorier som anges i den tredje kolumnen i tabellen i bilagan till direktivet (artikel 2.1).

Direktivet hindrar, enligt artikel 3, inte medlemsstaterna från att anta eller behålla bestämmelser i nationell rätt som syftar till att uppnå en högre grad av motståndskraft för kritiska entiteter, förutsatt att sådana bestämmelser står i överensstämmelse med medlemsstaternas förpliktelser enligt unionsrätten. Det rör sig därmed om ett så kallat minimidirektiv.

I CER-direktivet fastställs skyldigheter för medlemsstaterna att vidta särskilda åtgärder som syftar till att säkerställa att tjänster som är nödvändiga för att upprätthålla viktiga samhällsfunktioner eller central ekonomisk verksamhet inom tillämpningsområdet för artikel 114 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) tillhandahålls på ett obehindrat sätt på den inre marknaden (artikel 1.1 a). Direktivet innebär bland annat att medlemsstaterna senast den 17 juli 2026 ska identifiera de kritiska entiteterna för de sektorer och undersektorer som anges i direktivets bilaga (artikel 6.1). I tredje kolumnen i bilagan anges också kategorier av entiteter. Bilagan innehåller följande 11 sektorer:

- energi, med undersektorerna elektricitet, fjärrvärme eller fjärrkyla, olja, gas och vätgas
- transport, med undersektorerna luftfart, järnväg, vatten, väg och kollektivtrafik
- bankverksamhet
- finansmarknadsinfrastruktur
- hälso- och sjukvård
- dricksvatten
- avloppsvatten
- digital infrastruktur
- offentlig förvaltning
- rymden
- produktion, bearbetning och distribution av livsmedel.

EU-kommissionen ges i artikel 5.1 i direktivet befogenhet att anta en delegerad akt för att komplettera direktivet med en icke uttömmande förteckning över samhällsviktiga tjänster inom de sektorer och undersektorer som omfattas av direktivet. Kommissionen antog en sådan förordning den 25 juli 2023. Det rör sig om Kommissionens delegerade förordning (EU) 2023/2450 av den 25 juli 2023 om komplettering av Europaparlamentets och rådets direktiv (EU) 2022/2557 genom upprättande av en förteckning över samhällsviktiga tjänster (kompletteringsförordningen). De behöriga myndigheterna, som ska utses eller inrättas enligt artikel 9 i direktivet, ska använda förteckningen för att göra en nationell riskbedömning i enlighet med artikel 5.

När en medlemsstat identifierar kritiska entiteter ska den ta hänsyn till resultatet av sin riskbedömning samt den strategi för att stärka kritiska entiteters motståndskraft som ska antas. Regeringen beslutade i februari 2026 om Nationell strategi för motståndskraft i samhällsviktig verksamhet 2026–2030. För att en aktör ska identifieras som kritisk entitet enligt direktivet ska vissa kriterier vara uppfyllda. Varje medlemsstat ska vidare upprätta en förteckning över de kritiska entiteter som har identifierats och säkerställa att dessa underrättas om att de har identifierats som kritiska inom en månad från identifieringen. Medlemsstaterna ska också informera de kritiska entiteterna om deras skyldigheter och från och med vilket datum skyldigheterna gäller. Förteckningen ska ses över och uppdateras vid behov men minst vart fjärde år. Efter identifieringen ska varje medlemsstat vidare utan onödigt dröjsmål lämna viss information till kommissionen. (Artiklarna 4, 6 och 7)

Varje medlemsstat ska, enligt artikel 9, utse eller inrätta en eller flera behöriga myndigheter som ansvariga för den korrekta tillämpningen och, vid behov, efterlevnadskontrollen avseende reglerna i CER-direktivet på nationell nivå. Varje medlemsstat ska vidare, enligt samma artikel, utse eller inrätta en gemensam kontaktpunkt, som bland annat ska ha en sambandsfunktion för att säkerställa gränsöverskridande samarbete med de gemensamma kontaktpunkterna i andra medlemsstater.

Medlemsstaterna ska också säkerställa att kritiska entiteter gör en riskbedömning. Medlemsstaterna ska därutöver säkerställa att kritiska entiteter vidtar lämpliga och proportionella tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa sin motståndskraft. Entiteterna ska enligt samma artikel tillämpa en plan för motståndskraft eller ett eller flera likvärdiga dokument med en beskrivning av de åtgärder som har vidtagits. De kritiska entiteterna ska också utse en sambandsansvarig eller motsvarande som kontaktpunkt med de berörda myndigheterna. Medlemsstaterna ska vidare ange de villkor enligt vilka en kritisk entitet får ansöka om bakgrundskontroller av personer med vissa funktioner och uppgifter. (Artiklarna 13 och 14)

Medlemsstaterna ska enligt artikel 15 i direktivet se till att kritiska entiteter utan onödigt dröjsmål lämnar en anmälan till den behöriga myndigheten om incidenter som medför eller kan medföra en betydande störning i tillhandahållandet av samhällsviktiga tjänster. Den gemensamma kontaktpunkten ska informera dess motsvarigheter i andra medlemsstater som påverkas om incidenten har eller kan ha en betydande påverkan på kritiska entiteter och kontinuiteten i tillhandahållandet av samhällsviktiga tjänster i en eller flera andra medlemsstater. Så snart som möjligt efter en anmälan ska den behöriga myndigheten ge entiteten relevant uppföljningsinformation, inklusive information som skulle kunna hjälpa denne att reagera ändamålsenligt på incidenten. Medlemsstaterna ska informera allmänheten om de anser att det skulle ligga i allmänhetens intresse.

En entitet ska betraktas som en kritisk entitet av särskild europeisk betydelse om den har identifierats som kritisk enligt direktivet och den tillhandahåller samma eller liknande samhällsviktiga tjänster till eller i minst sex medlemsstater (artikel 17). För sådana entiteter gäller ett särskilt informationskrav och särskilda skyldigheter enligt direktivet.

På begäran av en medlemsstat som har identifierat en kritisk entitet av särskild europeisk betydelse ska kommissionen anordna ett så kallat rådgivande uppdrag för att bedöma de åtgärder som entiteten har vidtagit för att uppfylla sina skyldigheter enligt direktivet (artikel 18). Genom CER-direktivet inrättas därutöver en grupp för kritiska entiteters motståndskraft. Gruppen ska ge kommissionen stöd samt underlätta samarbete och informationsutbyte mellan medlemsstaterna i frågor som rör direktivet (artikel 19).

För att bedöma om de entiteter som har identifierats enligt direktivet fullgör de skyldigheter som fastställs i direktivet ska medlemsstaterna enligt artikel 21 säkerställa att de behöriga myndigheterna har befogenheter och medel för att bland annat genomföra inspektioner på plats av den kritiska infrastrukturen och utföra eller beställa revisioner av kritiska entiteter. Medlemsstaterna ska vidare till exempel säkerställa att de behöriga myndigheterna har befogenheter och medel för att bland annat kräva att entiteter som träffas av Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) och som har identifierats som kritiska enligt CER-direktivet inom en rimlig tidsfrist lämnar viss information (se vidare avsnitt 4.3). I CER-direktivet görs också flera andra kopplingar till entiteter som omfattas av NIS 2-direktivet (se till exempel artikel 6.4). Enligt artikel 1.2 i CER-direktivet ska medlemsstaterna bland annat med beaktande av förhållandet mellan kritiska entiteters fysiska säkerhet och cybersäkerhet säkerställa att CER-direktivet och NIS 2-direktivet genomförs på ett samordnat sätt.

Medlemsstaterna ska enligt CER-direktivet fastställa regler om sanktioner för överträdelser av de nationella åtgärder som antagits och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande (artikel 22).

4.3 NIS 2-direktivets innehåll i stort

Syftet med NIS 2-direktivet är att förbättra den inre marknadens funktion genom att fastställa åtgärder för att uppnå en hög gemensam cybersäkerhetsnivå inom unionen (artikel 1). NIS 2-direktivet är som utgångspunkt tillämpligt på offentliga eller privata entiteter av den typ som avses i direktivets bilaga 1 eller 2, som uppfyller ett visst storlekskrav och som tillhandahåller sina tjänster eller bedriver sin verksamhet i unionen (artikel 2). Med uttrycket entitet avses enligt artikel 6.38 i direktivet en fysisk eller juridisk person som bildats och erkänts som sådan enligt nationell rätt där den etablerats och som i eget namn får utöva rättigheter och ha skyldigheter. Direktivet är även tillämpligt på vissa entiteter oavsett storlek (artikel 2.2–2.4). Av artikel 2.3 i NIS 2-direktivet framgår att direktivet är tillämpligt på entiteter som identifieras som kritiska entiteter enligt CER-direktivet, oavsett entiteternas storlek. I bilaga 1 och 2 till NIS 2-direktivet anges de 18 sektorer, uppdelade i högkritiska och andra

kritiska sektorer och i viss utsträckning delsektorer, som omfattas av direktivet:

- energi
- transporter
- bankverksamhet
- finansmarknadsinfrastruktur
- hälso- och sjukvårdssektorn
- dricksvatten
- avloppsvatten
- digital infrastruktur
- förvaltning av IKT-tjänster (mellan företag)
- offentlig förvaltning
- rymden
- post- och budtjänster
- avfallshantering
- tillverkning, produktion och distribution av kemikalier
- produktion, bearbetning och distribution av livsmedel
- tillverkning
- digitala leverantörer
- forskning.

Entiteter som omfattas av direktivet ska antingen anses vara väsentliga eller viktiga beroende på bland annat vilken sorts entitet det är fråga om och entitetens storlek (artikel 3). Denna indelning påverkar bland annat vilka tillsynsåtgärder som kan komma i fråga. I artikel 3.1 f i NIS 2-direktivet anges att entiteter som identifierats som kritiska entiteter enligt CER-direktivet ska anses vara väsentliga entiteter enligt NIS 2-direktivet.

Genom NIS 2-direktivet ställs krav på vilka åtgärder berörda aktörer ska vidta för att bland annat hantera risker och förhindra incidenter kopplade till nätverks- och informationssystem som de använder (artikel 21). Dessutom gäller vissa rapporteringsskyldigheter, bland annat att på visst sätt rapportera alla betydande incidenter till en utpekad myndighet (artikel 23). NIS 2-direktivet innehåller även bestämmelser om tillsyns- och efterlevnadskontrollåtgärder samt sanktioner (artiklarna 31–36).

En ny lag som är en del av genomförandet av NIS 2-direktivet, cybersäkerhetslagen (2025:1506), trädde i kraft den 15 januari 2026 (se vidare prop. 2025/26:28).

5 En ny lag om motståndskraft hos kritiska verksamhetsutövare

5.1 CER-direktivet bör genomföras genom en ny lag och vissa uttryck i lagen bör definieras

Regeringens förslag

CER-direktivet ska i huvudsak genomföras genom en ny lag. De som omfattas av lagen ska benämnas kritiska verksamhetsutövare.

Syftet med den nya lagen ska vara att stärka kritiska verksamhetsutövares motståndskraft och förmåga att tillhandahålla samhällsviktiga tjänster.

Vissa uttryck som används i den nya lagen ska definieras.

Hänvisningar i lagen till direktivet ska vara statiska.

Regeringens bedömning

Definitionerna i lagen bör i huvudsak motsvara de som finns i CER-direktivet.

Utredningens förslag och bedömning

Förslaget från utredningen stämmer delvis överens med regeringens. Utredningen föreslår att det kopplat till lagens syfte även ska anges inom vilka sektorer de samhällsviktiga tjänsterna ska tillhandahållas. Utredningen föreslår att ett flertal uttryck som inte används i lagen ska definieras i densamma. Utredningen bedömer att definitionerna som utgångspunkt ska utformas utifrån den systematik och terminologi som används i nationell rätt. Utredningens hänvisningar till EU-rättsakter är dynamiska.

Remissinstanserna

En majoritet av remissinstanserna ställer sig positiva till förslaget om att införa en ny lag eller har inga synpunkter på förslaget.

Ett antal remissinstanser, däribland *Myndigheten för civilt försvar (MCF)* och *Totalförsvarets forskningsinstitut*, understryker vikten av en anpassning till de svenska förhållandena i utformningen av lagstiftningen och av att införa en reglering som är lämplig utifrån den befintliga strukturen för krisberedskap och civilt försvar i Sverige. *Naturvårdsverket* är inne på samma linje och avstyrker den övergripande systematiken för genomförandet av direktivet som föreslås. Många remissinstanser, exempelvis *Försvarsmakten, Trafikverket* och flertalet länsstyrelser, bedömer att det finns ett värde av att i framtiden se över bland annat CER-direktivets koppling till det svenska beredskapssystemet. *Post- och telestyrelsen (PTS)* är av en annan uppfattning. PTS anser att det svenska beredskapssystemet inte bör kopplas till CER-direktivet eftersom direktivet avser den inre marknaden. PTS påpekar att direktivet inte reglerar frågor som rör beredskapssystemen i medlemsstaterna och att det

sistnämnda många gånger ligger nära frågor om nationell säkerhet som tillhör medlemsstaternas nationella regleringskompetens.

Sveriges advokatsamfund, som avstyrker förslaget om införandet av den nya lagen i dess nuvarande form av olika skäl som behandlas i andra avsnitt i denna proposition, påpekar bland annat att många av de uttryck som definieras i CER-regelverket används i andra sammanhang och definieras på olika sätt i olika EU-rättsakter. Samfundet bedömer att detta riskerar att leda till begreppsförvirring.

Några remissinstanser, bland andra *Livsmedelsverket* och *Svensk Dagligvaruhandel*, anser att lagens syfte bör förtydligas.

Advokatfirman Kahn Pedersen anser att lagens föreslagna namn bör ändras. Advokatfirman motsätter sig att uttrycket kritisk verksamhetsutövare används för att definiera den som omfattas av lagen. Advokatfirman pekar på att den nya lagen och säkerhetsskyddslagen (2018:585) i vissa fall har ett helt eller delvis överlappande tillämpningsområde och att det därför är olyckligt om samma uttryck används för att definiera vilka som omfattas av respektive lag.

Skälen för regeringens förslag och bedömning

Uttryck i lagen och hänvisningar till EU-rättsakter

Av artikel 1 a i CER-direktivet framgår att direktivet fastställer skyldigheter för medlemsstaterna att vidta särskilda åtgärder som syftar till att säkerställa att tjänster som är nödvändiga för att upprätthålla viktiga samhällsfunktioner eller central ekonomisk verksamhet inom tillämpningsområdet för artikel 114 i EUF-fördraget tillhandahålls på ett obehindrat sätt på den inre marknaden. I artikeln anges vidare att direktivet innehåller skyldigheter för medlemsstaterna att identifiera kritiska entiteter och stödja entiteterna i deras uppfyllande av de skyldigheter som åläggs dem.

I artikel 1 b anges att direktivet fastställer skyldigheter för kritiska entiteter som syftar till att stärka deras motståndskraft och förmåga att tillhandahålla tjänster som är nödvändiga för att upprätthålla viktiga samhällsfunktioner eller central ekonomisk verksamhet på den inre marknaden på ovan angivet sätt. Av artikel 1 e framgår att det i direktivet fastställs åtgärder i syfte att uppnå en hög grad av motståndskraft för kritiska entiteter, för att säkerställa tillhandahållande av samhällsviktiga tjänster i unionen och förbättra den inre marknadens funktionssätt.

Enligt CER-direktivet kan EU-kommissionen anta delegerade akter respektive genomförandeakter i enlighet med vad som anges i artiklarna 5.1, 13.6 och 18.6. Vidare ska kommissionen i samarbete med medlemsstaterna utarbeta rekommendationer och icke-bindande riktlinjer för att stödja medlemsstaterna i arbetet med att identifiera kritiska entiteter (artikel 6.6).

I direktivet benämns alltså de som omfattas av regleringen som kritiska entiteter. I artikel 2 finns definitioner av andra uttryck som används i direktivet. Motsvarande uttryck bör som utgångspunkt även definieras i den nya lagen under förutsättning att de används i lagen. En kritisk entitet definieras i artikel 2.1 som en offentlig eller privat entitet som har identifierats av en medlemsstat i enlighet med artikel 6 som tillhörande en av de kategorier som anges i den tredje kolumnen i tabellen i bilagan till

direktivet. Endast sådana entiteter som har identifierats som kritiska omfattas av direktivets skyldigheter.

Utredningen föreslår att uttrycket verksamhetsutövare ska användas i den nya lagen i stället för entitet. Utredningen uttryckte i sitt delbetänkande att NIS 2-direktivet inte skulle införlivas direktivnära utan att det skulle ske en anpassning till den systematik som gäller för svensk rätt och att svenskt språkbruk skulle eftersträvas (se SOU 2024:18 s. 123). Utredningen gör i slutbetänkandet bedömningen att motsvarande även bör gälla för införlivandet av CER-direktivet. En direktivsnära terminologi underlättar dock både anpassningen till och tolkningen av den nya lagen. Att avvika från den terminologi som används i CER-direktivet och de rättsakter som direktivet hänvisar till skulle kunna innebära ett felaktigt eller otillräckligt genomförande av direktivet och även motverka ett harmoniserat genomförande av direktivet inom EU. Övervägande skäl talar därför enligt regeringen för att terminologin som används i den nya lagen så långt det är möjligt ska stämma överens med terminologin i CER-direktivet. Definitionerna i den nya lagen bör därför som utgångspunkt motsvara definitionerna i direktivet, även om viss anpassning till nationell rätt måste göras för att underlätta tillämpningen. *Sveriges advokatsamfund* påpekar att det i CER-regleringen används uttryck som också förekommer i andra rättsakter. Regeringen kan inte se att denna omständighet bör påverka hur definitionerna utformas i den lag som genomför direktivet. I linje med detta bör författningstexten som utgångspunkt följa direktivets utformning. Motsvarande bedömningen har gjorts vid införlivandet av NIS 2-direktivet (se vidare prop. 2025/26:28 s. 38 f.).

För att underlätta tillämpningen av den nya lagen anser regeringen att utformningen av lagen i största möjliga mån bör präglas av ett enkelt och lättillgängligt språkbruk. *Advokatfirman Kahn Pedersen* motsätter sig att uttrycket verksamhetsutövare används för att definiera den som omfattas av lagen och anser därför att lagens föreslagna namn bör ändras (se avsnittet nedan om lagens syfte och namn). Verksamhetsutövare är ett vedertaget uttryck och används sedan tidigare exempelvis i säkerhetsskyddslagen. Uttrycket används också i cybersäkerhetslagen. Regeringen anser därför, i likhet med utredningen, att uttrycket verksamhetsutövare bör användas i lagen i stället för entitet. Hänvisningar till CER-direktivet i lagen bör vara statiska och därmed avse EU-rättsakten i dess lydelse vid en viss tidpunkt. Regeringen bedömer i likhet med *Lagrådet* att det kan anges inledningsvis i lagen att det rör sig om statiska hänvisningar men bedömer att en omformulering bör göras i förhållandet till Lagrådets förslag.

Lagens syfte och namn

CER-direktivet syftar till att säkerställa att samhällsviktiga tjänster tillhandahålls på ett obehindrat sätt på den inre marknaden. För att kunna säkerställa det ska enligt direktivet kritiska entiteter som tillhandahåller sådana tjänster identifieras och deras motståndskraft ska stärkas (se artikel 1). Regeringen uttryckte i lagrådsremissen, i likhet med utredningen, att syftet med lagen bör vara att stärka kritiska verksamhetsutövares motståndskraft och förmåga att tillhandahålla samhällsviktiga tjänster och att detta bör återspeglas i lagens namn.

Lagrådet anser att man av språkliga skäl inte kan tala om kritiska verksamhetsutövare och att uttrycket verksamhetsutövare som omfattas av lagen bör användas i stället. Enligt Lagrådets synsätt är det inte heller verksamhetsutövarna som är kritiska, utan den verksamhet eller de funktioner som lagen tar sikte på. Enligt Lagrådet bör lagens namn därför vara lag om motståndskraft i samhällsviktiga tjänster, i stället för lag om motståndskraft hos kritiska verksamhetsutövare. Lagrådet föreslår också flera följdändringar till följd av sin inställning i denna del.

CER-direktivets syfte är att stärka motståndskraften hos vissa särskilt viktiga och utpekade aktörer, vilka i direktivet benämns kritiska entiteter. Eftersom uttrycket entitet är främmande för den svenska lagstiftningen har regeringen valt att i lagen benämna dessa aktörer kritiska verksamhetsutövare. Även om aktörerna ska pekas ut med anledning av de tjänster som de tillhandahåller står det klart att CER-direktivets fokus är på de utpekade subjekten. Det är därför följdenligt och direktivkonformt att även de svenska genomföranderegleрna fokuserar på dessa aktörer. Regeringen bedömer vidare, till skillnad från Lagrådet, att det ur ett språkligt perspektiv är godtagbart att använda uttrycket kritiska verksamhetsutövare. Det i lagrådsremissen föreslagna namnet på lagen motsvarar också hur direktivet benämns. Regeringen finner mot denna bakgrund varken skäl att ändra benämningen på de som omfattas av lagen eller lagens namn i enlighet med Lagrådets förslag och genomför därför inte heller de följdändringar som Lagrådet föreslår. Regeringen bedömer vidare, trots att Lagrådet ifrågasätter behovet av vissa definitioner och föreslår vissa omformuleringar, att de definitioner som föreslås i lagrådsremissen bör finnas med i den nya lagen. Definitionen av uttrycket samhällsviktig tjänst bör dock omformuleras i enlighet med Lagrådets förslag (se vidare avsnitt 6.2).

Regeringen ser, till skillnad från utredningen och med hänvisning till den föreslagna lagens innehåll i övrigt, inte behov av att redan kopplat till beskrivningen av lagens syfte ange inom vilka sektorer de samhällsviktiga tjänsterna ska tillhandahållas (jfr avsnitt 6.2).

Några remissinstanser anser att lagens syfte bör förtydligas. *Svensk Dagligvaruhandel* anser exempelvis att det krävs ett förtydligande i fråga om huruvida lagens syfte är att nå en hög grad av motståndskraft för kritiska entiteter för att säkerställa tillhandahållande av samhällsviktiga tjänster i unionen och förbättra den inre marknadens funktionssätt. Att stärka kritiska verksamhetsutövares motståndskraft och förmåga att tillhandahålla samhällsviktiga tjänster kan ytterst vara av betydelse för Sveriges säkerhet. Även om den nya lagen delvis tar sin utgångspunkt i nationella behov kommer det i förlängningen också att bidra till att främja den inre marknaden. Det är enligt regeringens mening inte nödvändigt att ange detta i lagen.

Kopplingen till det svenska beredskapssystemet

Ett antal remissinstanser, däribland *MCF*, understryker vikten av anpassning till de svenska förhållandena i utformningen av lagstiftningen och av att införa en reglering som är lämplig utifrån den befintliga strukturen för krisberedskap och civilt försvar i Sverige. MCF anser att regleringen bör integreras i de beredskapssektorer som har etablerats i förordningen

(2022:524) om statliga myndigheters beredskap. Många remissinstanser, exempelvis *Försvarsmakten*, bedömer att det finns ett värde av att i framtiden se över bland annat CER-direktivets koppling till det svenska beredskapssystemet. *PTS* är av en annan uppfattning och anser att det svenska beredskapssystemet inte bör kopplas till CER-direktivet.

Som MCF nämner finns det sedan 2022 en struktur för den svenska krisberedskapen och det civila försvaret med ett antal beredskapssektorer som utgör grund för myndighetsgemensam planering och beredskapsutveckling. Det finns i dag 12 beredskapssektorer med tillhörande 67 beredskapsmyndigheter. Det är myndigheter med särskild betydelse för samhällets krisberedskap och totalförsvar. Myndigheterna ska ha god förmåga att motstå hot och risker, förebygga sårbarheter, hantera fredstida krissituationer och genomföra sina uppgifter vid höjd beredskap. Utredningen gör bedömningen att den nya lagens tillämpningsområde, som behandlas vidare i avsnitt 6.2 och 6.3, inte bör gå utöver vad som krävs för genomförande av direktivet. Utredningen ser dock bland annat ett stort värde av att i framtiden se över CER-direktivets koppling till det svenska beredskapssystemet, där möjlighet att ensa såväl begrepp som sektorer som träffas av olika regelverk vore positivt. Utredningens förslag innebär att regelverket som genomför CER-direktivet och beredskapssystemet kommer att gälla delvis parallellt.

Regeringen konstaterar att det, utifrån de förslag som utredningen lämnar och inom ramen för detta lagstiftningsärende, inte finns något utrymme för att göra en anpassning till det svenska beredskapssystemet såsom bland annat MCF efterfrågar. Regeringen har uppmärksammat att detta medför delvis parallella system och att det kan föra med sig negativa effekter. Regeringen tar frågan om de negativa effekter som delvis parallella system i detta sammanhang kan föra med sig, som MCF nämner, på mycket stort allvar. Samtidigt är det av stor vikt att det regelverk som genomför CER-direktivet i Sverige kommer på plats så snart som möjligt, inte minst med anledning av att Europa och Sverige befinner sig i det allvarligaste säkerhetspolitiska läget sedan andra världskrigets slut. Regeringen gör bedömningen att det efter den nya lagens ikraftträdande finns skäl att genomföra en översyn av CER-direktivets koppling till det svenska beredskapssystemet.

5.2 Uppdelning i enskilda och offentliga verksamhetsutövare

Regeringens förslag

Som kritiska verksamhetsutövare ska räknas offentliga och enskilda verksamhetsutövare som har identifierats som kritiska med stöd av lagen.

Hela verksamheten hos en kritisk verksamhetsutövare ska som utgångspunkt omfattas av lagen.

Utredningens förslag

Förslaget från utredningen stämmer överens med regeringens. Utredningen yttrar sig inte i fråga om huruvida enbart den delen av verksamheten som tillhandahåller en samhällsviktig tjänst träffas av den nya lagen eller om verksamhetsutövaren i sin helhet omfattas.

Remissinstanserna

Sveriges universitets- och högskoleförbund (SUHF) undrar om hela verksamheten hos en kritisk verksamhetsutövare omfattas av lagen. Övriga remissinstanser yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag

Kritiska verksamhetsutövare bör delas in i offentliga och enskilda verksamhetsutövare

Enligt artikel 2.1 definieras en kritisk entitet som en offentlig eller privat entitet som medlemsstaten har identifierat i enlighet med artikel 6 som tillhörande en av de kategorier som anges i den tredje kolumnen i tabellen i bilagan till direktivet. Som en följd bör de som omfattas av den nya lagen, i enlighet med utredningens förslag, benämnas kritiska verksamhetsutövare och delas in i enskilda verksamhetsutövare och offentliga verksamhetsutövare som har identifierats som kritiska med stöd av lagen. Förutsättningarna för att identifieras som kritisk verksamhetsutövare behandlas i avsnitt 6.

Verksamhetsutövaren bör som utgångspunkt omfattas i sin helhet

En verksamhetsutövare kan bedriva verksamhet och tillhandahålla tjänster inom flera olika områden varav endast ett faller inom någon av de sektorer och undersektorer som föreslås omfattas av lagen (se vidare avsnitt 6.2). Genom att en verksamhetsutövare identifieras som kritisk uppstår skyldigheter för verksamhetsutövaren enligt lagen (se vidare avsnitt 8 och 9). Frågan är då, som *SUHF* anger, om enbart den delen av verksamheten som tillhandahåller en samhällsviktig tjänst ska omfattas av den nya lagen eller om verksamhetsutövaren i sin helhet ska omfattas. CER-direktivet reglerar inte denna fråga uttryckligen och utredningen berör inte frågan särskilt.

Regeringen anser att frågan om hur lagen ska utformas i detta avseende måste besvaras utifrån direktivets syfte. CER-direktivet handlar om att säkerställa att samhällsviktiga tjänster tillhandahålls på ett obehindrat sätt på den inre marknaden. För att kunna göra det ska kritiska verksamhetsutövare som tillhandahåller sådana tjänster identifieras och deras motståndskraft ska stärkas. Regeringen anser att direktivets utformning talar för att hela verksamhetsutövaren bör omfattas av lagens tillämpningsområde. Regeringen ser även en risk med att låta endast en del av verksamhetsutövarens verksamhet omfattas av lagens tillämpningsområde. En incident i en del av verksamheten som inte omfattas av lagens krav skulle kunna påverka även andra delar av verksamheten. Det skulle också kunna uppstå gränsdragningsproblem när det gäller att bestämma

vilka delar av en verksamhet som omfattas av lagen och därmed olika tolkningar bland berörda verksamhetsutövare.

Regeringen anser därför att en verksamhetsutövare som bedriver verksamhet inom någon av de utpekade sektorerna och undersektorerna, och som i övrigt uppfyller de föreslagna kriterierna för att omfattas av lagen, bör omfattas av regelverkets krav i sin helhet (jfr dock avsnitt 5.4.1 och 5.4.3). Av avsnitt 8.3 framgår dock att regeringen anser att uttrycket incident bör definieras som en händelse som kan medföra en betydande störning eller som medför en störning i den kritiska verksamhetsutövarens tillhandahållande av en samhällsviktig tjänst. Det innebär att det är den samhällsviktiga tjänsten som är i fokus vid bedömningen av vilka åtgärder som en kritisk verksamhetsutövare ska vidta enligt lagen (se vidare avsnitt 8 och 9). Om det krävs för att säkerställa den kritiska verksamhetsutövarens motståndskraft och tillhandahållandet av den samhällsviktiga tjänsten bör åtgärder vidtas även i förhållande till andra delar av verksamheten än den som tillhandahåller tjänsten.

5.3 Vilka bör räknas som offentliga och enskilda verksamhetsutövare?

Regeringens bedömning

Som offentlig förvaltningsentitet i bilagan till CER-direktivet bör räknas en statlig myndighet som har befogenhet att fatta beslut som påverkar fysiska eller juridiska personers rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital.

Regeringens förslag

Även de statliga myndigheter som regeringen bestämmer, som inte räknas som offentliga förvaltningsentiteter i bilagan till CER-direktivet eller ingår i någon annan kategori i bilagan, ska kunna omfattas av lagen och räknas som offentliga verksamhetsutövare om de identifieras som kritiska verksamhetsutövare.

Regeringen, Regeringskansliet, utlandsmyndigheter, kommittéväsendet, myndigheter under riksdagen, domstolar och nämnder som utövar rättsskipning ska inte omfattas av lagen.

Även regioner, kommuner och kommunalförbund, med undantag för fullmäktige och förbundsdirektion, ska räknas som offentlig verksamhetsutövare enligt lagen.

Som enskild verksamhetsutövare ska enligt lagen räknas en kritisk verksamhetsutövare som inte är en offentlig verksamhetsutövare.

Utredningens förslag och bedömning

Förslaget från utredningen stämmer delvis överens med regeringens. Utredningen föreslår att uttrycket offentlig verksamhetsutövare ska avse en aktör som bedriver verksamhet och som är en statlig myndighet, region eller kommun. I utredningens förslag nämns inte kommunalförbund.

Utredningen gör bedömningen att samtliga statliga myndigheter, inklusive statliga affärsverk, bör kunna räknas som offentlig förvaltningsentitet i bilagan till CER-direktivet. Utredningen bedömer att myndigheter som lyder under riksdagen ska undantas men föreslår endast ett undantag för Riksrevisionen, Riksdagens ombudsmän, Sveriges riksbank och Riksdagsförvaltningen. Utredningen föreslår att undantag ska göras för Sveriges domstolar. Utredningen föreslår att uttrycket enskild verksamhetsutövare ska definieras som en juridisk eller fysisk person som bedriver verksamhet och som inte är en statlig myndighet, region eller kommun.

Remissinstanserna

Malmö kommun anser att det är otydligt hur kategorin offentlig verksamhetsutövare ska avgränsas och har synpunkter på att kommuner inte ingår i sektorn offentlig förvaltning enligt den nya lagen men ingår i sektorn enligt NIS 2-regleringen. *Stockholms universitet* och *Sveriges universitets- och högskoleförbund* anser att det är oklart om universitet och högskolor kommer att omfattas av den nya lagen och anser att författningsförslaget avseende identifieringen av kritiska verksamhetsutövare inte ger någon vägledning om vad lärosätena kan förvänta sig. *Sveriges metereologiska och hydrologiska institut (SMHI)* anser att utredningens förslag om att samtliga statliga myndigheter ska inkluderas i kategorin offentliga verksamhetsutövare medför en för myndigheterna opåkallad ökad administrativ börda. SMHI anser att det enligt direktivet krävs att myndigheter, för att omfattas av lagen, har befogenhet att rikta administrativa eller reglerade beslut till fysiska eller juridiska personer som påverkar deras rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital.

Rymdstyrelsen framhåller att det finns fler statliga myndigheter som lyder under riksdagen än som nämns av utredningen och att det torde vara överflödigt att ange att det är Sveriges domstolar som undantas eftersom lagen endast gäller i Sverige. Rymdstyrelsen befarar att detta uttryckssätt även kan innebära en risk för förväxling med det inarbetade uttrycket Sveriges Domstolar.

Kalmar kommun är positiv till att kommunala bolag som bedriver verksamhet som omfattas av lagens bestämmelser räknas som enskilda verksamhetsutövare. Malmö kommun och *Sydvatten* motsätter sig dock att kommunala bolag, utan vinstintresse, likställs med privata företag. *Läkemedelsverket* påpekar att ambitionen är att genomförandet av NIS 2- och CER-direktiven till stora delar ska vara sammanhållen och anser att uttrycket enskild verksamhetsutövare bör definieras på samma sätt i den nya lagen och i cybersäkerhetslagen. *Transportstyrelsen* tolkar förslaget som att en koncern inte kan ses som en kritisk verksamhetsutövare och att en koncern därmed inte kan ha till exempel en gemensam samverkansansvarig, som enligt utredningens förslag ska vara en kontaktpunkt för berörda myndigheter.

Övriga remissinstanser yttrar sig inte särskilt över förslaget och bedömningen.

Skälen för regeringens förslag och bedömning

Direktivets definition av offentlig förvaltningsentitet

I avsnitt 6 föreslår regeringen, i likhet med utredningen, att en förutsättning för att omfattas av den nya lagen ska vara att en verksamhetsutövare har identifierats som kritisk utifrån vissa krav som behandlas i det avsnittet. För att identifieras som kritisk föreslår regeringen bland annat att verksamhetsutövaren ska omfattas av någon av kategorierna i bilagan till CER-direktivet.

Offentlig förvaltning är en av de sektorer som pekas ut i bilagan till CER-direktivet. Uttrycket avser enligt punkten 9 i bilagan till direktivet, där kategorin av entiteter anges, offentliga förvaltningsentiteter hos nationella regeringar såsom de definieras av en medlemsstat i enlighet med nationell rätt. Enligt artikel 2.10 i CER-direktivet ska en offentlig förvaltningsentitet definieras som en entitet som erkänts som sådan i en medlemsstat enligt nationell rätt, med undantag för rättsväsendet, parlament och centralbanker. Därutöver ska fyra kriterier vara uppfyllda.

Det första kriteriet innebär att entiteten ska ha inrättats för att tillgodose ett behov i det allmännas intresse och att verksamheten inte ska ha industriell eller kommersiell karaktär (a). Det andra kriteriet är att entiteten ska ha ställning som juridisk person eller ha lagstadgad rätt att agera för en annan entitet som har ställning som juridisk person (b). Det tredje kriteriet innebär att entiteten ska finansieras till största delen av statliga myndigheter eller av andra offentligrättsliga organ på central nivå, ska stå under administrativ tillsyn av dessa myndigheter eller organ, eller ha ett förvaltnings-, lednings-, eller tillsynsorgan där mer än hälften av ledamöterna utses av statliga myndigheter eller av andra offentligrättsliga organ på central nivå (c). Det sista kriteriet är att entiteten ska ha befogenhet att rikta administrativa eller reglerande beslut till fysiska eller juridiska personer som påverkar deras rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital (d).

Gällande genomförandet av NIS 2-direktivet, där en i allt väsentligt motsvarande definition av uttrycket offentlig förvaltningsentitet finns, drog utredningen slutsatsen att direktivets syfte inte var att dra en skiljelinje mellan offentlig verksamhet utifrån beslut om gränsöverskridande påverkan och beaktade även att NIS 2-direktivet är ett så kallat minimidirektiv. Utredningen bedömer att motsvarande slutsats bör dras kopplat till genomförandet av CER-direktivet. Detta innebär sammantaget enligt utredningen att den nya lagen bör kunna omfatta samtliga statliga myndigheter i Sverige med vissa undantag för bland annat riksdagen. Regeringen gör, av samma anledning som framgår av förarbetena till cybersäkerhetslagen, en annan bedömning i denna del och gör detta av de skäl som redovisas nedan (se vidare prop. 2025/26:28 s. 57 f.).

Endast vissa statliga myndigheter bör kunna omfattas av lagen

Regeringen bedömer, i likhet med utredningen, att uttrycket förvaltningsentiteter hos nationella regeringar för svensk del bör anses motsvara statliga myndigheter. Kriterierna i artikel 2.10 a och c, som bland annat innebär att entiteten ska ha inrättats för att tillgodose behov i det allmännas intresse stämmer väl överens med vad som gäller för svenska statliga

myndigheter. När det gäller kriteriet i artikel 2.10 b, som anger att entiteten ska ha ställning som juridisk person eller ha lagstadgad rätt att agera för annan juridisk person, bör enligt regeringen det sistnämnda innebära att det är tillräckligt med företrädesrätt för att räknas som offentlig förvaltningsentitet och att det inte behöver vara fråga om en egen juridisk person. Statliga myndigheter i Sverige är inte egna juridiska personer. De har dock rätt att företräda den juridiska personen staten.

Kriteriet i artikel 2.10 d, det vill säga att entiteten ska ha befogenhet att fatta vissa beslut med koppling till gränsöverskridande rörlighet för personer, varor, tjänster eller kapital, är mer svårtolkat. Utifrån en EU-rättslig kontext brukar uttrycket gränsöverskridande rörlighet tolkas i linje med de fyra friheterna för EU:s inre marknad enligt EUF-fördraget, det vill säga fri rörlighet för varor, tjänster, personer och kapital.

Många statliga myndigheter kan sägas ha befogenhet att fatta beslut som påverkar fysiska och juridiska personers gränsöverskridande rättigheter. Detta gäller till exempel Polismyndighetens rätt att i vissa fall frihetsberöva personer och Tullverkets befogenheter att omhänderta gods. Vilka statliga myndigheter som kan sägas uppfylla kriteriet beror dock på hur man ser på olika besluts påverkan i förlängningen. Det skulle kunna argumenteras för att även beslut som indirekt påverkar exempelvis möjligheten för en individ att studera, arbeta eller etablera sig i en annan medlemsstat, eller beslut som rör offentlig upphandling med potentiella gränsöverskridande effekter, innebär att kriteriet i artikel 2.10 d är uppfyllt. Med det resonemanget skulle till exempel varje myndighets beslut om anställning indirekt kunna anses ha sådana effekter. Regeringen bedömer dock att det skulle innebära en för extensiv tolkning av kriteriet.

Regeringen konstaterar att CER-direktivet är ett så kallat minimidirektiv, vilket innebär att fler tjänster inom respektive sektor och undersektor än vad som omfattas av bilagan till direktivet skulle kunna omfattas av den nya lagen. Regeringen bedömer dock, i likhet med *SMHI*, att det inte är motiverat att låta samtliga statliga myndigheter träffas av den nya lagens skyldigheter utan att ta hänsyn till kriteriet som anges i artikel 2.10 d. Detta innebär, enligt regeringens mening, att endast de statliga myndigheter som uppfyller samtliga krav i artikel 2.10 och därmed också har befogenhet att fatta beslut som påverkar fysiska eller juridiska personer och deras rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital bör kunna omfattas av lagen i egenskap av offentliga förvaltningsentiteter i enlighet med direktivets krav.

Det kan dock finnas skäl att låta även vissa andra statliga myndigheter, som inte fattar beslut i enlighet med artikel 2.10 d i direktivet, omfattas av lagens krav. Det är till exempel motiverat att en stor andel av beredskapsmyndigheterna omfattas av den nya lagens krav. Med hänvisning till förslaget i avsnitt 5.4.3 om undantag för verksamhetsutövare som bedriver säkerhetskänslig verksamhet eller brottsbekämpande verksamhet bör dock inte samtliga beredskapsmyndigheter omfattas av lagen. Det bör i stället införas en bestämmelse i den nya lagen som innebär att de myndigheter som regeringen bestämmer, med beaktande av de undantag som gäller enligt lagen, ska kunna identifieras som kritiska verksamhetsutövare och då räknas som offentliga verksamhetsutövare.

Regeringen anser att kravet i bilagan till direktivet om att offentliga förvaltningsentiteter ska finnas ”hos” nationella regeringar exkluderar regeringen och myndigheter som lyder under riksdagen. Det bör därför göras ett undantag i lagen för sådana myndigheter. Undantaget innebär att uppräknade myndigheter inte kan identifieras som kritiska i enlighet med förslaget som behandlas i avsnitt 6. Regeringen konstaterar, i likhet med *Rymdstyrelsen*, att det finns fler myndigheter som lyder under riksdagen än de myndigheter som utredningen räknar upp i sitt förslag. I stället för en uppräkning av enskilda myndigheter bör det anges att undantaget gäller generellt för myndigheter under riksdagen. Även Regeringskansliet, utlandsmyndigheter och kommittéväsendet bör undantas från tillämpningsområdet i enlighet med utredningens förslag. Uttrycket utlandsmyndigheter inbegriper ambassader, karriärkonsulat, representationer och delegationer vid internationella organisationer som EU, FN, OECD och Nato.

Rättsväsendet faller utanför direktivets definition av offentlig förvaltningsentitet och bör därför undantas från lagens tillämpningsområde. Utredningen föreslår att undantag ska göras för Sveriges domstolar. Som Rymdstyrelsen framhåller har uttrycket ingen entydig innebörd. Rättsväsendet omfattar de institutioner som ansvarar för rättssäkerhet och rättstrygghet i Sverige. I den engelska språkversionen av direktivet används uttrycket ”the judiciary”, vilket har en snävare innebörd. Enligt regeringens mening bör undantaget träffa rättskipningsorgan såsom domstolar och nämnder som utövar rättskipning. Detta innebär att specialdomstolar, såsom Arbetsdomstolen och Försvarsunderrättelsedomstolen, undantas från lagens krav. Exempelvis Rättshjälpsnämnden, Notarienämnden och Överklagandenämnden för nämndemannauppdrag omfattas också av undantaget. Däremot bör, till skillnad mot vad utredningen resonerar kring, inte Domarnämnden och Rättshjälpsmyndigheten omfattas av undantaget. Motsvarande bedömningar har gjorts i förhållande till cybersäkerhetslagen (se prop. 2025/26:28 s. 55 f.).

Bland andra *Stockholms universitet* anser att det är oklart om universitet och högskolor omfattas av den nya lagen. Högre utbildning och forskning bedrivs dels vid statliga universitet och högskolor som omfattas av högskolelagen (1992:1434), dels vid enskilda utbildningsanordnare som har fått tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina. De statliga universiteten och högskolorna är statliga myndigheter. Dessa ska därför omfattas av lagen i enlighet med direktivets krav, i egenskap av offentliga förvaltningsentiteter, om de har befogenhet att fatta beslut som påverkar fysiska eller juridiska personer och deras rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital. Enskilda utbildningsanordnare som har fått tillstånd att utfärda examina enligt lagen om tillstånd att utfärda vissa examina utgör inte statliga myndigheter och ingår därför inte i sektorn offentlig förvaltning. Statliga universitet, högskolor och enskilda utbildningssamordnare kan omfattas av lagen om de bedriver verksamhet inom någon av de sektorer eller undersektorer som omfattas av bilagan till direktivet, och i övrigt uppfyller de föreslagna kriterierna för att omfattas av lagen (se avsnittet nedan när det gäller enskilda verksamhetsutövare).

Enskilda verksamhetsutövare

I CER-direktivet definieras inte privat entitet, vilket föreslås motsvaras av uttrycket enskild verksamhetsutövare i den nya lagen. Utredningen föreslår att uttrycket enskild verksamhetsutövare ska definieras i lagen och att det ska avse en fysisk eller juridisk person som bedriver verksamhet och som inte är en statlig myndighet, region eller en kommun. Regeringen bedömer att uttrycket enskild verksamhetsutövare i lagen bör avse en verksamhetsutövare som inte är en offentlig sådan. Uttrycket föreslås därmed, som *Läkemedelsverket* anför, definieras på samma sätt som i cybersäkerhetslagen.

Som följer av *Transportstyrelsens* synpunkter finns det skäl att närmare beröra när lagen gäller för koncerner. I avsnitt 6.3 lämnas förslag på vilken reglering som ska gälla för att en verksamhetsutövare ska identifieras som kritisk. I samma avsnitt behandlas vilka kriterier som ska beaktas vid identifieringen. Enligt regeringens mening bör separata bedömningar göras för varje rättssubjekt, det vill säga för varje juridisk person, i fråga om det uppfyller de kriterier som lagen uppställer för att det ska vara fråga om en kritisk verksamhetsutövare. I fråga om en koncern bör således en enskild bedömning göras för varje koncernföretag. Regleringen om kontaktpunkt, som Transportstyrelsen också berör, behandlas i avsnitt 8.2.

Kommuner, regioner och bolag som ägs av kommuner, regioner och staten

Malmö kommun anser att det skapar onödig förvirring att kommuner inte ingår i sektorn offentlig förvaltning eftersom kommunerna samtidigt ingår i sektorn enligt NIS 2-regleringen. Varken regioner eller kommuner ingår i sektorn offentlig förvaltning enligt bilagan till CER-direktivet. Detta utgör en skillnad mot NIS 2-direktivet, där sektorn offentlig förvaltning även omfattar offentliga förvaltningsentiteter på regional nivå. Kommunernas verksamhet ryms däremot inte i sektorn offentlig förvaltning enligt NIS 2-direktivet. Enligt artikel 2.5 a i NIS 2-direktivet får dock medlemsstaterna föreskriva att direktivet ska tillämpas på offentliga förvaltningsentiteter på lokal nivå. Regeringen har gjort bedömningen att samtliga kommuner bör omfattas av cybersäkerhetslagen (se prop. 2025/26:28 s. 55 f.).

Reglering motsvarande den som finns i NIS 2-direktivet om offentliga förvaltningsentiteter på regional nivå och lokal nivå saknas alltså i CER-direktivet. Som utredningen anger är samtliga regioner i Sverige dock vårdgivare enligt definitionen i artikel 3 g i Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patient-rättigheter vid gränsöverskridande hälso- och sjukvård och bedriver därmed sådan verksamhet som ingår i sektorn hälso- och sjukvård i bilagan till CER-direktivet. Detsamma gäller majoriteten av alla kommuner i Sverige eftersom dessa bedriver hemsjukvård. Därutöver kan kommuner även bedriva verksamhet som ingår i andra sektorer i bilagan, exempelvis energi eller avloppsvatten. Samtliga regioner och kommuner bör därmed kunna räknas som kritiska verksamhetsutövare enligt den nya lagen. De kommuner och regioner som identifieras som kritiska verksamhetsutövare bör, som utredningen anger, räknas som offentliga verksamhetsutövare. När det gäller kommunfullmäktige och regionfullmäktige är dessa

beslutande församlingar och bör därmed falla utanför lagens tillämpningsområde.

Ett kommunalförbund är en offentligrättslig juridisk person för samverkan mellan kommuner eller regioner och är fristående i förhållande till sina medlemskommuner. Huvudregeln enligt 3 kap. 8 § kommunallagen (2017:725) är att vilken kommunal angelägenhet som helst får anförtros ett kommunalförbund, vilket även innefattar obligatoriska uppgifter som kommuner och regioner har att sköta utifrån olika författningar. Frågorna om vad samarbetet ska avse och hur arbetet bör bedrivas är i allt väsentligt överlämnat till den kommunala självstyrelsen. Kommunalförbund får utan särskilt lagstöd ha hand om myndighetsutövning. Bedrivs verksamheten genom ett kommunalförbund är det enligt regeringens mening inte kommunen som är verksamhetsutövare utan kommunalförbundet. Det bör tydliggöras i den nya lagen att även kommunalförbund kan omfattas av densamma.

Till exempel *Sydvatten* motsätter sig att kommunala bolag likställs med privata företag. Om berörd verksamhet bedrivs genom kommunal- eller regionägda bolag bör dock inte kommunen eller regionen räknas som verksamhetsutövare efter identifiering. Som följd bör kommunal- och regionägda bolag som bedriver verksamhet som omfattas av lagen räknas som enskilda verksamhetsutövare. Detta gäller även enligt cybersäkerhetslagen (se prop. 2025/26:28 s. 60). På motsvarande sätt bör bolag som helt eller delvis ägs av staten, och som identifieras som kritiska, anses vara enskilda verksamhetsutövare.

Malmö kommun anger att NIS 2-direktivet ställer krav på kommunen i sin helhet medan CER-direktivet ställer krav på den samhällsviktiga tjänst som kommunen tillhandahåller. Det skulle enligt kommunen kunna innebära att åtgärder som vidtas enligt NIS 2-direktivet centraliseras mer, medan riskbedömning och åtgärder enligt CER-direktivet blir mer decentraliserade. Detta kan enligt kommunen skapa utmaningar när det kommer till att ta hänsyn till synergier mellan den nya lagen respektive cybersäkerhetslagen och att undvika dubbelarbete. Enligt regeringen bör som utgångspunkt hela verksamhetsutövaren omfattas av lagens tillämpningsområde (se vidare avsnitt 5.2 och jfr avsnitt 5.4.3). Det innebär att de krav som ställs på verksamhetsutövare som har identifierats som kritiska, när det till exempel gäller att genomföra riskbedömningar och att vidta åtgärder enligt den nya lagen, bör tillämpas på verksamhetsutövaren i sin helhet.

5.4 Undantag från tillämpningsområdet

5.4.1 Undantag kopplat till bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur

Regeringens förslag

För en verksamhetsutövare som har identifierats som kritisk inom någon eller några av sektorerna bankverksamhet, finansmarknads-

infrastruktur eller digital infrastruktur i bilagan till CER-direktivet ska skyldigheterna enligt lagen inte gälla för den delen av verksamheten.

Utredningens förslag

Förslaget från utredningen stämmer överens med regeringens.

Remissinstanserna

Ett antal remissinstanser, däribland *Stiftelsen för Internetinfrastruktur* och *Svenska Bankföreningen,* tillstyrker förslaget. Svenska Bankföreningen pekar på att bankerna redan omfattas av heltäckande krav genom den så kallade DORA-förordningen. *Malmö kommun* är över lag positiv till förslaget men anser att de kritiska verksamhetsutövarna inom de undantagna sektorerna, som för övriga sektorer, bör undantas med stöd av förslaget som behandlas i avsnitt 5.4.2.

Vissa remissinstanser påtalar skillnader mellan skyldigheterna enligt CER-direktivet och annan lagstiftning. Exempelvis *Finansinspektionen* pekar på att det för finansiella företag saknas krav på att riskbedömningen ska beakta andra sektorers beroende av de tjänster som företaget tillhandahåller, motsvarande det krav som gäller för kritiska verksamhetsutövare i övrigt enligt CER-direktivet. Bland andra *Finansiell ID-Teknik BID AB (BID)* och *Post- och telestyrelsen (PTS)* påtalar att förslaget innebär att kritiska verksamhetsutövare i den digitala sektorn inte får samma rätt att begära utdrag ur belastningsregistret. BID anser därför att sådana aktörer inte bör undantas från reglerna om bakgrundskontroller som föreslås införas i den nya lagen och som behandlas i avsnitt 9.

PTS anser att det är otydligt om en verksamhetsutövare som har identifierats som kritisk och som är verksam i både sektorn digital infrastruktur och ytterligare minst en sektor som omfattas av lagen är undantagen från skyldigheterna. Även *Svenska Stadsnätsföreningen* anser att det är oklart om undantaget medför att verksamheten i sin helhet inte behöver uppfylla kraven i lagen. Svenska Stadsnätsföreningen föreslår flera alternativ för att tydliggöra att verksamheten är undantagen oavsett om den organisatoriskt är en del av verksamheten hos en verksamhetsutövare som också bedriver verksamhet inom en sektor som inte är undantagen. Ett alternativ som framförs är att, liksom beträffande säkerhetskänslig verksamhet, undanta just den delen av verksamheten. Ett annat alternativ är att specificera undantaget som att det gäller samhällsviktiga tjänster inom de undantagna sektorerna.

Skälen för regeringens förslag

Undantag för sektorerna enligt direktivet

Varje medlemsstat ska enligt artikel 6.3 i CER-direktivet upprätta en förteckning över kritiska entiteter. Medlemsstaterna ska enligt samma artikel informera kritiska entiteter i de sektorer som anges i punkterna 3, 4 och 8 i tabellen i bilagan till direktivet om att de inte har några skyldigheter enligt kapitlen III och IV i direktivet såvida inte nationella åtgärder föreskriver något annat. De sektorer som anges i punkterna är bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur.

Av artikel 8 i CER-direktivet följer att medlemsstaterna ska säkerställa att artikel 11 och kapitlen III, IV och VI i direktivet, som avser bestämmelser om kritiska entiteters motståndskraft, kritiska entiteter av särskild europeisk betydelse, tillsyn och efterlevnadskontroll, inte är tillämpliga på kritiska entiteter inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur. Artikel 11 avser samarbete mellan medlemsstaterna. Det framgår även av artikel 8 att medlemsstaterna får anta eller behålla bestämmelser i nationell rätt för att uppnå en högre grad av motståndskraft för kritiska entiteter inom angivna sektorer, förutsatt att dessa bestämmelser är förenliga med tillämplig unionsrätt. I skäl 20 och 21 motiveras detta undantag.

Av skäl 20 framgår sammanfattningsvis att NIS 2-direktivet redan ställer krav på åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem samt för att underrätta om betydande incidenter och cyberhot för sektorn digital infrastruktur. Dessa krav är enligt samma skäl minst likvärdiga kraven i CER-direktivet. På motsvarande sätt anges i skäl 21 att det i olika EU-rättsakter redan finns heltäckande krav på finansiella entiteter för att hantera alla risker de ställs inför, inklusive operativa risker, och säkerställa driftskontinuitet. Det handlar bland annat om Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (DORA-förordningen) som *Svenska Bankföreningen* nämner. För att undvika dubbelarbete och onödig administration bör därför, enligt samma skäl, bestämmelserna i artikel 11 och kapitel III, IV och VI i CER-direktivet inte gälla för dem. Med tanke på hur viktiga de tjänster som tillhandahålls av entiteter inom sektorn digital infrastruktur och i finanssektorn är för kritiska entiteter som tillhör alla andra sektorer, bör dock enligt angivna skäl medlemsstaterna, med utgångspunkt i de kriterier och enligt det förfarande som föreskrivs i CER-direktivet, identifiera entiteter som tillhör sektorn digital infrastruktur och i finanssektorn som kritiska entiteter. Strategierna, medlemsstaternas riskbedömningar och de stödåtgärder som anges i kapitel II i CER-direktivet bör följaktligen omfatta även dessa sektorer enligt samma skäl.

Vilket undantag bör göras i lagen?

Av CER-direktivet följer alltså att verksamhetsutövare inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur förvisso ska kunna pekas ut som kritiska, men att direktivets krav endast i mycket begränsad utsträckning bör gälla för dem. Vissa remissinstanser påtalar skillnader i skyldigheterna enligt CER-direktivet och annan lagstiftning, och förespråkar att skyldigheter enligt den nya lagen helt eller delvis ändå ska gälla för dessa verksamhetsutövare. Regeringen anser dock, till skillnad från till exempel *BID*, att det för att undvika en ytterligare administrativ börda för dessa verksamhetsutövare inte bör ställas strängare krav än vad som gäller enligt direktivet.

I lagen bör därför införas ett visst undantag som innebär att skyldigheterna enligt lagen att göra en anmälan, göra en riskbedömning, vidta åtgärder för motståndskraft, inbegripet att göra en befattningsanalys och

genomföra bakgrundskontroller, samt genomföra incidentrapportering inte gäller för kritiska verksamhetsutövare inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur (se vidare avsnitt 7–9). Regeringen anser, till skillnad mot *Malmö kommun*, att det finns ett värde i att tydligt reglera detta undantag i en särskild bestämmelse. Som framgår nedan bör det i lagen tydliggöras att undantaget gäller endast för verksamhetsutövare som har identifierats som kritiska inom någon eller några av sektorerna. Nedan redogörs för vad som gäller om verksamhetsutövaren också bedriver annan verksamhet som omfattas av lagen som bland andra *PTS* tar upp.

Lagrådet anser bland annat att det är otydligt vad lagen innebär för en verksamhetsutövare som omfattas av lagen men inte har några skyldigheter enligt densamma. Skälet till den föreslagna ordningen är att vissa aktörer, enligt CER-direktivet, ska identifieras som kritiska entiteter utan att omfattas av skyldigheterna enligt direktivet (se artikel 6.3 och skäl 20 respektive 21 i CER-direktivet). För att genomföra direktivet krävs motsvarande reglering i den nya lagen. Identifieringen som kritisk verksamhetsutövare får inga konsekvenser för verksamhetsutövaren.

Regeringen har den 11 september 2025 beslutat att ge en särskild utredare i uppdrag att ta ett brett grepp om frågan om bakgrundskontroller (dir. 2025:83). Det handlar till exempel om vilka ytterligare aktörer som bör få tillgång till eller utvidgad tillgång till utdrag från belastningsregistret, vilket är en fråga som bland andra BID och PTS lyfter. Uppdraget ska redovisas senast den 11 mars 2027.

Vad gäller om verksamhetsutövaren också bedriver annan verksamhet som omfattas av lagen?

Bland andra *PTS* påtalar att det är otydligt vad undantaget innebär för en verksamhetsutövare som också bedriver verksamhet i någon annan sektor som omfattas av den nya lagen. Någon uttrycklig reglering av denna fråga finns inte i direktivet.

Skälen för att undanta sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur från de skyldigheter som annars gäller för kritiska entiteter enligt CER-direktivet är, enligt skäl 20 och 21, att undvika dubbelarbete och onödig administration eftersom det för dessa verksamhetsutövare redan finns sektorsspecifika regleringar som innehåller heltäckande krav. Om verksamhetsutövaren har identifierats som kritisk även inom en annan sektor än sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur bör lagen gälla i sin helhet i förhållande till den förstnämnda delen av verksamheten. Även om regeringen har förståelse för synpunkten att det kan vara svårt att särskilja vilken del av verksamheten som är undantagen från den övriga anser regeringen inte att artikel 8 i direktivet ger utrymme för en annan lösning. Om någon annan ordning hade varit avsedd borde rimligen artikel 8 ha utformats som att verksamhetsutövarna helt undantas från direktivets tillämpningsområde snarare än att de undantas från skyldigheterna att vidta vissa åtgärder. Regeringen anser, i likhet med *Svenska Stadsnätsföreningen,* att det bör framgå av lagen att det är just den delen av verksamheten som bedrivs inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur som undantas från skyldig-

heterna enligt lagen. Enligt regeringen uppnås detta genom att det i lagen anges att för en verksamhetsutövare som har identifierats som kritisk inom någon eller några av de i undantagsbestämmelsen angivna sektorerna gäller inte skyldigheterna enligt lagen för den delen av verksamheten.

5.4.2 Undantag på grund av krav i andra författningar

Regeringens förslag

Om det i lag eller annan författning finns bestämmelser som innehåller krav på åtgärder för motståndskraft ska de bestämmelserna gälla om verkan av kraven minst motsvarar verkan av skyldigheterna enligt den nya lagen, med beaktande av bestämmelsernas omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till kraven i bestämmelserna.

Utredningens förslag

Förslaget från utredningen stämmer delvis överens med regeringens. Utredningen föreslår att undantaget ska gälla om annan författning innehåller bestämmelser om krav på riskbedömning, åtgärder för motståndskraft, bakgrundskontroller och incidentrapportering. Utredningen föreslår att regeringen i föreskrifter ska få ange vilka andra bestämmelser som har motsvarande verkan. Utredningen föreslår att det ska införas ett särskilt undantag om att lagen inte ska gälla för sådant som regleras i cybersäkerhetslagen.

Remissinstanserna

Många remissinstanser, däribland *Luftfartsverket, Svenskt Näringsliv* och flertalet länsstyrelser, tillstyrker förslaget och understryker vikten av att regeringen ges möjlighet att föreskriva vilka bestämmelser som har motsvarande verkan. *Energiföretagen Sverige* anser att en grundlig utredning avseende befintliga regleringar är nödvändig för att förhindra överlappningar och åstadkomma regelefterlevnad. *Försäkringskassan* anser att det bör förtydligas att kraven ska gälla i stället för lagen. *Karlstads kommun* delar utredningens uppfattning om att regeringen bör ge tillsynsmyndigheterna i uppdrag att utreda vilka kategorier av verksamhetsutövare inom respektive tillsynsområde som omfattas av annan lag eller andra bindande unionsrättsakter som innehåller bestämmelser med motsvarande verkan. *Transportstyrelsen* anser att det är oklart om en verksamhetsutövare kan undantas från kraven i CER-direktivet endast om det finns motsvarande krav på samtliga områden som utredningen föreslår, det vill säga riskbedömning, åtgärder för motståndskraft, bakgrundskontroller och incidentrapportering, eller om verksamhetsutövaren kan undantas från vissa delar av direktivet. Transportstyrelsen anser att det borde framgå av lagen vilka bestämmelser som har motsvarande verkan som bestämmelserna i lagen. *Stockholms kommun* anser att det även bör framgå att sanktionsavgift inte ska kunna

tas ut om en verksamhetsutövare uppfyller motsvarande krav i annan författning.

Flera remissinstanser, däribland *Tech Sverige* och ett antal kommuner, är positiva till utredningens förslag om att införa en bestämmelse som uttrycker att lagen inte gäller för sådant som regleras i cybersäkerhetslagen. Delvis samma remissinstanser anser att det är viktigt att förhållandet mellan lagarna förtydligas. Några remissinstanser, bland andra *Stiftelsen för Internetinfrastruktur, Säkerhets- och försvarsföretagen (SOFF)* och *Teknikföretagen*, anser att detta ska göras av tillsynsmyndigheterna. Ett antal remissinstanser anser att den föreslagna bestämmelsen bör omformuleras. Exempelvis *Livsmedelsverket* föreslår att lagen inte ska tillämpas i den mån cybersäkerhetslagen ställer krav på åtgärder som är tillräckliga för att uppnå en motsvarande nivå av skydd för den samhällsviktiga tjänsten. SOFF och Teknikföretagen anser att det möjligen vore lämpligare att göra gällande att åtgärderna som ska vidtas enligt den nya lagen, i den mån åtgärderna inte är direkt motsvarande vad som följer av cybersäkerhetslagen, ska vidtas utöver åtgärderna enligt cybersäkerhetslagen. *Post- och telestyrelsen (PTS)* påtalar, kopplat till förslaget i avsnitt 5.4.1 om ett särskilt undantag för bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur, att cybersäkerhetslagen inte ställer upp krav kopplat till den fysiska miljön på samma sätt som CER-direktivet. Transportstyrelsen anser att det borde framgå av lagen vilka delar av cybersäkerhetslagen som inte gäller. *Advokatfirman Kahn Pedersen* bedömer att den föreslagna bestämmelsen är överflödig.

Skälen för regeringens förslag

Undantag för åtgärder enligt andra regelverk med minst motsvarande verkan

I artikel 1.3 i CER-direktivet anges att om det enligt bestämmelser i sektorsspecifika unionsrättsakter krävs att kritiska entiteter ska vidta åtgärder för att stärka sin motståndskraft och om de kraven erkänns av medlemsstaten som åtminstone likvärdiga med de motsvarande skyldigheter som fastställs i direktivet ska de berörda bestämmelserna i CER-direktivet, inbegripet bestämmelserna om tillsyn och efterlevnadskontroll, inte vara tillämpliga. Som framgår av skäl 10 till direktivet bör i sådant fall de relevanta bestämmelserna i unionsrättsakterna tillämpas.

Regeringen konstaterar att undantaget i CER-direktivet tar sikte på sektorsspecifika unionsrättsakter som innehåller bestämmelser som innebär att det krävs att kritiska entiteter vidtar åtgärder för att stärka sin motståndskraft med motsvarande verkan. Regeringen anser att undantaget, i enlighet med utredningens förslag, bör gälla enligt den nya lagen oavsett om bestämmelserna finns i EU-rättsakter eller i nationell författning. Utredningen föreslår, vilket också *Transportstyrelsen* nämner, att undantaget ska gälla om annan författning innehåller bestämmelser om krav på riskbedömning, åtgärder för motståndskraft, bakgrundskontroller och incidentrapportering. De bestämmelser som avses i artikel 1.3 i direktivet bör dock enligt regeringen endast vara de som avser krav på åtgärder för motståndskraft, inbegripet att göra en befattningsanalys och genomföra bakgrundskontroller, som fastställs i artiklarna 13 och 14. Undantaget i lagen bör därmed begränsas i förhållande till utredningens

förslag. Undantaget innebär, som *Försäkringskassan* framhåller, att kraven i den andra författningen gäller i stället för den nya lagens krav. Vad som bör beaktas i samband med beslut om sanktionsavgift, som *Stockholms kommun* nämner, behandlas i avsnitt 11. Vad som avses med uttrycket motståndskraft och åtgärder för motståndskraft behandlas i avsnitt 8.2.

Utredningen föreslår att det i en bilaga till förordningen som hör till den nya lagen ska framgå vilka författningar som innehåller bestämmelser med motsvarande verkan. Bestämmelserna i bilagan bör enligt utredningen beredas av den eller de myndigheter som regeringen finner lämpligt. Utredningen föreslår också att regeringen ska ge tillsynsmyndigheterna i uppdrag att utreda vilka kategorier av verksamhetsutövare inom respektive tillsynsområde som omfattas av annan lag eller andra bindande unionsrättsakter som innehåller bestämmelser med motsvarande verkan. Det är dock enligt regeringen, och trots att flera remissinstanser ställer sig bakom utredningens förslag, inte görbart att sammanställa samtliga rättsregler som kan anses ha motsvarande verkan. Utredningens förslag i denna del bör därför inte genomföras. Motsvarande bedömning gjordes kopplat till genomförandet av NIS 2-direktivet (se prop. 2025/26:28 s. 70). Regeringen konstaterar dock att motsvarande bestämmelser kan finnas till exempel kopplat till hamnskydd. Nedan behandlas frågan om det bör införas ett särskilt undantag i förhållande till cybersäkerhetslagen.

Bör det införas ett särskilt undantag i förhållande till cybersäkerhetslagen?

I artikel 1.2 i CER-direktivet anges att direktivet inte ska vara tillämpligt på frågor som omfattas av NIS 2-direktivet, utan att detta påverkar tillämpningen av artikel 8 i direktivet. Vidare anges att medlemsstaterna, med beaktande av förhållandet mellan kritiska entiteters fysiska säkerhet och cybersäkerhet, ska säkerställa att NIS 2- och CER-direktiven genomförs på ett samordnat sätt. Innebörden av artikel 8 behandlas i avsnitt 5.4.1. I det avsnittet föreslår regeringen att skyldigheterna enligt lagen inte ska gälla för en verksamhetsutövare som har identifierats som kritisk inom någon eller några av sektorerna bankverksamhet, finansmarknadsinfrastruktur eller digital infrastruktur när det gäller den delen av verksamheten. Av skäl 9 till CER-direktivet framgår att eftersom cybersäkerhet hanteras i tillräcklig grad genom NIS 2-direktivet bör de frågor som omfattas av det direktivet uteslutas från tillämpningsområdet för CER-direktivet, utan att det påverkar tillämpningen av den särskilda ordningen för entiteter inom sektorn för digital infrastruktur. Av artikel 2.3 i NIS 2-direktivet framgår att direktivet är tillämpligt på entiteter som identifieras som kritiska entiteter enligt CER-direktivet, oavsett entiteternas storlek. En entitet som har identifieras som kritisk enligt CER-direktivet ska enligt artikel 3.1 f i NIS 2-direktivet vidare räknas som väsentlig entitet enligt NIS 2-direktivet.

Utredningen gör bedömningen att artikel 1.2 i CER-direktivet betyder att regleringen som genomför NIS 2-direktivet har företräde framför den reglering som genomför CER-direktivet och att detta bör framgå av den nya lagen. Utredningen föreslår att ett undantag bör utformas som att den nya lagen inte gäller för sådant som regleras i cybersäkerhetslagen. Detta

markerar enligt utredningen att lagen är subsidiär, men endast för sådant som faktiskt är reglerat och skyddas av cybersäkerhetslagen. Flera remissinstanser, däribland *Tech Sverige*, är som anges ovan positiva till utredningens förslag men ett antal remissinstanser anser att den föreslagna bestämmelsen bör omformuleras.

Vad som är innebörden av artikel 1.2 är, enligt regeringens mening, inte helt tydligt. Frågan är om artikeln är avsedd att utgöra ett undantag från tillämpningsområdet för CER-direktivet. Danmark har i den lag som genomför CER-direktivet i nationell rätt infört ett liknande undantag som utredningen föreslår (se 1 § andra stycket Lov om kritiske enheders modstandsdygtighed [CER-loven], LOV nr 433 af 06/05/2025). I förarbetena till den danska lagen konstateras med anledning av artikel 1.2 i CER-direktivet att cybersäkerhet regleras särskilt i NIS 2-direktivet och därför undantas från CER-direktivets tillämpningsområde (se Forslag til Lov om kritiske enheders modstandsdygtighed [CER-loven] s. 15). Något motsvarande undantag finns inte i den lag som genomför CER-direktivet i Finland (se lag om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft [310/2025]). Däremot anges i den finska lagen att bestämmelser om skyldigheten för en kritisk aktör som identifierats enligt den lagen att hantera cybersäkerhetsrelaterade risker finns i cybersäkerhetslagen (124/2025) (3 §). Den sistnämnda bestämmelsen påminner närmast om en så kallad upplysningsbestämmelse.

Tolkningen av artikel 1.2 bör enligt regeringens mening göras utifrån skäl 9 och delvis även skäl 20 i CER-direktivet. Eftersom cybersäkerhet, enligt skälen, hanteras i tillräcklig grad genom NIS 2-direktivet och för att undvika dubbelarbete och minska den administrativ bördan för kritiska verksamhetsutövare som omfattas av båda direktiven parallellt, bör den nya lagen inte innebära krav på motsvarande åtgärder som ska vidtas enligt NIS 2-direktivet. Frågan är hur detta ska komma till uttryck i den nya lagen.

Utredningen föreslår att ett undantag bör utformas som att den nya lagen inte gäller för sådant som regleras i cybersäkerhetslagen. Regeringen anser att ett sådant undantag är alltför otydligt. Regeringen kan konstatera att cybersäkerhetslagen och den lag som genomför CER-direktivet i stora delar kommer att innehålla olika slags reglering. En verksamhetsutövare som omfattas av endast cybersäkerhetslagen omfattas av andra krav, som ska vidtas utifrån ett annat syfte, än en verksamhetsutövare som omfattas av den nya lagen. Som exempelvis *PTS* påtalar ställer cybersäkerhetslagen inte upp krav kopplat till den fysiska miljön på samma sätt som CER-direktivet. Regeringen konstaterar dock att det även i cybersäkerhetslagen bland annat finns reglering om incidentrapportering. Artikel 1.2 bör, enligt regeringens mening, inte innebära att cybersäkerhetslagens reglering om till exempel incidentrapportering ska gälla framför den incidentrapportering som ska ske enligt CER-direktivet (jfr artikel 8). Syftet bör i stället, som anges ovan, vara att undvika dubbelreglering i den mån regelverken överlappar varandra och att regleringen som genomför NIS 2-direktivet i sådant fall ska ha företräde.

I linje med *Advokatfirman Kahn Pedersens* resonemang bör cybersäkerhetslagen betraktas som en sådan författning som innehåller krav på åtgärder för motståndskraft som kan anses ha motsvarande verkan som

vissa av kraven enligt lagen som genomför CER-direktivet. I lagrådsremissen gör regeringen bedömningen att det inte behöver införas något särskilt undantag kopplat till cybersäkerhetslagen för att den lagen ska ha företräde framför den nya lagen i den mån regleringarna överlappar.

Lagrådet uttrycker att undantaget kopplat till bestämmelser med motsvarande verkan främst torde syfta på föreskrifterna i cybersäkerhetslagen och anger att det finns ett undantag i 1 kap. 10 § den lagen med motsvarande innebörd som undantaget i den nya lagen. Lagrådet anser att det med den reglering som föreslås blir otydligt vilken lag som ska tillämpas om cybersäkerhetslagen och den nya lagen har samma verkan. I författningskommentaren sägs, utan reservationer, att cybersäkerhetslagen har företräde framför den i lagrådsremissen föreslagna lagen i den mån regleringarna överlappar varandra. Detta stämmer dock inte så som Lagrådet uppfattar den föreslagna lagtexten. Om avsikten är att cybersäkerhetslagen alltid ska ha företräde framför den nya lagen måste ett särskilt undantag införas i lagen enligt Lagrådet.

I 1 kap. 10 § cybersäkerhetslagen anges att om det i lag eller annan författning finns bestämmelser som innehåller krav på säkerhetsåtgärder eller incidentrapportering ska de bestämmelserna gälla om verkan av kraven minst motsvarar verkan av skyldigheterna enligt 2 kap. 3–10 §§ den lagen, med beaktande av bestämmelsernas omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till kraven i bestämmelserna.

Regeringen konstaterar att cybersäkerhetslagen, enligt 2 kap. 3 § samma lag, innebär att verksamhetsutövare är skyldiga att vidta lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att skydda nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och systemens fysiska miljö mot incidenter. Dessa slags åtgärder benämns säkerhetsåtgärder i cybersäkerhetslagen och nämns alltså i 1 kap. 10 § cybersäkerhetslagen. I 2 kap. 4–10 §§ samma lag, som också nämns i 1 kap. 10 §, regleras krav på utbildning om säkerhetsåtgärder för personer som ingår i verksamhetsutövarens ledning, incidentrapportering och informationsskyldighet. Det undantag som föreslås införas i den nya lagen tar, till skillnad från det undantag som finns i cybersäkerhetslagen, endast sikte på bestämmelser som innehåller motsvarande krav på åtgärder för motståndskraft. Vad som avses med åtgärder för motståndskraft behandlas i avsnitt 8.2.

Vid bedömningen av vilka åtgärder för motståndskraft som en kritisk verksamhetsutövare ska vidta enligt den nya lagen är den samhällsviktiga tjänsten i fokus och inte de nätverks- och informationssystem som verksamhetsutövaren använder för sin verksamhet eller för att tillhandahålla sina tjänster. Regeringen har svårt att se att den nya lagen och cybersäkerhetslagen skulle innebära motsvarande krav i någon större utsträckning eftersom regleringarna innebär att olika slags åtgärder ska vidtas och dessutom utifrån delvis olika fokus. Det föreslagna undantaget har inte heller någon särskild koppling till föreskrifterna i cybersäkerhetslagen utan motsvarande bestämmelser kan, som anges ovan, finnas till exempel kopplat till hamnskydd. Om det ändå skulle uppstå en situation där regleringarna faktiskt kan anses överlappa varandra, när det gäller krav på åtgärder för att skydda nätverks- och informationssystem, bör den nya lagen inte anses innebära motsvarande krav. Undantaget i cybersäkerhetslagen kommer då inte att kunna tillämpas av dem som omfattas av den nya

lagen och cybersäkerhetslagen har i en sådan situation alltså företräde framför den nya lagen i enlighet med vad som kommer till uttryck i artikel 1.2 i CER-direktivet.

I avsnitt 6.5 föreslår regeringen att en kritisk verksamhetsutövare ska omfattas av kraven i cybersäkerhetslagen och räknas som en väsentlig verksamhetsutövare enligt den lagen. Det ställs inte upp några andra krav utöver att verksamhetsutövaren ska vara identifierad som kritisk verksamhetsutövare enligt den nya lagen. Det noteras, även om frågan om utpekandet av tillsynsmyndigheterna inte är föremål för behandling i denna proposition i enlighet med resonemanget i avsnitt 10.1, att utredningen föreslår att samma myndigheter ska pekas ut som tillsynsmyndigheter enligt den nya lagen och cybersäkerhetslagen. I den mån svårigheter att avgöra vilka krav som gäller enligt respektive lag skulle uppstå finns det viss möjlighet att få vägledning och stöd från de utpekade myndigheterna (jfr 6 § förvaltningslagen [2017:900]). Sammanfattningsvis bedömer regeringen att det varken är motiverat att införa ett särskilt undantag i lagen kopplat till cybersäkerhetslagen eller i övrigt genomföra de ändringar som Lagrådet föreslår i denna del. Eftersom undantaget är formulerat på motsvarande sätt som i cybersäkerhetslagen bedömer regeringen inte heller att det bör göras en sådan omformulering som Lagrådet föreslår i övrigt.

5.4.3 Undantag för viss säkerhetskänslig verksamhet och brottsbekämpande verksamhet

Regeringens förslag

Lagen ska inte gälla för statliga myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen eller som till övervägande del bedriver brottsbekämpande verksamhet.

För en enskild verksamhetsutövare som bedriver enbart säkerhetskänslig verksamhet eller som erbjuder tjänster till enbart en sådan statlig myndighet som anges ovan ska skyldigheterna enligt lagen att göra en anmälan, göra en riskbedömning, vidta åtgärder för motståndskraft och rapportera incidenter inte gälla.

För andra kritiska verksamhetsutövare som till någon del bedriver säkerhetskänslig verksamhet eller brottsbekämpande verksamhet eller till någon del erbjuder tjänster till en sådan statlig myndighet som anges ovan ska angivna skyldigheter inte gälla i förhållande till den säkerhetskänsliga verksamheten, den brottsbekämpande verksamheten eller den verksamhet som erbjuder tjänsterna.

Utredningens förslag

Förslaget från utredningen stämmer delvis överens med regeringens. Utredningen föreslår att regeringen i föreskrifter ska få ange vilka statliga myndigheter som bedriver säkerhetskänslig verksamhet eller brottsbekämpning till övervägande del. Utredningen föreslår att undantaget för andra offentliga verksamhetsutövare än sådana statliga myndigheter bör utformas på ett sådant sätt att det endast undantar den del av den

samhällsviktiga tjänsten som utgör brottsbekämpning eller är säkerhetskänslig. Utredningen föreslår inget särskilt undantag för verksamhetsutövare som enbart eller till någon del erbjuder tjänster till en statlig myndighet som till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpande verksamhet. Utredningen föreslår att tillsynsmyndigheten ska underrätta den enligt säkerhetsskyddslagen ansvariga tillsynsmyndigheten om en kritisk verksamhetsutövare anger att den samhällsviktiga tjänsten till någon del är säkerhetskänslig. Utredningen föreslår även att en ny bestämmelse ska införas i säkerhetsskyddslagen som innebär att tillsynsmyndigheten inom fem arbetsdagar från att en sådan underrättelse har mottagits ska meddela tillsynsmyndigheten enligt den nya lagen huruvida den kritiska verksamhetsutövaren har anmält att den bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen.

Remissinstanserna

Flera myndigheter, däribland *Försvarsmakten*, *Försvarsunderrättelsedomstolen* och *Statens inspektion för försvarsunderrättelseverksamheten*, tillstyrker förslaget om att statliga myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet ska undantas från lagens tillämpningsområde och att regeringen ska ange dessa myndigheter i föreskrifter. *Livsmedelsverket* anser dock att strukturen inte är förenlig med säkerhetsskyddslagstiftningens systematik, där det är verksamhetsutövaren som bedömer i vilken utsträckning den bedriver säkerhetskänslig verksamhet. Livsmedelsverket förespråkar att samtliga verksamhetsutövare som bedriver säkerhetskänslig verksamhet ska omfattas av lagen med begränsningen som föreslås för kritiska verksamhetsutövare inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur i avsnitt 5.4.1. Flertalet av länsstyrelserna anser i stället att hela den offentliga sektorn bör omfattas av lagen för att underlätta tillämpningen och öka acceptansen för regelverket. *Myndigheten för civilt försvar (MCF)* och *Säkerhetspolisen* anser att även den säkerhetskänsliga verksamheten bör omfattas av kraven på att vidta åtgärder för stärkt motståndskraft utifrån ett allriskperspektiv i syfte att komplettera kraven som gäller kopplat till säkerhetsskydd. Säkerhetspolisen för fram att frågan om hur en enhetlig reglering av åtgärder för motståndskraft hos verksamhetsutövare som tillhandahåller kritiska samhällstjänster ska utformas bör utredas vidare. *Sydvatten* bedömer att verksamhetsutövare som omfattas av säkerhetsskyddslagstiftningen inte bör undantas från kravet på bakgrundskontroller som behandlas i avsnitt 9, förutom i de fall då säkerhetsskyddslagstiftningen ställer skarpare krav.

Flera remissinstanser resonerar kring om de bör omfattas av lagen eller inte med hänvisning till att de bedriver säkerhetskänslig verksamhet. Bland andra *Svenskt Vatten* framhåller att gränsdragningen gentemot säkerhetsskyddslagstiftningen blir viktig och utifrån de nya reglerna behöver förtydligas. *Tullverket* anser att förslaget innebär att fler myndigheter omfattas av lagens tillämpningsområde än vad som krävs enligt direktivet, och anser att lagstiftningen bör utformas mer direktivskonformt. Tullverket anser att direktivet inte kräver att någon av de uppräknade verksamheterna, endast sedd för sig, bedrivs till övervägande del för att en myndighet ska undantas från lagens tillämpningsområde.

Tullverket anser att det är tydligt att undantaget bör tillämpas på myndigheter som till övervägande del ägnar sig åt de uppräknade områdena även sett tillsammans. Tullverket noterar vidare att gränsdragningen i förhållande till de myndigheter som bör falla innanför direktivets tillämpningsområde formuleras annorlunda i direktivet, nämligen som att undantaget inte gäller för förvaltningsentiteter som endast marginellt ägnar sig åt de aktuella verksamhetsområdena. Tullverket avstyrker därför förslaget i denna del.

Vissa remissinstanser yttrar sig över utredningens förslag om att tillsynsmyndigheten ska underrätta ansvarig tillsynsmyndighet enligt säkerhetsskyddslagen om en kritisk verksamhetsutövare anger att den samhällsviktiga tjänsten till någon del är säkerhetskänslig, och att tillsynsmyndigheten enligt säkerhetsskyddslagen ska meddela huruvida verksamhetsutövaren har anmält att den bedriver sådan verksamhet enligt den lagen. Däribland *Transportstyrelsen* och ett antal länsstyrelser, för fram att uppgiften om att en verksamhetsutövare har anmält att den bedriver säkerhetskänslig verksamhet inte ger närmare upplysningar om i vilken omfattning säkerhetskänslig verksamhet bedrivs eller i vilken del av verksamheten. *Affärsverket svenska kraftnät* har synpunkter på utredningens förslag som innebär att tillsynsmyndigheten enligt säkerhetsskyddslagen ska lämna informationen inom fem arbetsdagar. Affärsverket svenska kraftnät anser att tidsramen inte behöver anges i ett visst antal arbetsdagar, och påtalar att den typen av tidsgränser framstår som främmande inom säkerhetsskyddslagstiftningen. I stället bör det enligt Affärsverket svenska kraftnät anges att tillsynsmyndigheten enligt säkerhetsskyddslagen ska lämna informationen inom skälig tid eller liknande. Myndigheten anser även att bestämmelsen bör införas i förordning i stället för i lag.

Skälen för regeringens förslag

Undantaget i direktivet

Av artikel 1.5 i CER-direktivet följer att direktivet inte påverkar medlemsstaternas ansvar att skydda den nationella säkerheten och försvaret eller deras befogenhet att skydda andra väsentliga statliga funktioner, inbegripet att säkerställa statens territoriella integritet och upprätthålla lag och ordning.

I artikel 1.6 anges att direktivet inte är tillämpligt på offentliga förvaltningsentiteter som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning. I uttrycket brottsbekämpning ingår utredning, upptäckt och lagföring av brott. Enligt skäl 11 i direktivet bör undantaget för offentliga förvaltningsentiteter omfatta entiteter vars verksamhet till övervägande del bedrivs på de områden som anges i artikel 1.6. Offentliga förvaltningsentiteter vars verksamhet endast marginellt hänför sig till dessa områden bör dock, enligt samma skäl, inte vara undantagna från direktivets tillämpningsområde. Vid tillämpningen av direktivet anses vidare entiteter med tillsynsbefogenheter inte bedriva verksamhet på brottsbekämpningsområdet, och de är därför inte undantagna från tillämpningsområdet för direktivet. Däremot är offentliga förvaltningsentiteter som inrättats gemensamt med ett tredjeland i enlighet med ett internationellt avtal och

medlemsstaternas diplomatiska och konsulära beskickning i tredje länder undantagna från direktivets tillämpningsområde enligt samma skäl. Bestämmelserna är i denna del närmast identiska med de i NIS 2-direktivet.

Medlemsstaterna får enligt artikel 1.7 i CER-direktivet undanta särskilda kritiska entiteter som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet utredning, upptäckt och lagföring av brott, eller som uteslutande tillhandahåller tjänster till en offentlig förvaltningsentitet som avses i artikel 1.6 från vissa skyldigheter. Undantag får göras från bestämmelserna i artikel 11 och kapitlen III, IV och VI i direktivet, det vill säga de som avser samarbete mellan medlemsstaterna, kritiska entiteters motståndskraft och kritiska entiteter av särskild europeisk betydelse samt tillsyn och efterlevnadskontroll. I skäl 11 i direktivet anges med tanke på medlemsstaternas ansvar att skydda den nationella säkerheten och försvaret att medlemsstaterna bör kunna besluta att skyldigheterna för kritiska entiteter enligt direktivet helt eller delvis inte ska gälla dessa kritiska entiteter om de tjänster de tillhandahåller eller den verksamhet de bedriver till övervägande del har anknytning till områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet utredning, upptäckt och lagföring av brott. Kritiska entiteter vars tjänster eller verksamhet endast marginellt hänför sig till dessa områden bör, enligt samma skäl, fortfarande omfattas av direktivets tillämpningsområde.

Vad tar undantaget sikte på för verksamhet?

CER-direktivet är alltså inte tillämpligt på offentliga förvaltningsentiteter som bedriver verksamhet inom områdena nationell säkerhet, allmän säkerhet, försvar och brottsbekämpning, inbegripet utredning, upptäckt och lagföring av brott. Det utvecklas inte närmare i direktivet vad som avses med uttrycken. För att genomföra direktivet på korrekt sätt i nationell rätt krävs en tolkning av vad de avser för slags verksamhet i Sverige.

I förarbetena till cybersäkerhetslagen konstateras att uttrycket nationell säkerhet är ett vedertaget begrepp inom unionsrätten, men att det saknas en tydlig definition i densamma (se prop. 2025/26:28 s. 73 f.). I samma förarbeten konstaterar regeringen att uttrycket Sveriges säkerhet används i olika sammanhang. Innebörden av uttrycket har behandlats i flera lagstiftningsärenden de senaste åren, och uttrycket tar sikte på förhållanden av grundläggande betydelse för Sverige. Det kan handla om både militär och civil verksamhet, så länge verksamheten har en sådan betydelse. Uttrycket används exempelvis i 1 kap. 1 § säkerhetsskyddslagen, som gäller bland annat för den som till någon del bedriver verksamhet som är av betydelse för detta skyddsintresse. En slutsats av det anförda är att CER-direktivet bland annat inte är tillämpligt på säkerhetskänslig verksamhet.

Uttrycket allmän säkerhet i direktivet bör, i likhet med vad som anges i förarbetena till cybersäkerhetslagen, anses omfatta det som avses med uttrycket i EUF-fördraget. Allmän säkerhet gäller skydd av en medlemsstats institutioner, dess väsentliga offentliga tjänster och dess invånares överlevnad. Vilken verksamhet som uttrycket försvar avser i direktivet bör

enligt regeringen inte kräva någon närmare analys (se prop. 2025/26:28 s. 74).

CER-direktivet, i likhet med NIS 2-direktivet, är inte tillämpligt på offentliga förvaltningsentiteter som bedriver verksamhet inom området brottsbekämpning, inbegripet utredning, upptäckt och lagföring av brott. Utredningen angav i delbetänkandet att undantaget tar sikte på de myndigheter som betecknas som rättsvårdande myndigheter.

Med brottsbekämpande verksamhet avses, i bland annat lagen (2025:170) om skyldighet att lämna uppgifter till de brottsbekämpande myndigheterna, sådan verksamhet som en brottsbekämpande myndighet bedriver för att förebygga, förhindra eller upptäcka brottslig verksamhet eller för att utreda eller lagföra brott. Verksamhet för att verkställa straffrättsliga påföljder, upprätthålla allmän ordning och säkerhet och sådan kontrollverksamhet som brottsbekämpande myndigheter i vissa fall bedriver omfattas inte av uttrycket i lagen (se prop. 2024/25:65 s. 201).

I förarbetena till lagen om skyldighet att lämna uppgifter till de brottsbekämpande myndigheterna anges att det är underrättelseverksamhet som avses när formuleringen förebygga, förhindra eller upptäcka brottslig verksamhet används. Med att utreda brott avses vidare i lagen framför allt att genomföra förundersökning enligt 23 kap. rättegångsbalken. Med brott avses ett konkret brott. Med uttrycket lagföra brott avses i lagen framför allt åklagares beslut i åtalsfrågor och om åtalsunderlåtelser samt brottmålsförfaranden i allmän domstol. Enligt regeringens mening bör uttrycket brottsbekämpande verksamhet användas i den nya lagen och ha samma innebörd som i lagen om skyldighet att lämna uppgifter till de brottsbekämpande myndigheterna. Motsvarande bedömning gjordes vid genomförandet av NIS 2-direktivet (se prop. 2025/26:28 s. 74).

Undantag för statliga myndigheter som till övervägande del bedriver aktuell verksamhet

Flera remissinstanser, däribland *MCF*, *Säkerhetspolisen* och flertalet länsstyrelser, anser att undantag inte bör göras för säkerhetskänslig verksamhet och brottsbekämpande verksamhet. *Livsmedelsverket* förespråkar att samtliga verksamhetsutövare som bedriver säkerhetskänslig verksamhet ska omfattas av lagen med begränsningen som föreslås för kritiska verksamhetsutövare inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur (se avsnitt 5.4.1).

Enligt regeringens uppfattning, vilken överensstämmer med utredningens men inte med *Tullverkets*, bör de offentliga verksamhetsutövare som undantas helt från lagens tillämpningsområde vara de verksamhetsutövare som till övervägande del bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen eller brottsbekämpande verksamhet. Detta innebär, i linje med utredningens resonemang, att endast statliga myndigheter bör undantas i sin helhet från lagens tillämpningsområde. Regeringen anser inte att det är en lämplig ordning att, som utredningen föreslår, låta det framgå av förordning vilka statliga myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet. Eftersom undantaget i en del knyts till säkerhetsskyddslagens tillämpningsområde finns det inte skäl för att, trots vissa remissinstansers begäran om förtydliganden, resonera kring vilka myndigheter som kommer att anses omfattas av detsamma. Vilka

myndigheter som bedriver säkerhetskänslig verksamhet till övervägande del får bedömas i varje enskilt fall. Det finns inte heller skäl för att i en förordning ange vilka myndigheter som till övervägande del bedriver brottsbekämpande verksamhet. Det bör därmed inte införas något sådant bemyndigande för regeringen som utredningen föreslår i denna del. Polismyndigheten är dock exempelvis en myndighet som till övervägande del bedriver brottsbekämpande verksamhet.

Lagrådet lyfter att det i författningskommentaren anges att uttrycket övervägande del avser att myndighetens huvudsakliga verksamhet rör säkerhetskänslig verksamhet eller utgör brottsbekämpning. Lagrådet anger att uttrycken till övervägande del och huvudsakliga verksamhet knappast är synonymer och att det finns ett behov av ett klarläggande av vad som avses med uttrycket till övervägande del. Enligt Svensk ordbok avser den övervägande delen dock den huvudsakliga delen av något och de aktuella uttryckssätten är därmed just synonyma. Motsvarande skrivning finns också i författningskommentaren till cybersäkerhetslagen. Regeringen finner därför inte skäl att göra någon ändring i förhållande till lagrådsremissens förslag i denna del.

Tullverket anser att direktivet inte kräver att någon av de uppräknade verksamheterna, endast sedd för sig, bedrivs till övervägande del för att undantaget ska vara tillåtet. Tullverket anser att det är tydligt att undantaget bör tillämpas på myndigheter som till övervägande del ägnar sig åt verksamhet på de uppräknade områdena även sett tillsammans. Om en verksamhetsutövare till någon mindre del, än till övervägande del, bedriver säkerhetskänslig verksamhet eller brottsbekämpande verksamhet föreslås att den nya lagen i begränsad omfattning ska gälla för den delen av verksamheten. Regeringen bedömer att detta är en ändamålsenlig lösning och att det inte bör göras en sådan helhetsbedömning som Tullverket nämner.

Regeringen konstaterar att frågan om att tillsätta en sådan utredning som Säkerhetspolisen föreslår ligger utanför sådant som kan behandlas inom ramen för denna proposition.

I vissa fall bör endast en del av verksamheten vara undantagen

I likhet med utredningen anser regeringen att en särreglering bör gälla för offentliga verksamhetsutövare som bedriver säkerhetskänslig verksamhet eller brottsbekämpande verksamhet men inte till övervägande del. En sådan ordning gäller även enligt 1 kap. 12 § cybersäkerhetslagen. Undantag görs enligt den lagen i förhållande till den säkerhetskänsliga delen av verksamheten och den del av verksamheten som avser brottsbekämpning.

Utredningen föreslår att undantaget i den nya lagen bör utformas på ett sådant sätt att undantaget endast avser den del av den samhällsviktiga tjänsten som utgör brottsbekämpning eller är säkerhetskänslig. Regeringen anser att undantaget bör utformas på motsvarande sätt som i cybersäkerhetslagen och därmed relateras till verksamheten i stället för tjänsten. Även om CER-direktivet handlar om att säkerställa tillhandahållandet av samhällsviktiga tjänster, fastställs i direktivet en skyldighet att identifiera kritiska verksamhetsutövare som tillhandahåller sådana tjänster och att vidta åtgärder för att deras motståndskraft ska stärkas. Det är enligt

regeringens mening därför rimligt att i utformningen av lagen förhålla sig till den verksamhet som tillhandahåller tjänsterna.

För en offentlig verksamhetsutövare som bedriver säkerhetskänslig verksamhet eller brottsbekämpande verksamhet men inte till övervägande del bör alltså, i enlighet med artikel 1.7 i CER-direktivet, den säkerhetskänsliga delen av verksamheten och verksamheten som avser brottsbekämpning undantas från kraven i den nya lagen. För den delen av verksamheten bör inte skyldigheterna enligt lagen att göra en anmälan, göra en riskbedömning och vidta åtgärder för motståndskraft, inbegripet att göra en befattningsanalys och genomföra bakgrundskontroller, samt genomföra incidentrapportering gälla.

Undantag för enskilda verksamhetsutövare

För enskilda verksamhetsutövare som till någon del bedriver säkerhetskänslig verksamhet ska, enligt utredningens förslag, skyldigheterna enligt lagen inte gälla för den del av den samhällsviktiga tjänsten som är säkerhetskänslig. Om det finns delar av den samhällsviktiga tjänsten som inte är säkerhetskänslig ska, enligt utredningen, kraven i lagen tillämpas fullt ut i förhållande till dessa delar. Utredningen föreslår därmed ett undantag som även i denna del är relaterat till den samhällsviktiga tjänsten och inte till verksamheten i stort.

Utredningen föreslår inte något särskilt undantag för verksamhetsutövare som enbart eller till någon del erbjuder tjänster till en sådan statlig myndighet som till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpande verksamhet. Ett sådant undantag föreslogs i delbetänkandet kopplat till genomförandet av artikel 2.8 i NIS 2-direktivet.

Av artikel 2.8 i NIS 2-direktivet framgår att medlemsstaterna får undanta särskilda entiteter som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott, eller som tillhandahåller tjänster uteslutande till en offentlig förvaltningsentitet som avses i artikel 2.7, från skyldigheterna i artiklarna 21 eller 23 med avseende på sådan verksamhet eller sådana tjänster. I sådana fall ska de tillsyns- och efterlevnadskontrollåtgärder som avses i kapitel VII i NIS 2-direktivet inte tillämpas på denna specifika verksamhet eller dessa specifika tjänster. Om entiteterna bedriver verksamhet eller tillhandahåller tjänster uteslutande av den typ som avses i artikel 2.8, får medlemsstaterna besluta att befria dessa entiteter också från skyldigheterna i artiklarna 3 och 27.

Artikel 2.8 i NIS 2-direktivet genomfördes i svensk nationell rätt genom 1 kap. 12 § cybersäkerhetslagen. Undantaget i artikel 1.7 i CER-direktivet är på samma sätt som i artikel 2.8 i NIS 2-direktivet relaterat till verksamheten och inte till tjänsten. Regeringen anser därmed, till skillnad från utredningen, att undantaget även i denna del bör relateras till verksamheten i stället för tjänsten. Regeringen bedömer vidare inte att skillnaderna mellan regleringen i artikel 1.7 i CER-direktivet och regleringen i artikel 2.8 i NIS 2-direktivet i någon del är sådana att det är motiverat att genomföra direktiven på olika sätt. Det är av värde att NIS 2- och CER-direktiven genomförs på ett samordnat sätt och det finns skäl att utforma

undantaget i den nya lagen i linje med motsvarande undantag i cybersäkerhetslagen.

Utformningen av undantaget i denna del bör mot denna bakgrund innebära att enskilda verksamhetsutövare som enbart bedriver säkerhetskänslig verksamhet inte omfattas av skyldigheterna enligt lagen. Detsamma bör gälla för en enskild verksamhetsutövare som enbart erbjuder tjänster till en statlig myndighet som är helt undantagen från lagens tillämpningsområde med hänvisning till att den bedriver säkerhetskänslig verksamhet eller brottsbekämpande verksamhet. Av samma skäl bör för övriga enskilda verksamhetsutövare som bedriver säkerhetskänslig verksamhet eller erbjuder tjänster till en statlig myndighet som är undantagen från lagens tillämpningsområde, men i annan utsträckning än vad som nämns ovan, skyldigheterna enligt den nya lagen inte gälla för den säkerhetskänsliga delen av verksamheten eller den del av verksamheten som erbjuder tjänsterna. För den delen av verksamheten som inte är säkerhetskänslig eller tillhandahåller tjänsterna bör lagen gälla i sin helhet.

Underrättelse om säkerhetskänslig verksamhet

Utredningen föreslår att det enligt den nya lagen ska finnas en skyldighet för tillsynsmyndigheten att, i de fall verksamhetsutövaren anger att den samhällsviktiga tjänsten till någon del är säkerhetskänslig, underrätta berörd tillsynsmyndighet enligt säkerhetsskyddslagen. Kopplat till detta föreslås en skyldighet för berörd tillsynsmyndighet enligt säkerhetsskyddslagen att, inom viss tid från att ha mottagit underrättelsen, meddela om verksamhetsutövaren har anmält att den bedriver säkerhetskänslig verksamhet. En sådan skyldighet föreslås införas genom en ny bestämmelse i säkerhetsskyddslagen. Bakgrunden till förslaget är att en verksamhetsutövare inte ska kunna undvika tillsyn genom att ange att en viss samhällsviktig tjänst är säkerhetskänslig trots att den inte är det, och på så sätt kringgå tillsyn enligt regelverken. Vissa remissinstanser motsätter sig att förslaget genomförs. Föreslagna uppgiftsskyldigheter behöver under alla förhållanden, som *Affärsverket svenska kraftnät* anger, inte regleras i lag. Utredningens förslag i denna del bör redan av detta skäl inte genomföras.

5.4.4 Undantag för säkerhetsskyddsklassificerade uppgifter

Regeringens förslag

Skyldigheterna att lämna uppgifter enligt lagen ska inte gälla uppgifter som är säkerhetsskyddsklassificerade enligt säkerhetsskyddslagen.

Regeringens bedömning

Det behöver inte införas någon ytterligare reglering för att undanta sådana delar av områden, lokaler eller andra utrymmen där säkerhetskänslig verksamhet bedrivs från tillsynsmyndighetens befogenheter.

Utredningens förslag

Förslaget från utredningen stämmer delvis överens med regeringens. Utredningen föreslår att det ska anges särskilt i lagen att tillsynsmyndighetens undersökningsbefogenheter inte omfattar sådana delar av områden, lokaler eller andra utrymmen där säkerhetskänslig verksamhet bedrivs.

Remissinstanserna

Flera remissinstanser, bland andra *Försvarets radioanstalt*, tillstyrker förslaget om att skyldigheten att lämna uppgifter enligt lagen inte ska gälla uppgifter som är säkerhetsskyddsklassificerade. Några remissinstanser, exempelvis *Strålsäkerhetsmyndigheten*, bedömer att undantaget kommer att medföra en risk för gränsdragningsproblem. *Transportstyrelsen* bedömer att förslaget innebär att tillsynen enligt lagen kan försvåras. Enligt Transportstyrelsen skulle en verksamhetsutövare som omfattas av säkerhetsskyddslagen bland annat kunna använda säkerhetsskyddsklassificeringen som en förevändning för att inte lämna ut en uppgift till tillsynsmyndigheten.

Några remissinstanser, däribland *Försvarsmakten* och *Länsstyrelsen i Skåne län*, tillstyrker förslaget om att från tillsynsmyndighetens undersökningsbefogenheter undanta sådana delar av områden, lokaler eller andra utrymmen där säkerhetskänslig verksamhet bedrivs. Transportstyrelsen anser dock att tillsynsmyndigheten borde få tillträde till de lokaler och andra utrymmen som krävs för att myndigheten ska kunna utföra sitt uppdrag, även om det där bedrivs säkerhetskänslig verksamhet, eftersom en annan ordning försvårar tillsynen över verksamheten.

Skälen för regeringens förslag och bedömning

Ett undantag för säkerhetsskyddsklassificerade uppgifter

Av artikel 1.8 i CER-direktivet följer att skyldigheterna som fastställs i direktivet inte får medföra tillhandahållande av information vars utlämnande skulle strida mot väsentliga intressen i fråga om medlemsstaternas nationella säkerhet, allmänna säkerhet eller försvar. Av skäl 11 i direktivet framgår att ingen medlemsstat bör vara skyldig att lämna information vars avslöjande skulle strida mot dess väsentliga intressen i fråga om nationell säkerhet. I detta sammanhang är unionsregler eller nationella regler till skydd för säkerhetsskyddsklassificerade uppgifter och sekretessavtal relevanta.

Med säkerhetsskyddsklassificerade uppgifter avses i 1 kap. 2 § andra stycket säkerhetsskyddslagen uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) (OSL) eller som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig. I bland annat avsnitt 8 föreslås att kritiska verksamhetsutövare ska vara skyldiga att lämna ut uppgifter med stöd av den nya lagen. För att säkerställa att säkerhetsskyddsklassificerade uppgifter inte lämnas ut med stöd av den nya lagen är det inte tillräckligt att vissa verksamhetsutövare som bedriver säkerhetskänslig verksamhet undantas från lagens tillämpningsområde. Det bör därför, som utredningen föreslår, införas ett undantag som innebär

att skyldigheten att lämna ut uppgifter inte gäller uppgifter som är säkerhetsskyddsklassificerade enligt säkerhetsskyddslagen. Regeringen delar inte *Transportstyrelsens* uppfattning att tillsynen kan komma att försvåras med ett sådant undantag. Det finns effektiva ingripandemöjligheter vid bristande uppfyllelse av skyldigheterna enligt lagen (se vidare avsnitt 11). Det är inte heller ett alternativ att avstå från att införa ett undantag kopplat till säkerhetsskyddsklassificerade uppgifter. En sådan ordning skulle innebära en risk för att uppgifter röjs på ett sätt som kan medföra skada för Sveriges säkerhet. En likalydande bestämmelse finns dessutom i 1 kap. 13 § cybersäkerhetslagen.

Några remissinstanser bedömer att undantaget kommer att medföra en risk för gränsdragningsproblem. Undantaget knyter an till säkerhetsskyddslagens tillämpningsområde och regeringen kan inte se att det skulle vara otydligt vilka uppgifter som avses eller i vilka situationer som undantaget aktualiseras. Vilka uppgifter som är säkerhetsskyddsklassificerade och omfattas av undantaget får bedömas i varje enskilt fall.

Tillträdesrätt till lokaler och andra utrymmen där säkerhetskänslig verksamhet bedrivs

Av artikel 1.5 i CER-direktivet framgår att direktivet inte påverkar medlemsstaternas ansvar att skydda den nationella säkerheten och försvaret eller deras befogenhet att skydda andra väsentliga statliga funktioner, inbegripet att säkerställa statens territoriella integritet och upprätthålla lag och ordning.

När det gäller bestämmelserna om så kallade rådgivande uppdrag anges i artikel 18.8 att rådgivande uppdrag ska genomföras i enlighet med tillämplig nationell rätt i den medlemsstat där de äger rum, med respekt för den medlemsstatens ansvar för den nationella säkerheten och skyddet av sina säkerhetsintressen (se vidare avsnitt 7.2).

Enligt artikel 21.1 a ska medlemsstaterna, för att bedöma om de entiteter som medlemsstaterna har identifierat som kritiska entiteter enligt artikel 6.1 fullgör de skyldigheter som fastställs i CER-direktivet, säkerställa att de behöriga myndigheterna har befogenheter och medel för att genomföra inspektioner på plats av den kritiska infrastruktur och de lokaler som den kritiska entiteten använder för att tillhandahålla sina samhällsviktiga tjänster och tillsyn på distans av de åtgärder som vidtagits av kritiska entiteter i enlighet med artikel 13. Tillsynsmyndighetens befogenheter behandlas i avsnitt 10.

Utredningen föreslår att det ska införas en bestämmelse i lagen som begränsar undersökningsbefogenheterna avseende sådana områden, lokaler och andra utrymmen där säkerhetskänslig verksamhet bedrivs. Begränsningen ska enligt utredningen inte uppfattas som att den träffar alla sådana utrymmen där säkerhetsskyddsåtgärder har vidtagits, utan endast sådana platser där den säkerhetskänsliga verksamheten bedrivs och platser i direkt anslutning till sådana platser där den säkerhetskänsliga verksamheten bedrivs. Begränsningen i tillträdesrätten föreslås utformas som att tillsynsmyndighetens undersökningsbefogenheter inte omfattar sådana delar av områden, lokaler och andra utrymmen där säkerhetskänslig verksamhet enligt säkerhetsskyddslagen bedrivs.

Regeringen bedömer att CER-direktivet inte bör vara tillämpligt på säkerhetskänslig verksamhet (se avsnitt 5.4.3). Undantaget för säkerhetskänslig verksamhet innebär att inte heller tillsyn enligt lagen kan ske i förhållande till sådan verksamhet. Regeringen anser därför, till skillnad från utredningen och bland annat *Försvarsmakten*, att det inte finns något behov av att i lagen införa en bestämmelse som begränsar tillsynsmyndighetens undersökningsbefogenheter i förhållande till sådana områden, lokaler och andra utrymmen där säkerhetskänslig verksamhet bedrivs.

6 Identifiering av kritiska verksamhetsutövare utifrån bland annat en nationell riskbedömning

6.1 Den myndighet som regeringen pekar ut bör genomföra riskbedömningen

Regeringens förslag

Det ska införas en upplysningsbestämmelse i lagen om att den myndighet som regeringen bestämmer ska genomföra en nationell riskbedömning enligt artikel 5 i CER-direktivet.

Utredningens förslag

Förslaget från utredningen stämmer delvis överens med regeringens. Utredningen föreslår att den nationella riskbedömningens innehåll och genomförande ska regleras i lagen.

Remissinstanserna

En majoritet av remissinstanserna tillstyrker eller har inga synpunkter på förslaget. Bland andra *Finansinspektionen* och *Livsmedelsverket* yttrar sig gällande den nationella riskbedömningens innehåll och syfte. Vissa remissinstanser, till exempel *Myndigheten för psykologiskt försvar* och *Sveriges metereologiska och hydrologiska institut*, för fram synpunkter kring den nationella riskbedömningens förhållande till liknande bedömningar som redan görs. Ett par remissinstanser, exempelvis *Affärsverket svenska kraftnät*, har synpunkter kopplade till informationshanteringen som sker i anledning av den nationella riskbedömningen. *Post- och telestyrelsen (PTS)* anser att det inte är helt klart hur uttrycket alla relevanta risker i den av utredningen föreslagna bestämmelsen om riskbedömningens innehåll ska tolkas. Några remissinstanser yttrar sig i frågan om vilka aktörer som ska delges den nationella riskbedömningen i enlighet med utredningens förslag till förordning.

Skälen för regeringens förslag

Enligt artikel 5.1 i CER-direktivet skulle de behöriga myndigheterna senast den 17 januari 2026 göra en riskbedömning och därefter när så är nödvändigt och minst vart fjärde år. Riskbedömningen ska sedan användas av de behöriga myndigheterna vid identifiering av kritiska entiteter, samt för att bistå de kritiska entiteterna med att vidta åtgärder för motståndskraft (se avsnitt 8.2). Riskbedömningen ska enligt samma artikel innehålla en redogörelse för relevanta risker för naturolyckor och risker orsakade av människan, inbegripet risker av sektorsövergripande eller gränsöverskridande slag, olyckor, naturkatastrofer, hot mot folkhälsan och hybridhot eller andra antagonistiska hot, inklusive terroristbrott enligt Europaparlamentets och rådets direktiv (EU) 2017/541 av den 15 mars 2017 om bekämpande av terrorism, om ersättande av rådets rambeslut 2002/475/RIF och om ändring av rådets beslut 2005/671/RIF (terrorismdirektivet). Utöver detta framgår det av artikel 5.2 i CER-direktivet vad medlemsstaterna åtminstone ska ta hänsyn till när de gör riskbedömningarna.

Uttrycket risk definieras i artikel 2.6 i CER-direktivet som risk för förlust eller störning orsakad av en incident, som ska uttryckas som en kombination av omfattningen av förlusten eller störningen och sannolikheten för att incidenten inträffar. Med riskbedömning avses enligt artikel 2.7 i direktivet den övergripande processen för att fastställa arten och omfattningen av en risk genom att identifiera och analysera potentiella relevanta hot, sårbarheter och faror som skulle kunna leda till en incident och genom att utvärdera den potentiella förlusten eller störningen i samband med tillhandahållandet av en samhällsviktig tjänst till följd av den incidenten.

Utredningens förslag innebär att det i den nya lagen regleras vad riskbedömningen åtminstone ska innehålla, vad som ska beaktas vid framtagandet samt hur ofta den ska uppdateras. Utredningen föreslår också en skyldighet för tillsynsmyndigheterna och kritiska verksamhetsutövare som står under tillsyn att tillhandahålla viss information som underlag till riskbedömningen. Regeringen konstaterar att utredningens förslag i denna del i allt väsentligt överensstämmer med regleringen i artikel 5.2 c och d i CER-direktivet. Utredningen har inte motiverat varför riskbedömningens innehåll bör regleras i lag. Utöver detta föreslår utredningen att utpekandet av den myndighet som ska genomföra den nationella riskbedömningen ska ske i förordning. Utredningen föreslår också att reglering av till vilka riskbedömningen ska delges och om lämnande av information till EU-kommissionen ska införas på förordningsnivå.

Med hänsyn till att den nationella riskbedömningen ska beaktas vid identifieringen av de kritiska verksamhetsutövarna och vid de kritiska verksamhetsutövarnas riskbedömningar bör den nationella riskbedömningen i viss mån regleras i den nya lagen. Regeringen uttryckte i lagrådsremissen att det i lagen bör finnas en bestämmelse som upplyser om att den myndighet som regeringen bestämmer ska genomföra en nationell riskbedömning enligt artikel 5 i CER-direktivet.

Lagrådet ifrågasätter att det rör sig om endast en upplysningsbestämmelse och gör det även i förhållande till motsvarande slags förslag i avsnitt 13.1 som handlar om utpekandet av en gemensam kontaktpunkt

enligt artikel 9 i direktivet. Som lagtexten är utformad föreligger det åtminstone, enligt Lagrådet, den bundenheten att den myndighet som regeringen bestämmer ska vara både kontaktpunkt och göra en nationell riskbedömning. Eftersom det rör sig om två olika väsensskilda uppdrag bör paragrafen också enligt Lagrådet delas upp i två stycken. Regeringen konstaterar att liknande reglering finns i 1 kap. 17 § cybersäkerhetslagen, och att den aktuella paragrafen inte innehåller någon materiell reglering. I stället rör det sig om en upplysning om regeringens möjlighet att utse en myndighet som ska vara gemensam kontaktpunkt respektive göra en nationell riskbedömning. Det finns inget som hindrar att regeringen utser olika myndigheter för de olika funktioner som nämns i paragrafen. Någon ändring behöver därmed inte göras utifrån Lagrådets synpunkter i denna del.

Regeringen anser, av bland annat flexibilitetsskäl, att den övriga regleringen om riskbedömningens innehåll och genomförande samt om skyldighet att dela riskbedömningen lämpligen bör regleras på annan författningsnivå än lag. Bestämmelser i detta avseende kan meddelas av regeringen med stöd av 8 kap. 7 § regeringsformen. Med hänvisning till bedömningen om att lagreglering inte krävs respektive inte är lämplig saknas det anledning att behandla remissinstansernas synpunkter i denna proposition.

Utredningen föreslår att uttrycken risk och riskbedömning ska definieras i lagen. Denna fråga behandlas i avsnitt 8.1.

6.2 Uttrycket samhällsviktig tjänst bör definieras i lagen och styra vilka som kan identifieras

Regeringens förslag

Uttrycket samhällsviktig tjänst ska i lagen avse en tjänst som är avgörande för upprätthållandet av centrala samhällsfunktioner, ekonomisk verksamhet, folkhälsa, allmän säkerhet eller för skyddet av miljön och som omfattas av bilagan till CER-direktivet.

Utredningens förslag

Förslaget från utredningen stämmer i huvudsak överens med regeringens. Utredningen föreslår inte att det i lagen ska anges att den samhällsviktiga tjänsten ska omfattas av bilagan till CER-direktivet. Utredningen föreslår att uttrycket viktiga samhällsfunktioner ska användas i stället för centrala samhällsfunktioner.

Remissinstanserna

Majoriteten av remissinstanserna är positiva till eller har inte några synpunkter på förslaget.

Många remissinstanser, däribland *Försvarsmakten, Myndigheten för civilt försvar (MCF), Naturvårdsverket, Svenskt Näringsliv, Tech Sverige* och ett flertal länsstyrelser, anser att den föreslagna regleringen bör

kopplas till det svenska beredskapssystemet eller att en sådan koppling bör utredas. MCF anser att den nya lagen bör omfatta all samhällsviktig verksamhet och att det är av stor vikt att regleringen utgår från befintlig systematik. MCF anser också att uttryck som används inom den svenska krisberedskapen och det civila försvaret bör användas i lagen. MCF anser vidare att den föreslagna lagen inte bör hänvisa till direktivets bilaga för att definiera de sektorer som ska omfattas av lagen.

Innovations- och kemiindustrierna i Sverige (IKEM) välkomnar den tydliga uppställningen av sektorer och kategorier av kritiska verksamhetsutövare som finns i bilagan till direktivet. Eventuell utvidgning av sektorer bör enligt IKEM göras på ett samordnat sätt i hela EU. *Post- och telestyrelsen (PTS)* anser att det svenska beredskapssystemet inte bör kopplas till den reglering som genomför CER-direktivet eftersom direktivet avser att reglera den inre marknaden. PTS för fram att beredskapsfrågor ligger nära frågor om nationell säkerhet, vilket tillhör medlemsstaternas nationella regleringskompetens. Därför är det enligt PTS positivt att det i den föreslagna lagen görs en åtskillnad mellan uttrycken samhällsviktig tjänst och samhällsviktig verksamhet.

Bland andra *Bolagsverket, Malmö kommun*, *Myndigheten för psykologiskt försvar (MPF)* och Naturvårdsverket resonerar om skillnaderna mellan uttrycken samhällsviktig tjänst och samhällsviktig verksamhet, lyfter fram behovet av att ensa begreppsanvändningen i olika regelverk samt anser att uttrycket samhällsviktig verksamhet bör användas i lagen. Försvarsmakten anser att det är av vikt att tillsynsmyndigheterna vid behov samråder med sektorsansvariga myndigheter enligt förordningen om statliga myndigheters beredskap. *Trafikverket* delar utredningens uppfattning att det finns ett stort värde av att i framtiden se över CER-direktivets koppling till det svenska beredskapssystemet och för fram att det finns ett behov av att harmonisera uttryck, verktyg och arbetssätt för identifiering, incidentrapportering, ingripanden och sanktioner samt sekretess.

Energiföretagen Sverige framhåller att CER-direktivet anger att de delar av kärnkraftsproduktion som inkluderar överföring av el kan omfattas, medan andra delar som rör kärnteknisk verksamhet kan undantas om det bedöms lämpligt. Energiföretagen Sverige anser att den föreslagna lagen endast bör tillämpas på de delar av kärnkraftverk som inte omfattas av lagen (1984:3) om kärnteknisk verksamhet, såsom elöverföring. Energiföretagen Sverige föreslår att detta klargörs i lagförslaget.

Finansiell ID-Teknik BID AB (BID) för fram att minst en utpekad myndighet bör få befogenhet att identifiera verksamhetsutövare som kritiska även utanför sektorerna som anges i direktivets bilaga.

Finansinspektionen bedömer att det finns anledning att beakta fler samhällsviktiga tjänster inom banksektorn än de som anges i CER-direktivets bilaga och i kompletteringsförordningen.

Skälen för regeringens förslag

Regleringen i direktivet

Enligt artikel 2.1 i CER-direktivet är en kritisk entitet en offentlig eller privat entitet som har identifierats av en medlemsstat i enlighet med artikel 6 som tillhörande en av de kategorier som anges i den tredje

kolumnen i tabellen i bilagan till direktivet. Av artikel 6.1 i CER-direktivet framgår att medlemsstaterna senast den 17 juli 2026 ska identifiera de kritiska entiteterna för de sektorer och undersektorer som anges i direktivets bilaga. När en medlemsstat identifierar kritiska entiteter ska den, enligt artikel 6.2 i direktivet, bland annat beakta om entiteten tillhandahåller en eller flera samhällsviktiga tjänster.

Samhällsviktig tjänst definieras i artikel 2.5 i CER-direktivet som en tjänst som är avgörande för att upprätthålla viktiga samhällsfunktioner, ekonomisk verksamhet, folkhälsa och allmän säkerhet, eller miljön. Bilagan till CER-direktivet innehåller 11 sektorer och ett antal undersektorer (se vidare avsnitt 4.2). Kopplat till dessa sektorer och undersektorer anges i sin tur ett antal kategorier av entiteter. EU-kommissionen har i kompletteringsförordningen fastställt en icke uttömmande förteckning över samhällsviktiga tjänster, enligt definitionen i artikel 2.5 i CER-direktivet, i de sektorer och undersektorer som anges i bilagan till direktivet.

Tjänsten bör omfattas av direktivets bilaga för att räknas som samhällsviktig

Ett antal remissinstanser, däribland *MCF*, argumenterar för att den föreslagna regleringen ska kopplas till det svenska beredskapssystemet och att den nya lagen ska omfatta samhällsviktig verksamhet i den bemärkelse som avses i förordningen om statliga myndigheters beredskap i stället för samhällsviktig tjänst enligt direktivet. Som utvecklas i avsnitt 5.1 finns det inte utrymme för att inom ramen för detta lagstiftningsärende göra de förändringar som remissinstanserna efterfrågar men en översyn bör ske på sikt. Denna slutsats innebär bland annat att regeringen, till skillnad mot till exempel *MPF*, bedömer att samhällsviktig tjänst bör användas som uttryck i lagen i stället för samhällsviktig verksamhet.

Utredningens förslag innebär att uttrycket samhällsviktig tjänst definieras i lagen i enlighet med vad som anges i direktivet. Utredningen bedömer att det som utgångspunkt endast är sådana samhällsviktiga tjänster som träffas av definitionen i artikel 2.5 och som ingår i någon av sektorerna eller undersektorerna i bilagan till CER-direktivet som ska anses omfattas av uttrycket samhällsviktig tjänst i lagen. Utredningens förslag till definition av uttrycket innehåller dock inte något krav på att en samhällsviktig tjänst ska omfattas av bilagan till direktivet.

Definitionen av samhällsviktig tjänst i CER-direktivet innehåller inte heller något krav på att den samhällsviktiga tjänsten ska omfattas av direktivets bilaga. Regeringen konstaterar dock att uttrycket samhällsviktig tjänst i kombination med de sektorer och undersektorer som framgår av bilagan till CER-direktivet är centrala vid bedömningen av vilka krav som direktivet innebär och vilken slags verksamhet direktivet träffar. Kombinationen innebär en avgränsning till vissa typer av verksamheter. Bilagans tredje kolumn pekar i sin tur ut kategorier av entiteter, vilket begränsar kretsen av entiteter som omfattas av direktivets krav. Ett av direktivets syften är enligt skäl 16 att åstadkomma en harmonisering när det gäller de entiteter som omfattas av dess tillämpningsområde. En sådan harmonisering kan enligt regeringens mening åstadkommas om de samhällsviktiga tjänsterna som omfattas av de nationella regleringarna

även ryms inom direktivets bilaga. Kompletteringsförordningens förteckning, som ska användas vid bedömningen av om en tjänst är samhällsviktig, avser vidare samhällsviktiga tjänster i de sektorer och undersektorer som anges i bilagan till CER-direktivet. Regeringen instämmer därför i utredningens uppfattning att det bör krävas att en tjänst omfattas av bilagan till CER-direktivet för att den ska räknas som samhällsviktig. Detta bör framgå av definitionen av uttrycket i lagen. Det bör inte göras något tillägg eller förtydligande i förhållande till direktivets innehåll som till exempel *Energiföretagen Sverige* efterfrågar.

Frågan blir då om alla delar av bilagan till CER-direktivet är relevanta vid bedömningen av om en tjänst är samhällsviktig. Bilagans tredje kolumn, som avser kategorier av entiteter, bör vid en tolkning av artiklarna 2.1 och 6.1, vara avsedd att användas som identifieringskriterium avseende verksamhetsutövarna som sådana. Kompletteringsförordningen hänvisar till sektorer och undersektorer som anges i bilagan till CER-direktivet och inte till den tredje kolumnen i tabellen i bilagan. Detta, tillsammans med tolkningen av artiklarna 2.1 och 6.1, innebär enligt regeringen att de samhällsviktiga tjänsterna som omfattas av lagens tillämpningsområde bör ingå i direktivets sektorer och undersektorer (se även skäl 3 i kompletteringsförordningen). Med hänsyn till att den tredje kolumnen tydligt pekar ut typer av aktörer och inte kategorier av tjänster anser regeringen att denna distinktion inte behöver framgå av lagen.

Definitionen av uttrycket samhällsviktig tjänst i övrigt

Samhällsviktig tjänst definieras i artikel 2.5 i CER-direktivet som en tjänst som är avgörande för att upprätthålla viktiga samhällsfunktioner, ekonomisk verksamhet, folkhälsa och allmän säkerhet, eller miljön. Utredningens förslag innebär att definitionen av samhällsviktig tjänst i lagen är densamma som i direktivet i dessa delar. Varken CER-direktivet eller utredningens förslag innehåller några resonemang om innebörden av definitionens beståndsdelar.

För att genomföra direktivet på korrekt sätt i nationell rätt krävs en viss tolkning av vad samhällsviktig tjänst avser för slags verksamhet och vad innebörden av definitionens beståndsdelar är. Innebörden av definitionens beståndsdelar begränsas dock av och bör tolkas i ljuset av utformningen av bilagan till CER-direktivet eftersom tjänsten, enligt regeringens bedömning ovan, bör omfattas av bilagan för att räknas som en samhällsviktig tjänst. Vidare gör regeringen i avsnitt 6.3 bedömningen att verksamhetsutövaren bör omfattas av någon av kategorierna i bilagan till CER-direktivet för att kunna identifieras som kritisk. Samtliga tjänster som är avgörande för att upprätthålla viktiga samhällsfunktioner, ekonomisk verksamhet, folkhälsa och allmän säkerhet, eller miljön kommer därmed inte att räknas som samhällsviktiga tjänster enligt lagen.

När det kommer till de områden som tjänsterna ska vara avgörande för att upprätthålla för att kunna anses vara samhällsviktiga gör regeringen följande överväganden. Uttrycket viktiga samhällsfunktioner som används i den svenska språkversionen av CER-direktivet definieras inte i direktivet. I EU:s strategi för en beredskapsunion (JOIN [2025] 130 FINAL) används det närliggande uttrycket centrala samhällsfunktioner, vilka enligt strategin utgörs av grundläggande system och strukturer som gör det

möjligt för ett samhälle att fungera, samtidigt som de skyddar våra samhällen, ekonomier, kulturer och demokratiska institutioner i alla situationer. Dessa funktioner omfattar enligt strategin först och främst säkerheten för EU:s befolkning, inklusive skydd mot naturkatastrofer, myndigheters verksamhetskontinuitet och beslutsfattande, demokratiska processer, social sammanhållning och ekonomisk stabilitet samt inre och yttre säkerhet.

I den engelska språkversionen av strategin motsvaras uttrycket centrala samhällsfunktioner av uttrycket vital societal functions, vilket är samma uttryck som används i den engelska språkversionen av CER-direktivet och som i den svenska versionen alltså har översatts till viktiga samhällsfunktioner. Även i de franska och italienska språkversionerna av direktivet och strategin används uttryck motsvarande centrala samhällsfunktioner. Enligt regeringen talar detta för att det är samma innebörd som eftersträvas i CER-direktivet och strategin. Därmed bör samma uttryck användas i lagen som i strategin, nämligen centrala samhällsfunktioner, och innebörden bör i stort anses vara densamma som i strategin. I svensk kontext bör uttrycket i många fall kunna avse sådana verksamheter som MCF har identifierat i myndighetens lista över viktiga samhällsfunktioner (se Lista med viktiga samhällsfunktioner – Utgångspunkt för att stärka samhällets beredskap, MSB1844, och jfr även Lista med de viktigaste samhällsfunktionerna, MCF0018).

När det gäller uttrycket ekonomisk verksamhet bör ledning kunna tas från hur uttrycket används i förhållande till EU-regleringen om statsstöd. Uttrycket bör därför omfatta all verksamhet som går ut på att erbjuda varor och tjänster på en marknad (se Kommissionens tillkännagivande om begreppet statligt stöd som avses i artikel 107.1 i fördraget om Europeiska unionens funktionssätt [2016/C 262/01] och däri angiven praxis).

Gällande uttrycket folkhälsa bör ledning kunna tas från artikel 168 i EUF-fördraget. Uttrycket bör därför omfatta skyddet och främjandet av människors fysiska och psykiska hälsa, samt förebyggande av sjukdomar och undanröjande av hälsorisker. Uttrycket allmän säkerhet bör enligt regeringen anses ta sikte på det som avses med uttrycket i EUF-fördraget. Allmän säkerhet bör därmed gälla skydd av en medlemsstats institutioner, dess väsentliga offentliga tjänster och dess invånares överlevnad.

När det gäller uttrycket miljön bör ledning i tolkningen av det avsedda skyddsområdet kunna tas från definitionen av miljöskada i artikel 2.1 i Europaparlamentets och rådets direktiv 2004/35/EG av den 21 april 2004 om miljöansvar för att förebygga och avhjälpa miljöskador.

I fråga om när en tjänst som sådan ska anses vara avgörande för att upprätthålla angivna funktioner och verksamhet bör viss ledning kunna tas från definitionen av uttrycket samhällsviktig tjänst i den upphävda lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen) samt från förarbetena till cybersäkerhetslagen. I förarbetena till NIS-lagen framgår att det rör sig om tjänster som är viktiga för samhällets funktionalitet i sin helhet och där ett avbrott i tjänsten hindrar genomförandet av ekonomisk verksamhet, genererar omfattande förluster, undergräver användarnas förtroenden och medför allvarliga konsekvenser för landets och unionens ekonomi (se prop. 2017/18:205 s. 33 f. och jfr även prop. 2025/26:28 s. 54).

6.3 Krav för att identifieras som kritisk verksamhetsutövare

Regeringens förslag

För att identifieras som kritisk verksamhetsutövare ska det krävas att

1. verksamhetsutövaren tillhandahåller en eller flera samhällsviktiga tjänster,
2. verksamhetsutövaren omfattas av någon av kategorierna i bilagan till CER-direktivet eller är en statlig myndighet som regeringen i övrigt bestämmer ska kunna omfattas av lagen,
3. verksamhetsutövaren bedriver verksamhet i och har kritisk infrastruktur belägen i Sverige, och
4. en incident skulle få en betydande störande effekt för verksamhetsutövarens tillhandahållande av en eller flera samhällsviktiga tjänster, eller tillhandahållandet av andra samhällsviktiga tjänster som är beroende av den eller de samhällsviktiga tjänsterna som verksamhetsutövaren tillhandahåller.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om vad som utgör en betydande störande effekt.

Uttrycket kritisk infrastruktur ska i lagen avse en tillgång, en anläggning, utrustning, ett nätverk eller ett system, eller en del av en tillgång, en anläggning, utrustning, ett nätverk eller ett system, som krävs för tillhandahållandet av en samhällsviktig tjänst.

Utredningens förslag

Förslaget från utredningen stämmer delvis överens med regeringens. För att identifieras som kritisk verksamhetsutövare krävs enligt utredningens förslag att verksamhetsutövaren tillhandahåller en samhällsviktig tjänst i eller till Sverige och som omfattas av någon av sektorerna som finns i bilagan till CER-direktivet, att verksamhetsutövaren har kritisk infrastruktur belägen i Sverige, och att en incident skulle få en betydande störande effekt för verksamhetsutövarens tillhandahållande av den samhällsviktiga tjänsten. Utredningen föreslår att det ska framgå av lagen att tillsynsmyndigheten vid identifieringen ska beakta den nationella riskbedömningen och strategin för kritiska verksamhetsutövares motståndskraft samt kommissionens genomförandeakter på området.

Remissinstanserna

Majoriteten av remissinstanserna är positiva till eller har inga synpunkter på förslaget.

Bland andra *Affärsverket svenska kraftnät, Länsstyrelsen i Hallands län, Myndigheten för civilt försvar (MCF)* och *Trafikverket* har synpunkter gällande användningen av uttrycket kritisk infrastruktur. MCF bedömer att användningen av uttrycket innebär att regleringen inte kommer att omfatta system och tjänster som upprätthåller viktiga samhällsfunktioner och som inte brukar benämnas infrastruktur vid ett normalt svenskt språkbruk. *Post- och telestyrelsen (PTS)* anser bland annat att det bör förtydligas att

en verksamhetsutövare inom sektorn digital infrastruktur kan pekas ut som kritisk även om den har huvudsakligt etableringsställe i en annan medlemsstat inom EU. Trafikverket anser att det bör tydliggöras att verksamhetsutövaren inte behöver äga den kritiska infrastrukturen som används vid tillhandahållandet av tjänsten. En annan ordning skulle enligt myndigheten innebära att till exempel flygtrafiktjänster utesluts från lagens tillämpningsområde eftersom leverantörer av sådana tjänster sällan äger infrastruktur.

Ett stort antal remissinstanser för fram synpunkter kring regleringen avseende uttrycket betydande störande effekt. *Göteborgs kommun*, *Karlstads kommun, Livsmedelsverket, Luleå kommun*, Länsstyrelsen i Hallands län, *SJ AB*, *Stiftelsen för Internetinfrastruktur*, *Stockholms universitet*, *Sveriges Kommuner och Regioner (SKR)*, *Sveriges universitets- och högskoleförbund (SUHF), Totalförsvarets forskningsinstitut*, *Transportstyrelsen* och *Tågföretagen* för fram synpunkter när det gäller bland annat tröskelvärden och efterfrågar närmare vägledning i myndighetsföreskrifter i enlighet med utredningens förslag samt efterfrågar i vissa fall en möjlighet att lämna synpunkter på föreskrifterna. MCF för fram att utredningens förslag ger ett stort tolkningsutrymme som kan leda till att incidenter som bör bedömas som relevanta faller utanför regelverket. SKR och SUHF för fram att det bör tydliggöras att det som ska bedömas är den betydande störande effekten på tillhandahållandet av den samhällsviktiga tjänsten i stort och inte effekten på den berörda verksamhetsutövarens tillhandahållande av tjänsten.

Svensk Dagligvaruhandel och *Svensk Handel* bedömer att ett utpekande som kritisk verksamhetsutövare, och därmed även som väsentlig enligt NIS 2-direktivet, kan vara kostnadsdrivande. Verksamhetsutövaren får även möjlighet att bedriva och utveckla sin verksamhet under kristid, med risk att slå ut andra aktörer. Det finns därmed en risk för att konkurrensen snedvrids inom dagligvaruhandeln, där det finns få stora aktörer enligt branschorganisationerna. I utpekandet av kritiska verksamhetsutövare bör det därför också ingå en bedömning av risken för snedvridande konkurrens och lämpliga åtgärder för att minimera eller mildra denna.

Skälen för regeringens förslag

Regleringen i direktivet

I artikel 2.1 i CER-direktivet definieras uttrycket kritisk entitet som en offentlig eller privat entitet som har identifierats av en medlemsstat i enlighet med artikel 6 som tillhörande en av de kategorier som anges i den tredje kolumnen i tabellen i bilagan till direktivet. Av artikel 6.1 i CER-direktivet framgår att medlemsstaterna senast den 17 juli 2026 ska identifiera de kritiska entiteterna för de sektorer och undersektorer som anges i direktivets bilaga.

När en medlemsstat identifierar kritiska entiteter ska den enligt artikel 6.2 ta hänsyn till resultatet av sin riskbedömning samt sin strategi. För att en entitet ska kunna identifieras som kritisk i en medlemsstat krävs därutöver enligt artikeln att entiteten tillhandahåller en eller flera samhällsviktiga tjänster (a), att entiteten bedriver verksamhet och dess kritiska infrastruktur är belägen på medlemsstatens territorium (b) samt att en incident skulle få betydande störande effekter, enligt vad som fastställs i

enlighet med artikel 7.1, för entitetens tillhandahållande av en eller flera samhällsviktiga tjänster eller för tillhandahållandet av andra samhällsviktiga tjänster i de sektorer som anges i bilagan och som är beroende av den eller de samhällsviktiga tjänsterna (c).

Verksamhetsutövaren bör tillhandahålla åtminstone en samhällsviktig tjänst och omfattas av någon av kategorierna i bilagan

Som utredningen föreslår bör kriteriet i artikel 6.2 a i CER-direktivet, att verksamhetsutövaren tillhandahåller en eller flera samhällsviktiga tjänster, regleras i den nya lagen och vara en förutsättning för identifiering som kritisk verksamhetsutövare. Vad som avses med uttrycket samhällsviktig tjänst behandlas i avsnitt 6.2. Som utredningen konstaterar tydliggör inte direktivet vad uttrycket tillhandahåller innebär. Regeringen instämmer i utredningens uppfattning att uttrycket bör tolkas som att något görs tillgängligt för användning eller konsumtion, inklusive led som exempelvis etablering, drift eller kontroll.

Utredningen föreslår, såvitt nu är av intresse, att det för identifiering endast ska krävas att verksamhetsutövaren tillhandahåller en samhällsviktig tjänst som omfattas av någon av sektorerna som finns i bilagan till CER-direktivet. I bilagan görs en åtskillnad mellan sektorer, undersektorer och kategorier av entiteter. Artikel 6.1 anger att de kritiska entiteterna ska omfattas av bilagans sektorer och undersektorer, medan artikel 2.1 i sin tur anger att en kritisk entitet ska tillhöra en av de kategorier som anges i den tredje kolumnen i tabellen i bilagan. Med hänsyn till hur artiklarna är utformade bör det, enligt regeringens mening, för identifiering inte vara tillräckligt att verksamhetsutövaren bedriver verksamhet som omfattas av sektorerna och undersektorerna, det vill säga första och andra kolumnen i bilagan. Det bör, till skillnad från vad utredningens förslag innebär, också som utgångspunkt krävas att verksamhetsutövaren som sådan omfattas av någon av kategorierna i tredje kolumnen i tabellen i bilagan till CER-direktivet. Detta bör framgå av lagen.

Vilka verksamhetsutövare som bör omfattas av bilagans kategori offentliga förvaltningsentiteter behandlas i avsnitt 5.3.

Verksamhetsutövaren bör också bedriva verksamhet i Sverige

I artikel 6.2 b i CER-direktivet anges bland annat kriteriet att en entitet bedriver verksamhet på medlemsstatens territorium. Gällande detta anges i direktivets skäl 16 att en entitet bör anses bedriva verksamhet på territoriet i en medlemsstat där den utför verksamhet som är nödvändig för den eller de samhällsviktiga tjänsterna i fråga och där den entitetens kritiska infrastruktur, som används för att tillhandahålla tjänsten eller tjänsterna, är belägen. Om ingen entitet uppfyller dessa kriterier i en medlemsstat bör den medlemsstaten inte vara skyldig att identifiera en kritisk entitet i motsvarande sektor eller undersektor.

Utredningens förslag innebär att kravet på att bedriva verksamhet på medlemsstatens territorium knyts till tillhandahållandet av den samhällsviktiga tjänsten och att det är den samhällsviktiga tjänsten som ska tillhandahållas i eller till Sverige. Regeringen konstaterar att detta inte är i linje med hur direktivet är utformat. Inte heller det som anges i punkt 29 i kommissionens icke-bindande riktlinjer för att stödja identifieringen av

kritiska entiteter talar för en sådan tolkning (se Kommissionens riktlinjer och rapporteringsmall som utarbetats i enlighet med artiklarna 5.5, 6.6 och 7.3 i direktiv [EU] 2022/2557 om kritiska entiteters motståndskraft, C/2025/4990). Kravet på att verksamhetsutövaren ska bedriva verksamhet i Sverige bör därför, enligt regeringens mening, vara ett självständigt krav för identifiering och inte knytas till tillhandahållandet av den samhällsviktiga tjänsten som utredningen föreslår.

När det gäller uttrycket bedriva verksamhet bör detta tolkas i enlighet med direktivets skäl 16, det vill säga att verksamhetsutövaren utför verksamhet som är nödvändig för den eller de samhällsviktiga tjänsterna i fråga. Kravet på nödvändighet bör endast innebära att det ska finnas en koppling mellan den verksamhet som bedrivs och tillhandahållandet av den samhällsviktiga tjänsten. Det bör inte innebära att verksamheten som bedrivs i Sverige behöver vara avgörande för tillhandahållandet av den samhällsviktiga tjänsten eller att all verksamhetsutövarens verksamhet måste bedrivas här. Förekomsten av kritisk infrastruktur i Sverige kan i sig tala för att kravet på att bedriva verksamhet i landet är uppfyllt. I enlighet med vad som anges i artikel 6.2 b i CER-direktivet och punkt 32 i kommissionens icke-bindande riktlinjer bör verksamhetsutövarens etableringsort anses vara irrelevant vid bedömning av om kravet är uppfyllt.

När det gäller rekvisitet ”i Sverige” bedömer regeringen att detta i regel inte bör innebära några tolkningssvårigheter. Ledning bör vid behov kunna tas från punkterna 30, 31 och 32 i kommissionens icke-bindande riktlinjer. Punkt 30 i de icke-bindande riktlinjerna anger, i relevanta delar, att en medlemsstats territorium bör anses omfatta, med förbehåll för de begränsningar som följer av artikel 355 i EUF-fördraget, den medlemsstatens landterritorium och inre vattenvägar samt det territorialhav och dess bädd och underliggande jordlager som fastställts av den medlemsstaten i enlighet med FN:s havsrättskonvention (Unclos). Den omfattar dessutom den ekonomiska zon som medlemsstaten och kontinentalsockeln har upprättat, men endast om det finns en förbindelse mellan den kritiska infrastruktur som är belägen i deras ekonomiska zon eller på kontinentalsockeln och de suveräna rättigheter eller jurisdiktioner som en kuststat utövar i enlighet med Unclos i dessa delar av havet, utan att inkräkta på andra staters rättigheter och friheter som garanteras av Unclos. Vid tillämpningen av artikel 6.2 b i direktivet bör medlemsstaterna därför i förekommande fall göra en bedömning från fall till fall för att fastställa i vilken utsträckning kritisk infrastruktur i deras ekonomiska zon och på kontinentalsockeln omfattas.

I punkt 31 i kommissionens icke-bindande riktlinjer anges att när det till exempel gäller undervattenskablar eller rörledningar som upprättats av andra stater vid utövandet av deras rättigheter enligt artiklarna 58.1 och 79.1 i Unclos och som passerar genom en kustmedlemsstats ekonomiska zon eller kontinentalsockel, ska den medlemsstaten inte vara skyldig att fullgöra sina skyldigheter enligt direktivet med avseende på denna kritiska infrastruktur, i den mån den inte omfattas av dess funktionella suveränitet och jurisdiktion i den ekonomiska zonen och kontinentalsockeln enligt Unclos. Däremot bör undervattenskablar eller rörledningar i en kustmedlemsstats ekonomiska zon eller kontinentalsockel i den staten omfattas av de skyldigheter som fastställs i direktivet, om denna kritiska

infrastruktur är kopplad till den verksamhet genom vilken den staten utövar sin suveränitet eller jurisdiktion i den ekonomiska zonen eller kontinentalsockeln enligt artiklarna 56 och 77 i Unclos.

Av punkt 32 i riktlinjerna framgår att entitetens etableringsort bör anses vara irrelevant för processen med att identifiera kritiska entiteter enligt direktivet.

Verksamhetsutövaren bör också ha kritisk infrastruktur belägen i Sverige

I artikel 6.2 b i CER-direktivet anges också kriteriet att en entitet har dess kritiska infrastruktur belägen på medlemsstatens territorium. Kritisk infrastruktur definieras i artikel 2.4 som en tillgång, en anläggning, utrustning, ett nätverk eller ett system, eller en del av en tillgång, en anläggning, utrustning, ett nätverk eller ett system, som krävs för tillhandahållandet av en samhällsviktig tjänst. Förslaget från utredningen innebär att en verksamhetsutövare måste ha kritisk infrastruktur belägen i Sverige för att kunna identifieras som kritisk och att uttrycket kritisk infrastruktur definieras i enlighet med direktivets definition.

Regeringen instämmer i utredningens uppfattning att kravet på att verksamhetsutövaren ska ha kritisk infrastruktur i Sverige och definitionen av kritisk infrastruktur bör framgå av lagen. Regeringen instämmer även, trots det som bland andra *MCF* för fram, i att definitionen av kritisk infrastruktur bör följa direktivets definition. Direktivet innehåller inte någon närmare reglering om vad som ska anses omfattas av uttrycket kritisk infrastruktur eller hur definitionens beståndsdelar ska tolkas. Regeringen ställer sig bakom utredningens slutsats att definitionen är mycket bred och att den kan innefatta exempelvis byggnader, nätverks- eller informationssystem eller en maskin. Det bör inte finnas någon angiven nedre gräns för vad som ska kunna anses utgöra en del av kritisk infrastruktur. Regeringen anser att uttrycket kritisk infrastruktur bör tolkas i ljuset av direktivets syften, sektorsindelningen och den stora bredd av samhällsviktiga tjänster som omfattas av direktivet där den kritiska infrastrukturen, enligt uttryckets definition, ska krävas för tillhandahållandet. Det pågår en ständig utveckling gällande tillhandahållandet av samhällsviktiga tjänster. Det är därför ändamålsenligt att uttrycket inte ges en alltför snäv innebörd i den nya lagen.

Som utredningen föreslår bör det i lagen ställas upp ett krav på att verksamhetsutövaren har kritisk infrastruktur belägen i Sverige. Uttrycket belägen bör tolkas som att det innebär att infrastrukturen fysiskt ska finnas i Sverige. Uttrycket i Sverige bör tolkas på samma sätt som kopplat till att verksamheten ska bedrivas här. Att verksamhetsutövaren ska ha sådan infrastruktur bör, som *Trafikverket* för fram, omfatta både innehav och nyttjande. Det bör inte spela någon roll huruvida verksamhetsutövaren exempelvis äger, hyr, lånar eller innehar, nyttjar eller råder över den kritiska infrastrukturen på annan grund. Som *PTS* noterar innebär kravet på att verksamhetsutövaren ska ha kritisk infrastruktur belägen i Sverige inte något krav på att verksamhetsutövaren även måste ha sitt huvudsakliga etableringsställe här.

Affärsverket svenska kraftnät för fram, angående kravet att den kritiska infrastrukturen ska vara belägen i Sverige, att kravet innebär att verksamhetsutövare som exempelvis har ett kontrollrum i en annan medlemsstat

som styr anläggningar i Sverige men som saknar anläggningar i det medlemsland där kontrollrummet är beläget inte kommer att identifieras som kritisk i Sverige och antagligen inte heller i den andra medlemsstaten. Regeringen konstaterar dock att detta bland annat beror på om anläggningarna eller kontrollrummet bedöms falla in under definitionen av kritisk infrastruktur i det enskilda fallet. Regeringen bedömer även att kravet på att verksamhetsutövaren ska ha kritisk infrastruktur på medlemsstatens territorium inte bör innebära att all verksamhetsutövarens kritiska infrastruktur måste vara belägen inom en och samma medlemsstats territorium för att verksamhetsutövaren ska kunna identifieras som kritisk. För denna tolkning talar bland annat att artikel 11.1 a i direktivet beskriver en situation där kritiska entiteter använder kritisk infrastruktur som är fysiskt sammankopplad mellan två eller flera medlemsstater.

Att den kritiska infrastrukturen ska krävas för tillhandahållandet av en samhällsviktig tjänst, som nämns i artikel 2.4, bör innebära att det måste finnas en koppling mellan den kritiska infrastrukturen som sådan och tillhandahållandet. Hur stark denna koppling måste vara får bedömas i det enskilda fallet med hänsyn till den kritiska infrastrukturens art och dess betydelse för den samhällsviktiga tjänsten och till den samhällsviktiga tjänsten som sådan.

PTS föreslår att det ska förtydligas att infrastruktur som ägs, förvaltas eller drivs av unionen eller för unionens räkning inom ramen för dess rymdprogram inte omfattas av lagen i enlighet med vad som anges i direktivets skäl 5. Regeringen anser att ett sådant klargörande är överflödigt bland annat eftersom det i bilagan till CER-direktivet i anslutning till sektorn rymden anges att den markbaserade infrastrukturen ska ägas, förvaltas och drivas av medlemsstater eller privata parter.

Vad bör räknas som betydande störande effekt?

I artikel 6.2 c i CER-direktivet anges kriteriet att en incident skulle få betydande störande effekter, enligt vad som fastställs i enlighet med artikel 7.1, för entitetens tillhandahållande av en eller flera samhällsviktiga tjänster eller för tillhandahållandet av andra samhällsviktiga tjänster i de sektorer som anges i bilagan och som är beroende av den eller de samhällsviktiga tjänsterna. Artikel 7.1 anger i sin tur ett antal kriterier som ska beaktas vid bedömningen av om en störande effekt är betydande. Kommissionens icke-bindande riktlinjer, som har antagits med stöd av artikel 7.3, syftar bland annat till att ge ledning avseende tolkningen av uttrycket betydande störande effekt och bedömningen av kriterierna som anges i artikel 7.1.

Innebörden av uttrycket incident behandlas i avsnitt 8.3. Utredningen föreslår att det för identifiering, i detta avseende, ska krävas att en incident skulle få en betydande störande effekt för verksamhetsutövarens tillhandahållande av den samhällsviktiga tjänsten. Utredningens förslag innebär dels att enbart en samhällsviktig tjänst beaktas vid bedömningen, dels att delar av artikel 6.2 c utelämnas. Regeringen uttryckte i lagrådsremissen att regleringen i stället bör följa direktivets utformning. En kritisk verksamhetsutövare kan tillhandahålla flera samhällsviktiga tjänster och en incidents effekter bör bedömas i relation till samtliga dessa. Det bör

därför anges att entitetens tillhandahållande av en eller flera samhällsviktiga tjänster ska beaktas. Att tillhandahållandet av andra samhällsviktiga tjänster än den som den kritiska verksamhetsutövaren tillhandahåller ska beaktas bör vidare vara en viktig del av bedömningskriterierna vid identifieringen av kritiska verksamhetsutövare och bör därför framgå av lagen.

Som *Lagrådet* noterar innebär den i lagrådsremissen föreslagna definitionen av uttrycket incident, som behandlas i avsnitt 8.3, och regleringen om identifiering av kritiska verksamhetsutövare, där effekterna av en incident är ett av kriterierna, en viss dubbelreglering. Lagrådet föreslår att detta bör lösas bland annat genom att uttrycket betydande störande effekt ersätts med det liknande uttrycket betydande störning som används kopplat till uttrycket incident. Detta eftersom det enligt Lagrådet inte finns någon saklig skillnad mellan uttrycken.

Regeringen konstaterar att den i lagrådsremissen föreslagna regleringen, som skiljer på störning, betydande störning och betydande störande effekt, följer CER-direktivets utformning. Enligt artikel 6.2 c ska medlemsstaterna, när de identifierar kritiska entiteter, pröva om en incident skulle få betydande störande effekter enligt artikel 7.1 på ovan angivet sätt. En incident definieras i sin tur enligt artikel 2.3 i direktivet, såvitt nu är av relevans, som varje händelse som kan medföra en betydande störning, eller som medför en störning, av tillhandahållandet av en samhällsviktig tjänst. De kriterier som enligt artikel 7.1 ska beaktas vid bedömningen av om en incident skulle få betydande störande effekter och de kriterier som enligt artikel 15.1 ska beaktas vid bedömningen av om störningen är betydande skiljer sig åt.

Att genomföra Lagrådets förslag innebär enligt regeringens synsätt en risk för ett felaktigt genomförande av CER-direktivet, givet vad som har angetts ovan om att det finns skillnader i sak mellan de bedömningar som ska göras. Regeringen konstaterar vidare att direktivet har genomförts på liknande sätt i Finland och Danmark som föreslås i lagrådsremissen (se lag om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft, 310/2025, och Lov om kritiske enheders modstandsdygtighed [CER-loven], LOV nr 433 af 06/05/2025). Inte heller bör den aktuella inkonsekvensen, där definitionen av uttrycket incident inte helt stämmer överens med hur uttrycket används i regleringen om identifiering, orsaka några praktiska tillämpningsproblem för myndigheterna som ska identifiera kritiska verksamhetsutövare. Regeringen anser därför att det inte finns skäl att frångå direktivets utformning i den del som Lagrådet föreslår och genomför, mot denna bakgrund, inte heller de följdändringar som Lagrådet föreslår kopplat till bemyndigandena att meddela föreskrifter.

Lagrådet föreslår även en omformulering som innebär att bedömningen av en incidents effekter ska göras endast i förhållande till samhällsviktiga tjänster som är beroende av den eller de samhällsviktiga tjänster som verksamhetsutövaren tillhandahåller. Regeringen bedömer att det inte finns möjlighet att frångå direktivet på föreslaget sätt. Regeringen genomför därför inte heller den ändring som Lagrådet föreslår i denna del.

När det gäller det *SKR* och *SUHF* för fram om att det bör tydliggöras att det som ska bedömas är effekten på tillhandahållandet av den samhällsviktiga tjänsten i stort snarare än effekten på den berörda verksamhets-

utövarens tillhandahållande av tjänsten konstaterar regeringen att direktivet innehåller två olika slags skrivningar. När det gäller betydande störande effekter för de samhällsviktiga tjänster som entiteten själv tillhandahåller är det enligt artikel 6.2. c just entitetens egna tillhandahållande som är relevant att beakta. Utformningen av kriterierna i artikel 7.1 talar inte emot en sådan tolkning eftersom exempelvis även entitetens marknadsandel (artikel 7.1 d) bör påverka bedömningen av vad som bör vara att anse som en betydande störande effekt i förhållande till entitetens tillhandahållande av en samhällsviktig tjänst. Som den andra delen av artikel 6.2. c är formulerad är det, vid bedömningen av om en incident skulle få betydande störande effekter för tillhandahållandet av andra samhällsviktiga tjänster i de sektorer som anges i bilagan och som är beroende av den eller de samhällsviktiga tjänsterna, effekterna på tillhandahållandet av de samhällsviktiga tjänsterna i stort som är relevanta att beakta. Med hänsyn till att regeringens förslag innebär att lagstiftningen formuleras i enlighet med direktivet saknas det behov av ett sådant förtydligande som SKR och SUHF efterfrågar.

Bedömningen av om en incident skulle få en betydande störande effekt kommer att göras i förhållande till många olika samhällsviktiga tjänster och verksamhetsutövare inom de sektorer som anges i bilagan. Med beaktande av detta och med hänsyn till de kriterier som anges i artikel 7.1 instämmer regeringen i utredningens uppfattning att uttrycket bör kunna definieras närmare i förordning och i föreskrifter som meddelas av en myndighet. Det tolkningsutrymme som *MCF* resonerar kring bör därför, vid behov, hanteras kopplat till reglering på lägre författningsnivå än lag och frågan faller därmed utanför denna proposition. Detsamma gäller de synpunkter som förs fram av bland andra *Göteborgs kommun*, *Livsmedelsverket* och *SJ AB*. Frågan om möjlighet att meddela föreskrifter på annan författningsnivå gällande uttrycket incident behandlas i avsnitt 8.3.

Vad bör i övrigt beaktas vid identifieringen?

Av artikel 6.2 följer att medlemsstaterna, vid identifieringen av kritiska entiteter, bland annat ska ta hänsyn till resultatet av sin riskbedömning och till sin strategi. EU-kommissionen har i enlighet med artiklarna 5.1 och 23 antagit kompletteringsförordningen, vilken innehåller en icke uttömmande lista över samhällsviktiga tjänster inom de sektorer och undersektorer som omfattas av bilagan till direktivet. Vidare har kommissionen med stöd av artikel 7.3 antagit icke-bindande riktlinjer som bland annat syftar till att ge stöd och ledning i arbetet med att identifiera kritiska entiteter.

Utredningen föreslår att tillsynsmyndigheten vid identifiering ska beakta den nationella riskbedömningen och strategin för kritiska verksamhetsutövares motståndskraft samt kommissionens genomförandeakter på området. Regeringen konstaterar att utformningen av artikel 6.2 inte innebär en uttömmande uppräkning av vad som ska beaktas vid identifieringen. Vidare följer det av tillsynsmyndighetens allmänna utredningsansvar att beakta relevant information och relevanta underlag i identifieringsarbetet, däribland riskbedömningen och strategin. Dessutom bör den föreslagna regleringen tolkas direktivkonformt och då även med beaktande av till exempel kompletteringsförordningen. Därmed framstår den reglering som utredningen föreslår som överflödig. Regeringen anser

därför att det inte bör anges i lagen att riskbedömningen, strategin och kommissionens genomförandeakter ska beaktas särskilt.

Gällande *Svensk Dagligvaruhandels* och *Svensk Handels* synpunkter kopplat till konsekvenserna av att identifieras som en kritisk verksamhetsutövare konstaterar regeringen att närmare överväganden i fråga om förslagens konsekvenser finns i avsnitt 16. Syftet med den nya lagen föreslås vara att stärka kritiska verksamhetsutövares motståndskraft och förmåga att tillhandahålla samhällsviktiga tjänster. Detta bör också vara i fokus vid utformningen av regleringen om identifiering och det finns därutöver ett värde i att följa direktivets utformning i fråga om vad som ska beaktas vid identifiering. Regeringen bedömer därmed att det inte bör ingå vid identifieringen att göra en bedömning av risken för snedvridande konkurrens och lämpliga åtgärder för att minimera eller mildra denna som remissinstanserna föreslår.

6.4 Beslutet om identifiering och reglering om när skyldigheter enligt lagen bör gälla

Regeringens förslag

Den eller de myndigheter som regeringen bestämmer ska i enskilda fall besluta om identifiering av kritiska verksamhetsutövare.

En sådan myndighet ska så snart det kan ske fatta beslut om att en verksamhetsutövare inte längre ska vara en kritisk verksamhetsutövare, om myndigheten bedömer att kraven för att identifieras som en kritisk verksamhetsutövare inte längre är uppfyllda. Beslutet ska gälla omedelbart.

En kritisk verksamhetsutövares skyldighet att vidta åtgärder för motståndskraft samt rapportera incidenter ska börja gälla tio månader efter det att verksamhetsutövaren har fått del av beslutet om identifiering.

Utredningens förslag

Förslaget från utredningen stämmer i huvudsak överens med regeringens. Utredningen föreslår att det i lagen ska anges att det är tillsynsmyndigheterna som inom sina tillsynsområden ska besluta om identifiering och avidentifiering av kritiska verksamhetsutövare. Utredningen föreslår att vissa krav avseende innehållet i ett beslut om identifiering som kritisk verksamhetsutövare ska framgå av lag. Utredningen föreslår också att det ska regleras i lagen att tillsynsmyndigheten, om den beslutar att en verksamhetsutövare inte längre är kritisk, ska underrätta verksamhetsutövaren om detta omedelbart.

Remissinstanserna

Majoriteten av remissinstanserna är positiva till eller har inga synpunkter på förslaget.

Enköpings kommun, *Nynäshamns kommun*, *Salems kommun*, *Stiftelsen för Internetinfrastruktur*, *Tech Sverige* och *Vetenskapsrådet* är positiva till förslaget att det är tillsynsmyndigheterna som, inom sina respektive tillsynsområden, ska ansvara för prövningen av vilka verksamhetsutövare som ska anses vara kritiska. *Sveriges advokatsamfund* anser å andra sidan att en enda myndighet bör få ansvaret, vilken bör samverka med andra berörda myndigheter med särskild kompetens inom relevanta verksamhetsområden. Detta eftersom det enligt samfundet finns en risk att de olika myndigheterna inte kommer att ha den kompetens eller de resurser som krävs för att tillse att lagens syfte uppnås.

Innovations- och kemiindustrierna i Sverige (IKEM) och *Läkemedelsindustriföreningen* för fram att det är viktigt att identifieringen av kritiska verksamhetsutövare sker skyndsamt och att berörda verksamhetsutövare informeras i god tid för att underlätta efterlevnaden av reglerna.

Bland andra *Länsstyrelsen i Västra Götalands län*, *Malmö kommun, Region Stockholm, Sveriges Kommuner och Regioner (SKR)* och Tech Sverige uttalar sig om förslaget om inom vilken tidsfrist kraven enligt lagen ska börja gälla. Malmö kommun ser ett behov av att det tydliggörs om åtgärderna ska vara genomförda inom den tid som föreslås eller om det räcker att de är påbörjade. Om åtgärderna ska vara genomförda vid den tidpunkten anser kommunen, i likhet med *Bolagsverket*, Länsstyrelsen i Västra Götalands län, Region Stockholm och SKR, att tiden för genomförandet är för kort. SKR pekar särskilt på att den föreslagna tidsfristen kan medföra praktiska problem för kritiska verksamhetsutövare som lyder under upphandlingslagstiftningen. Tech Sverige för fram att 18 månader är minimum för att göra större administrativa eller tekniska omställningar. *Advokatfirman Kahn Pedersen* anser att fristen bör löpa ut tio månader efter det att beslutet om att en verksamhet omfattas av lagen har fått laga kraft.

Bland andra *Luleå kommun, Länsstyrelsen i Stockholms län, Svenskt Näringsliv*, *Svenskt Vatten*, *Säkerhets- och försvarsföretagen (SOFF)* och *Teknikföretagen* för fram att det inte har beskrivits i betänkandet hur bedömningen vid identifieringen av kritiska verksamhetsutövare ska gå till. Dessa remissinstanser anser att det är oklart om verksamhetsutövaren förväntas medverka i det arbetet och hur omfattande arbetsinsatsen blir. Länsstyrelserna i Stockholms län och Västra Götalands län för fram att tillsynsmyndigheterna bör ha möjlighet att begära att få del av information om de potentiella kritiska verksamhetsutövarna. När det gäller frågan om behovet av information under identifieringsprocessen för Advokatfirman Kahn Pedersen och *Post- och telestyrelsen (PTS)* fram att det bör införas en skyldighet för tillsynsmyndigheten att upplysa om att verksamhet som omfattas av säkerhetsskyddslagen är undantagen från lagens tillämpningsområde.

Skälen för regeringens förslag

Den eller de myndigheter som regeringen bestämmer bör besluta om identifiering

Enligt artikel 6.1 i CER-direktivet ska medlemsstaterna senast den 17 juli 2026 identifiera de kritiska entiteterna för de sektorer och undersektorer som anges i bilagan till direktivet. Av artikel 6.3 framgår också att

medlemsstaterna ska säkerställa att de kritiska entiteterna underrättas om att de har identifierats som kritiska inom en månad från identifieringen. Medlemsstaterna ska enligt samma artikel informera de kritiska entiteterna om deras skyldigheter enligt kapitlen III och IV i CER-direktivet och om det datum från och med vilket dessa skyldigheter är tillämpliga på dem, utan att detta påverkar tillämpningen av artikel 8. Medlemsstaterna ska informera kritiska entiteter i de sektorer som anges i punkterna 3 (bankverksamhet), 4 (finansmarknadsinfrastruktur) och 8 (digital infrastruktur) i bilagan till CER-direktivet om att de inte har några skyldigheter enligt kapitlen III och IV i CER-direktivet såvida inte nationella åtgärder föreskriver något annat. Artikel 6.4 anger bland annat att medlemsstaterna ska säkerställa att de behöriga myndigheterna enligt CER-direktivet underrättar de behöriga myndigheterna enligt NIS 2-direktivet om identiteten på de kritiska entiteter som de har identifierat inom en månad från identifieringen. Enligt artikel 6.5 är medlemsstaterna också skyldiga att bland annat underrätta ytterligare entiteter som identifieras som kritiska på motsvarande sätt som anges i artikel 6.3. Om en entitet inte längre bedöms vara kritisk ska den enligt artikel 6.5 underrättas om det i god tid och om att den inte längre omfattas av skyldigheterna i kapitel III i CER-direktivet från och med dagen för mottagandet av denna underrättelse.

Utredningens förslag innebär att tillsynsmyndigheterna ska ansvara för att identifiera och besluta om huruvida en verksamhetsutövare är kritisk (se vidare avsnitt 10.1). Utredningens förslag i denna del innebär att en och samma verksamhetsutövare kan identifieras som kritisk av flera tillsynsmyndigheter. Utredningen föreslår även att respektive tillsynsmyndighet ska besluta om att en kritisk verksamhetsutövare inte längre ska vara kritisk samt underrätta verksamhetsutövaren om detta. Utredningen anser att det som i artikel 6.3 beskrivs som en underrättelse till en kritisk verksamhetsutövare bör ske genom beslut mot bakgrund av de skyldigheter som följer av en sådan underrättelse. Utredningen föreslår inte att tidsfristen om en månad för underrättelse avseende identifiering ska regleras i lag. Utredningen anser inte heller att skyldigheten att underrätta de behöriga myndigheterna enligt NIS 2-direktivet ska regleras i lag.

Sveriges advokatsamfund anser att ansvaret för att identifiera kritiska verksamhetsutövare i stället bör läggas på Myndigheten för civilt försvar (MCF). Regeringen har svårt att se att det skulle vara möjligt för en enda myndighet att göra de bedömningar som krävs för identifiering avseende samtliga berörda aktörer. Regeringen instämmer i utredningens uppfattning att det kan vara lämpligt att låta tillsynsmyndigheterna, inom respektive tillsynsområde, identifiera kritiska verksamhetsutövare samt fatta beslut om identifiering. Det kan dock uppkomma situationer där även en myndighet som inte är tillsynsmyndighet bör kunna besluta om identifiering av vissa kritiska verksamhetsutövare, till exempel under en gradvis övergång av tillsynsansvaret från en myndighet till en annan. Det bör därför endast anges i lagen att den eller de myndigheter som regeringen bestämmer i enskilda fall ska besluta om identifiering av kritiska verksamhetsutövare. Regeringen instämmer i utredningens uppfattning att tidsfristen för underrättelser om identifiering samt den beslutande myndighetens skyldighet att underrätta de behöriga myndigheterna enligt NIS 2-direktivet om identifiering inte bör regleras i lag.

Av samma skäl som anges ovan bör den eller de myndigheter som regeringen bestämmer även fatta beslut i enskilda fall om att en verksamhetsutövare inte längre är att bedöma som en kritisk verksamhetsutövare. Det kan handla om situationer där myndigheten till exempel får kännedom om att verksamhetsutövarens verksamhet har utvecklats på visst sätt eller att det i övrigt har tillkommit en omständighet som innebär att myndigheten bedömer att förutsättningarna för att denne ska räknas som en kritisk verksamhetsutövare inte är uppfyllda. Ett sådant beslut bör fattas så snart det kan ske efter att myndigheten har bedömt att kraven för att identifieras som en kritisk verksamhetsutövare inte längre är uppfyllda. Uttrycket så snart det kan ske bör tolkas på så sätt att det inte ska förekomma något onödigt dröjsmål innan ett sådant beslut fattas. Beslutet bör gälla omedelbart.

Lagrådet föreslår en viss omformulering som bland annat innebär att ordet identifiering inte används i aktuell paragraf och rubrik. Ordet förekommer dock på flera ställen i CER-direktivet. Det finns ett visst, om än begränsat värde, i att hålla sig till formuleringen i direktivet enligt regeringens bedömning. Regeringen bedömer inte heller att Lagrådets förslag innebär någon särskild fördel, till exempel i tydlighetshänseende, jämfört med förslaget i lagrådsremissen. Lagrådets förslag genomförs därför inte.

Som utredningen konstaterar innebär beslutet om identifiering skyldigheter för de verksamhetsutövare som identifieras som kritiska. Vilka beslut som bör vara överklagbara behandlas i avsnitt 12. När det gäller frågan om verksamhetsutövarnas deltagande under identifieringsprocessen som väcks av bland andra *Luleå kommun* och *Svenskt Näringsliv* konstaterar regeringen att utredningen inte föreslår någon reglering i denna del. Inte heller CER-direktivet ställer krav på sådan reglering. Den beslutande myndighetens skyldigheter gällande bland annat kommunicering följer dock redan av förvaltningslagen. Det behövs, enligt regeringens mening, ingen kompletterande reglering i denna del. Den beslutande myndighetens skyldigheter enligt förvaltningslagen tillgodoser även det behov av skyndsamhet och information som *IKEM* och *Läkemedelsindustriföreningen* lyfter fram och möter även behovet av en sådan upplysning som *Advokatfirman Kahn Pedersen* och *PTS* nämner. Regeringen anser att det inte har framkommit något tydligt behov av en sådan uppgiftsskyldighet som exempelvis *Länsstyrelsen i Västra Götalands län* föreslår. Det bör ligga i den enskilde verksamhetsutövarens intresse att medverka i processen gällande identifiering.

När det gäller beslutets innehåll anser regeringen, till skillnad från utredningen, att detta inte bör regleras i lag. Enligt regeringens tolkning motsvaras de krav på underrättelsens innehåll som ställs i artikel 6.3 i CER-direktivet av vad som i allmänhet gäller för utformningen av beslut enligt bland annat förvaltningslagen.

När bör skyldigheterna uppstå? Och vad innebär uttrycket har fått del av?

Av artikel 6.3 i CER-direktivet följer att bestämmelser avseende riskbedömningar, åtgärder för motståndskraft, inklusive bakgrundskontroller, samt incidentrapportering ska vara tillämpliga från och med tio månader

efter dagen för en sådan underrättelse som avses i artikel 6.1. I artikel 12.1 anges dock att medlemsstaterna, utan hinder av den tidsfrist som anges i artikel 6.3, ska säkerställa att kritiska entiteter gör en riskbedömning inom nio månader från mottagandet av den underrättelse som avses i artikel 6.3. Tidsfristen gällande skyldigheterna enligt den nya lagen att göra en riskbedömning behandlas i avsnitt 8.1. Även tidsfristen för att vidta övriga åtgärder som nämns i artikel 6.3 bör anges i den nya lagen.

Utredningens förslag innebär att fristen inom vilken skyldigheterna ska börja gälla börjar löpa när den kritiska verksamhetsutövaren har fått del av beslutet om att denne har identifierats som kritisk verksamhetsutövare. Utredningen för inte något resonemang kring innebörden av uttrycket har fått del av och om det bör ställas krav på att verksamhetsutövaren ska delges beslutet. Regeringen anser att uttrycket bör tolkas i ljuset av hur det används i andra svenska författningar, bland annat i 44 § förvaltningslagen där det används för att beskriva tidpunkten för när den enskilde underrättas om ett beslut. När det gäller frågan om det bör ställas krav på delgivning konstaterar regeringen att sådana krav finns i vissa författningar när det gäller för den enskilde betungande beslut i form av exempelvis förbud, tvångsåtgärder, återkallelser av tillstånd eller andra förmåner eller om sanktionsavgifter. Ett beslut om identifiering som kritisk verksamhetsutövare för visserligen med sig vissa skyldigheter men är inte betungande på samma sätt som exempelvis ett beslut om ingripande i form av förbud eller tvångsåtgärder. Med hänsyn till detta, till regleringens syften och till att beslutsmyndigheten alltid har möjlighet att välja att beslutet ska delges bedömer regeringen att det inte bör föreskrivas ett krav på att beslutet om identifiering ska delges.

CER-direktivet anger att tidsfristerna ska börja löpa när verksamhetsutövaren underrättats om att denne har identifierats som kritisk. Regeringen anser att det därför inte är möjligt att föreskriva att fristen ska börja löpa när beslutet om identifiering har fått laga kraft som *Advokatfirman Kahn Pedersen* föreslår. När det gäller det som bland andra *Malmö kommun* och *SKR* för fram gällande vilka åtgärder som ska vara genomförda vid utgången av tidsfristen konstaterar regeringen att innebörden av skyldigheterna behandlas i avsnitt 8.2, 8.3 och 9. En bedömning av om verksamhetsutövaren har vidtagit tillräckliga åtgärder vid den tidpunkt då skyldigheterna har aktualiserats måste göras i varje enskilt fall utifrån hur skyldigheterna är formulerade.

6.5 En kritisk verksamhetsutövare bör räknas som en väsentlig verksamhetsutövare enligt cybersäkerhetslagen

Regeringens förslag

En kritisk verksamhetsutövare ska omfattas av kraven i cybersäkerhetslagen och räknas som en väsentlig verksamhetsutövare enligt den lagen.

Utredningens förslag

Förslaget från utredningen stämmer delvis överens med regeringens. Utredningens förslag innebär att en verksamhetsutövare som har identifierats som kritisk enligt den föreslagna lagen också måste omfattas av bilaga 1 eller 2 till NIS 2-direktivet samt uppfylla kravet på etablering i 1 kap. 4 § cybersäkerhetslagen för att cybersäkerhetslagen ska gälla för den kritiska verksamhetsutövaren med hänvisning till att denne har identifierats som kritisk enligt den nya lagen. Utredningen föreslår att kraven enligt cybersäkerhetslagen ska börja gälla först tio månader efter den dag verksamhetsutövaren har fått del av beslutet om att denne har identifierats som kritisk.

Remissinstanserna

Majoriteten av remissinstanserna är positiva till eller yttrar sig inte särskilt över förslaget. *Livsmedelsverket* efterfrågar ett förtydligande av vilken tillsynsmyndighet som en verksamhetsutövare ska anmäla sig till om verksamhetsutövaren tillhandahåller tjänster inom flera olika sektorer som omfattas av cybersäkerhetslagen. Livsmedelsverket noterar också, i likhet andra remissinstanser, att det finns skillnader i hur avgränsningarna för sektorerna är formulerade i CER-direktivets respektive NIS 2-direktivets bilagor, vilket enligt Livsmedelsverket riskerar att leda till fall där en kritisk verksamhetsutövare som omfattas av CER-direktivets bilaga inte omfattas av bilagorna till NIS 2-direktivet. *Läkemedelsverket* noterar att det finns vissa skillnader vad gäller sektorn hälso- och sjukvård i bilagorna till direktiven, där verksamhetsutövare med tillstånd att bedriva partihandel omfattas av sektorn enligt CER-direktivet men inte enligt NIS 2-direktivet. Läkemedelsverket anser även att det bör förtydligas vilka krav som ska uppfyllas för att en kritisk verksamhetsutövare ska omfattas cybersäkerhetslagen.

Post- och telestyrelsen (PTS) noterar att varken direktivet eller utredningens förslag innebär något krav på att en verksamhetsutövare ska ha huvudsakligt etableringsställe i Sverige för att kunna identifieras som kritisk. Utredningens förslag innebär dock ett krav på att den kritiska verksamhetsutövaren ska ha huvudsakligt etableringsställe i Sverige för att denne ska räknas som väsentlig verksamhetsutövare enligt utredningens förslag till lag som genomför NIS 2-direktivet. Därmed riskerar det att uppstå en situation där en verksamhetsutövare inom sektorn digital infrastruktur omfattas av kraven enligt CER-direktivet i en medlemsstat och kraven enligt NIS 2-direktivet i en annan. PTS önskar förtydliganden avseende hur det gränsöverskridande samarbetet mellan medlemsstaterna bör utformas vid beslut om identifiering av kritiska verksamhetsutövare och även vid tillämpning av övriga bestämmelser som omfattar digital infrastruktur. *Stiftelsen för Internetinfrastruktur (Internetstiftelsen)* anser också att det finns en risk för oklara ansvarsförhållanden eftersom vissa verksamhetsutövare kan omfattas av CER-direktivet men inte av NIS 2-direktivet. Enligt Internetstiftelsen är det därför viktigt med tydliga ansvarsområden för att undvika duplicering av tillsyn och rapporteringskrav. *Transportstyrelsen* påpekar att inom sektorn transport anges kollektivtrafikföretag i bilagan till CER-direktivet men inte i bilagorna till NIS 2-direktivet. Transportstyrelsen instämmer inte i utredningens

uppfattning att en kritisk verksamhetsutövare måste bedriva verksamhet som omfattas av bilagorna till NIS 2-direktivet för att omfattas av cybersäkerhetslagen.

Skälen för regeringens förslag

Kraven enligt NIS 2-direktivet

NIS 2-direktivet är som utgångspunkt tillämpligt på offentliga eller privata entiteter av den typ som avses i direktivets bilaga 1 eller 2, som uppfyller ett visst storlekskrav och som tillhandahåller sina tjänster eller bedriver sin verksamhet i unionen (artikel 2.1). Direktivet är även tillämpligt på vissa entiteter oavsett storlek (artikel 2.2–2.4). Artikel 2.2 a–e i NIS 2-direktivet innehåller särskilda kvalificeringsgrunder för entiteter som omfattas av bilaga 1 eller 2, men som inte uppfyller storlekskravet. I bilaga 1 och 2 till direktivet anges de 18 sektorer, uppdelade i högkritiska och andra kritiska sektorer och i viss utsträckning delsektorer, som omfattas av direktivet (se vidare avsnitt 4.3). Entiteter som omfattas av direktivet ska antingen anses vara väsentliga eller viktiga beroende på bland annat vilken sorts entitet det är fråga om och entitetens storlek (artikel 3). Denna indelning påverkar bland annat vilka tillsynsåtgärder som kan komma i fråga vid överträdelser av regleringen.

Enligt huvudregeln ska entiteter som omfattas av direktivet enligt artikel 26.1 i NIS 2-direktivet anses omfattas av jurisdiktionen i den medlemsstat där de är etablerade, utom när det gäller vissa särskilt angivna entiteter. I fråga om vissa entiteter gäller att de omfattas av jurisdiktionen i den medlemsstat där de tillhandahåller sina tjänster (artikel 26.1 a). Andra entiteter ska, såvitt nu är av intresse, enligt artikel 26.1 b anses omfattas av jurisdiktionen i den medlemsstat där de har sitt huvudsakliga etableringsställe i unionen i enlighet med artikel 26.2.

Av artikel 2.3 i NIS 2-direktivet framgår att direktivet är tillämpligt på entiteter som identifieras som kritiska entiteter enligt CER-direktivet, oavsett entiteternas storlek. I artikel 3.1 f i NIS 2-direktivet anges vidare att entiteter som identifierats som kritiska entiteter enligt CER-direktivet ska anses vara väsentliga entiteter enligt NIS 2-direktivet.

På vilka grunder bör kritiska verksamhetsutövare omfattas av cybersäkerhetslagen?

Utredningens förslag innebär att verksamhetsutövare som har identifierats som kritiska enligt den nya lagen ska omfattas av cybersäkerhetslagen och räknas som väsentliga verksamhetsutövare enligt den lagen. Utredningen bedömer att det, utöver att verksamhetsutövaren har identifierats som kritisk, ska krävas att verksamhetsutövaren bedriver verksamhet som omfattas av bilaga 1 eller 2 till NIS 2-direktivet och att verksamheten ska vara etablerad i Sverige i NIS 2-direktivets mening. Utredningen menar att denna ordning följer av regleringen i NIS 2-direktivet och att det enda undantaget från kraven i NIS 2-direktivet avser storlekskravet. Enligt utredningen skulle en annan bedömning medföra komplicerade ställningstaganden kring jurisdiktion samt svårförutsägbara konsekvenser. Till följd av skillnaderna vad gäller de sektorer som omfattas av direktiven skulle det till exempel kunna finnas verksamhetsutövare som inte omfattas av

NIS 2-direktivet, men som identifieras enligt CER-direktivet och därmed inte omfattas av tillsynsområdet för tillsynsmyndigheterna enligt den lag som genomför NIS 2-direktivet.

Regeringen instämmer i utredningens uppfattning att NIS 2-direktivets krav innebär att cybersäkerhetslagen bör ändras på så sätt att verksamhetsutövare som har identifierats som kritiska enligt den nya lagen ska omfattas av cybersäkerhetslagen och att de bör räknas som väsentliga verksamhetsutövare enligt samma lag. Regeringen instämmer även i att det inte bör ställas upp något storlekskrav för att kritiska verksamhetsutövare ska omfattas av cybersäkerhetslagen.

När det gäller frågan om kritiska verksamhetsutövare behöver bedriva verksamhet som omfattas av bilaga 1 eller 2 till NIS 2-direktivet för att omfattas av cybersäkerhetslagen konstaterar regeringen att detta inte uttrycks tydligt i CER-direktivet respektive NIS 2-direktivet. Som *Transportstyrelsen* lyfter fram anges det dock, i artikel 1.2 b i NIS 2-direktivet, att direktivet fastställer riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter för entiteter av den typ som avses i bilagorna till direktivet samt för entiteter som identifieras som kritiska entiteter enligt CER-direktivet. Vidare nämns bilagorna särskilt i artikel 2.1 och 2.2 i NIS 2-direktivet, men inte i artikel 2.3. Mot denna bakgrund anser regeringen att det inte bör ställas upp krav på att kritiska verksamhetsutövare ska omfattas av bilaga 1 eller 2 till NIS 2-direktivet för att de ska omfattas av cybersäkerhetslagen. Tolkningen i denna del innebär att skillnaderna mellan bilagorna till NIS 2- och CER-direktiven, som till exempel *Livsmedelsverket* och *Läkemedelsverket* lyfter fram, inte bör innebära några problem vid tillämpningen av regelverken. De följder som denna tolkning får för tillsynsmyndigheternas uppdrag får, i den mån det behövs, hanteras genom utformningen av tillsynsområdena kopplat till NIS 2-direktivet. Tillsynsområdena, som regleras i cybersäkerhetsförordningen (2025:1507), är inte föremål för behandling i denna proposition.

Utredningen bedömer att kritiska verksamhetsutövare även behöver uppfylla kravet på etablering enligt NIS 2-direktivet för att de ska omfattas av cybersäkerhetslagen med hänvisning till att de är kritiska verksamhetsutövare. Utredningen drar denna slutsats eftersom artikel 2.3 endast innebär ett uttryckligt undantag från storlekskravet. En annan bedömning skulle enligt utredningen medföra komplicerade ställningstaganden kring jurisdiktion samt svårförutsägbara konsekvenser för både verksamhetsutövare och tillsynsmyndigheterna. Regeringen gör andra bedömningar än utredningen i dessa delar.

Artikel 2.3 i NIS 2-direktivet är visserligen inte formulerad som att det görs ett undantag från kraven gällande jurisdiktion i artikel 26. Enligt bland annat skäl 30 i NIS 2-direktivet bör man dock, med tanke på kopplingarna mellan cybersäkerhet och entiteters fysiska säkerhet, säkerställa samstämmighet mellan NIS 2- och CER-direktiven. För att uppnå detta bör enligt samma skäl entiteter som identifieras som kritiska entiteter enligt CER-direktivet anses vara väsentliga entiteter enligt NIS 2-direktivet. Utgångspunkten bör därmed vara att kritiska verksamhetsutövare ska omfattas av regleringen som genomför NIS 2-direktivet. Utredningens förslag innebär dock att en kritisk verksamhetsutövare behöver uppfylla kraven på jurisdiktion enligt både CER-direktivet och

NIS 2-direktivet. Utredningens förslag skulle därmed kunna innebära att det uppstår situationer där en verksamhetsutövare omfattas av regleringen som genomför CER-direktivet i Sverige men inte regleringen som genomför NIS 2-direktivet, vilket inte är i linje med hur direktiven är utformade. Regeringen gör därför bedömningen att det inte bör föreskrivas att kritiska verksamhetsutövare ska uppfylla krav på etablering i cybersäkerhetslagen för att omfattas av den lagen. Med föreslagen reglering krävs inga sådana förtydliganden som *PTS* efterfrågar.

När det gäller de synpunkter kring behovet av tydliga ansvarsområden för att undvika duplicering av tillsyn och rapporteringskrav som *Internetstiftelsen* för fram samt Livsmedelsverkets synpunkt om ansvarig tillsynsmyndighet konstaterar regeringen följande. Vilka som är tillsynsmyndigheter enligt cybersäkerhetslagen och vilka områden som de utövar tillsyn över regleras i cybersäkerhetsförordningen. Det föreslås inte heller regleras i lag vilka myndigheter som ska utöva tillsyn enligt den nya lagen (se avsnitt 10.1). Det finns därmed inte anledning att göra några uttalanden i denna proposition om tillsynsområdena. Det kan dock konstateras att en myndighet, enligt 6 § myndighetsförordningen (2007:515), ska verka för att genom samarbete med bland annat andra myndigheter ta till vara de fördelar som kan vinnas för enskilda och för staten som helhet. Enligt 8 § förvaltningslagen ska en myndighet vidare inom sitt verksamhetsområde samverka med andra myndigheter och i rimlig utsträckning hjälpa den enskilde genom att själv inhämta upplysningar eller yttranden från andra myndigheter. Regeringen utgår ifrån att samverkan mellan tillsynsmyndigheterna kommer att fungera väl när det gäller bland annat sådana frågor som behöver hanteras gemensamt. En anmälan enligt cybersäkerhetslagen ska, som svar på Livsmedelsverkets fråga, enligt 5 § cybersäkerhetsförordningen göras till den gemensamma kontaktpunkten enligt 23 § samma förordning.

Ingen reglering om när skyldigheterna ska börja gälla

Utredningen föreslår att skyldigheterna enligt cybersäkerhetslagen för verksamhetsutövare som omfattas av den lagen med hänvisning till att de är kritiska verksamhetsutövare ska börja gälla tio månader efter att den kritiska verksamhetsutövaren fått del av beslutet om identifiering (se avsnitt 6.4). Utredningen motiverar förslaget med att det syftar till att mildra konsekvenserna för små företag. Regeringen konstaterar att en sådan frist är främmande för både cybersäkerhetslagen och NIS 2-direktivet. Vidare konstaterar regeringen att fristen skulle tillämpas även på andra verksamhetsutövare än små företag. Sammantaget bedömer regeringen att det inte bör införas en sådan tidsfrist som utredningen föreslår. Vilka krav enligt cybersäkerhetslagen som vid var tid ska vara uppfyllda bör hanteras i enlighet med vad som föreskrivs i den lagen och i enlighet med vad som framgår av förarbetena till cybersäkerhetslagen (se prop. 2025/26:28 s. 79 f.).

7 Kritiska verksamhetsutövare av särskild europeisk betydelse

7.1 Anmälningsskyldighet

Regeringens förslag

En kritisk verksamhetsutövare som tillhandahåller en samhällsviktig tjänst till eller i minst sex medlemsstater inom EU ska så snart det kan ske anmäla detta till den eller de myndigheter som regeringen bestämmer.

Utredningens förslag

Förslaget från utredningen stämmer delvis överens med regeringens. Utredningen föreslår att det ska regleras i lag vad anmälan ska innehålla och att anmälan ska ske till tillsynsmyndigheten. Utredningen föreslår också att det ska regleras särskilt att anmälningsskyldigheten inte gäller för kritiska verksamhetsutövare inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur. I betänkandet lämnas även förslag om att det ska regleras i lag att den myndighet som regeringen bestämmer och den kritiska verksamhetsutövaren ska delta i EU-kommissionens samråd enligt artikel 17.2 i CER-direktivet. Utredningen föreslår vidare att det ska regleras i lag att den myndighet som regeringen bestämmer ska vidarebefordra informationen i en underrättelse från kommissionen, om att en verksamhetsutövare är att betrakta som kritisk entitet av särskild europeisk betydelse, till verksamhetsutövaren.

Remissinstanserna

Advokatfirman Kahn Pedersen och *Finansinspektionen* för fram att utredningen föreslår en dubbelreglering i fråga om att anmälningsskyldigheten inte gäller för verksamhetsutövare inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur. *Drivkraft Sverige* anser att det bör finnas tröskelvärden att tillämpa vid bedömningen av tillhandahållandet av den samhällsviktiga tjänsten per land. Övriga remissinstanser yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag

Reglering om identifiering i direktivet

Kritiska entiteter bedriver, enligt skäl 35 i CER-direktivet, i allmänhet sin verksamhet inom ramen för ett alltmer sammankopplat nätverk av tillhandahållande av tjänster och infrastruktur och tillhandahåller ofta samhällsviktiga tjänster i mer än en medlemsstat. Vissa av dessa kritiska entiteter har särskild betydelse för unionen och den inre marknaden eftersom de tillhandahåller samhällsviktiga tjänster till eller i minst sex medlemsstater, och kan därför omfattas av särskilt stöd på unionsnivå. Därför bör det enligt samma skäl fastställas regler om rådgivande uppdrag med avseende på sådana kritiska entiteter av särskild europeisk betydelse

(se vidare artikel 18 och avsnitt 7.2). Dessa regler påverkar, enligt skäl 35, inte de regler om tillsyn och kontroll av efterlevnad som fastställs i direktivet.

Enligt artikel 17 ska kritiska entiteter av särskild europeisk betydelse identifieras. För att betraktas som en sådan entitet ska kraven i artikel 17.1 vara uppfyllda. Entiteten ska ha identifierats som en kritisk entitet enligt artikel 6.1 (a), tillhandahålla samma eller liknande samhällsviktiga tjänster till eller i minst sex medlemsstater (b), och ha mottagit en underrättelse från kommissionen enligt artikel 17.3 (c).

Av artikel 17.2 framgår att medlemsstaterna ska säkerställa att en kritisk entitet, efter den underrättelse som avses i artikel 6.3 och som behandlas i avsnitt 6.4, informerar sin behöriga myndighet om den tillhandahåller samhällsviktiga tjänster till eller i minst sex medlemsstater. I ett sådant fall ska medlemsstaterna säkerställa att den kritiska entiteten underrättar sin behöriga myndighet om de samhällsviktiga tjänster som den tillhandahåller till eller i dessa medlemsstater och till eller i vilka medlemsstater den tillhandhåller sådana samhällsviktiga tjänster. Medlemsstaterna ska också utan onödigt dröjsmål underrätta kommissionen om identiteten på dessa kritiska entiteter och den information som de tillhandahåller enligt artikel 17.2.

Kommissionen ska samråda med den behöriga myndigheten som har identifierat en sådan kritisk entitet som avses i artikel 17.2, de behöriga myndigheterna i andra berörda medlemsstater samt den kritiska entiteten. Vid dessa samråd ska varje medlemsstat informera kommissionen om den bedömer att de tjänster som den kritiska entiteten tillhandahåller den medlemsstaten är samhällsviktiga tjänster.

Av artikel 17.3 framgår att om kommissionen, på grundval av de samråd som avses i artikel 17.2, fastställer att den berörda kritiska entiteten tillhandahåller samhällsviktiga tjänster till eller i fler än sex medlemsstater, ska kommissionen underrätta den berörda entiteten, genom dess behöriga myndighet, om att den betraktas som en kritisk entitet av särskild europeisk betydelse och informera den kritiska entiteten om dess skyldigheter enligt kapitel IV i CER-direktivet samt från och med vilken dag dessa skyldigheter är tillämpliga på entiteten. Kapitel IV, som benämns Kritiska entiteter av särskild europeisk betydelse, omfattar artiklarna 17 och 18 i CER-direktivet. När kommissionen underrättar den behöriga myndigheten om sitt beslut ska den behöriga myndigheten utan onödigt dröjsmål vidarebefordra underrättelsen till den kritiska entiteten.

Enligt artikel 17.4 ska kapitel IV i CER-direktivet tillämpas på berörda kritiska entiteter av särskild europeisk betydelse från och med dagen för mottagandet av den underrättelse som avses i artikel 17.3. Av artikel 8 följer att kapitlet inte är tillämpligt på kritiska entiteter som har identifierats inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur.

Verksamhetsutövaren bör vara skyldig att göra en anmälan men det krävs ingen reglering om samråd

För att kunna identifiera kritiska entiteter av särskild europeisk betydelse, härefter kritiska verksamhetsutövare av särskild europeisk betydelse, och för att genomföra artikel 17.2 i CER-direktivet behöver det, som utred-

ningen bedömer, regleras hur relevant myndighet ska få del av den information som krävs enligt artikeln. Utredningens bedömning är att det bör införas en skyldighet för en kritisk verksamhetsutövare att så snart det kan ske anmäla om den tillhandahåller den samhällsviktiga tjänsten till eller i minst sex medlemsstater till tillsynsmyndigheten. Av anmälan ska det, enligt utredningens förslag, framgå vilken samhällsviktig tjänst som tillhandahålls och till eller i vilka medlemsstater den tillhandahålls.

Regeringen bedömer att det bör införas en sådan skyldighet som utredningen föreslår med viss omformulering. Anmälningsskyldigheten bör gälla för en kritisk verksamhetsutövare som tillhandahåller en samhällsviktig tjänst till eller i minst sex medlemsstater inom EU och en anmälan bör göras så snart det kan ske till den eller de myndigheter som regeringen bestämmer. Som *Lagrådet* noterar talas det i artikel 17.2 i CER-direktivet, till skillnad från i regeringens förslag, om samhällsviktiga tjänster i pluralis. Som anges i författningskommentaren bör en anmälan göras även om verksamhetsutövaren tillhandahåller olika samhällsviktiga tjänster i de olika medlemsstaterna. Regeringens förslag innebär därmed ingen ändring i sak i förhållande till direktivet. Lagrådet anser att det även krävs en förklaring när det gäller hur artikel 17.1 b, där uttrycket samma eller liknande samhällsviktiga tjänster används, ska uppfattas. Den sistnämnda artikeln behandlar förutsättningarna för att betraktas som en kritisk verksamhetsutövare av särskild europeisk betydelse medan artikel 17.2 behandlar en verksamhetsutövares skyldighet att lämna information på ovan angivet sätt.

Anmälans innehåll kan regleras på lägre författningsnivå än lag. I enlighet med de överväganden som görs i avsnitt 6.4 gällande vilken eller vilka myndigheter som bör besluta om identifiering av kritiska verksamhetsutövare bedömer regeringen att det i lagen bör anges att anmälan ska göras till den eller de myndigheter som regeringen bestämmer. *Drivkraft Sverige* anser att det bör finnas tröskelvärden att tillämpa vid bedömningen av tillhandahållandet av den samhällsviktiga tjänsten per land. Regeringen konstaterar att kraven för att betraktas som en kritisk verksamhetsutövare av särskild europeisk betydelse följer av utformningen av artikel 17.1 i CER-direktivet. Det finns ingen möjlighet att utforma den nationella regleringen på ett sätt som avviker från direktivet i denna del.

Att en anmälan ska göras så snart det kan ske bör innebära att en anmälan ska göras i omedelbar anslutning till att verksamhetsutövaren identifieras som kritisk enligt den nya lagen, om det rör sig om en verksamhetsutövare som redan vid den tidpunkten tillhandahåller en samhällsviktig tjänst till eller i minst sex medlemsstater. Om en verksamhetsutövare utvecklar sin verksamhet på ett sätt som gör att denne omfattas av anmälningsskyldigheten bör en anmälan göras i samband med att verksamhetsutövaren börjar att tillhandahålla en samhällsviktig tjänst i eller till minst sex medlemsstater. Det kommer i det enskilda fallet att vara tillsynsmyndigheten och ytterst en domstol som avgör om en anmälan har gjorts i rätt tid (se vidare avsnitt 11).

Eftersom kapitel IV i CER-direktivet inte ska tillämpas på kritiska verksamhetsutövare inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur bör anmälningsskyldigheten, som utredningen anger, inte gälla för dessa kritiska verksamhetsutövare. Det

behöver dock enligt regeringen, och som bland andra *Finansinspektionen* för fram, inte införas ett särskilt undantag avseende detta utöver det som behandlas i avsnitt 5.4.1.

Utredningen föreslår att det i lagen också ska regleras att dels den myndighet som regeringen bestämmer, dels den kritiska verksamhetsutövare som har gjort en anmälan ska delta i kommissionens samråd enligt artikel 17.2 i CER-direktivet. Den förstnämnda delen behöver inte regleras i lag (jfr 8 kap. 2 § regeringsformen). När det gäller en kritisk verksamhetsutövares skyldighet att delta i samrådet gör regeringen följande överväganden. Det finns ingen beskrivning i betänkandet om vilka skyldigheter som utredningens förslag skulle innebära i praktiken. Utredningen anger inte att verksamhetsutövaren inom ramen för samråd skulle vara skyldig att bidra med information, delta vid möten eller liknande. Både den engelska och franska språkversionen av direktivet ger dessutom uttryck för att artikel 17.2 handlar om att kommissionen ska konsultera bland annat den kritiska verksamhetsutövaren inför ett beslut om att betrakta verksamhetsutövaren som en kritisk verksamhetsutövare av särskild europeisk betydelse. Formuleringarna i dessa språkversioner talar därmed närmast för att artikeln tar sikte på att bland annat den kritiska verksamhetsutövaren ska få tillfälle att yttra sig inför beslutet. Direktivet ställer, enligt regeringens tolkning av detsamma, varken krav på något särskilt deltagande från verksamhetsutövarens sida vid ett samråd enligt artikel 17.2 eller krav på medlemsstaterna att införa reglering om sådant deltagande. Mot denna bakgrund bör det inte införas sådan reglering i lagen som utredningen föreslår i denna del.

Utredningen föreslår också att det ska införas en bestämmelse i lagen som upplyser om att den myndighet som regeringen bestämmer så snart det kan ske ska vidarebefordra den information som finns i en underrättelse från kommissionen till en sådan verksamhetsutövare som betraktas som en kritisk verksamhetsutövare av särskild europeisk betydelse. Kommissionen ska i sin underrättelse informera den kritiska verksamhetsutövaren om verksamhetsutövarens skyldigheter enligt kapitel IV i CER-direktivet samt från och med vilken dag dessa skyldigheter är tillämpliga på entiteten. Underrättelsen innehåller alltså information om skyldigheter för enskilda men vidarebefordran får inte i sig någon rättsverkan. Det finns därmed, även med beaktande av underrättelsens innehåll, ingen anledning att reglera frågan om en skyldighet att vidarebefordra informationen i lag (jfr särskilt 8 kap. 2 § 1 och 2 regeringsformen). Detta kan göras på en annan författningsnivå. Utredningens förslag i denna del bör därmed inte genomföras.

7.2 Medverkan till genomförande av rådgivande uppdrag

Regeringens förslag

En tillsynsmyndighet ska inom ramen för sin tillsyn medverka till genomförande av rådgivande uppdrag i enlighet med artikel 18 i CER-direktivet.

Utredningens förslag

Förslaget från utredningen stämmer delvis överens med regeringens. Utredningen föreslår att en kritisk verksamhetsutövare av särskild europeisk betydelse på begäran av Myndigheten för samhällsskydd och beredskap, numera Myndigheten för civilt försvar (MCF), ska tillhandahålla sin riskbedömning och en förteckning över relevanta vidtagna åtgärder för motståndskraft. Skyldigheten ska enligt utredningens förslag gälla från och med den dag som den kritiska verksamhetsutövaren mottagit EU-kommissionens underrättelse. Utredningen föreslår att det ska införas särskild reglering i vilken det lämnas upplysning om att rådgivande uppdrag anordnas av kommissionen, att rådgivande uppdrag genomförs inom ramen för tillsyn och vad syftet är med ett rådgivande uppdrag.

Remissinstanserna

Advokatfirman Kahn Pedersen anser att den av utredningen föreslagna paragrafen som bland annat upplyser om att ett rådgivande uppdrag anordnas av kommissionen bör utgå eftersom den bör vara av informativ art. *Transportstyrelsen* för fram att det inte framgår av förslaget att rådgivande uppdrag kan bli aktuellt även för kritiska verksamhetsutövare som inte är av särskild europeisk betydelse. Övriga remissinstanser yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag

Reglering om rådgivande uppdrag i direktivet

Enligt artikel 13.4 i CER-direktivet ska, på begäran av den medlemsstat som identifierade den kritiska entiteten och med den berörda kritiska entitetens samtycke, kommissionen anordna rådgivande uppdrag i enlighet med de arrangemang som fastställs i artikel 18.6, 18.8 och 18.9 för att tillhandahålla rådgivning för den berörda kritiska entiteten avseende uppfyllandet av dess skyldigheter enligt kapitel III, som handlar om kritiska entiteters motståndskraft och som omfattar artiklarna 12–16. Det rådgivande uppdraget ska rapportera sina slutsatser till kommissionen, medlemsstaten och den berörda kritiska entiteten.

I artikel 18 finns bestämmelser om skyldigheten för kommissionen att i vissa andra fall anordna rådgivande uppdrag och om hur ett rådgivande uppdrag ska rapporteras samt bestämmelser om kommissionens yttrande till berörd medlemsstat. Kommissionen ska enligt artikel 18.6 anta en genomförandeakt avseende dessa förfaranden.

På motiverad begäran från kommissionen eller från en eller flera medlemsstater till eller i vilka den samhällsviktiga tjänsten tillhandahålls, ska den medlemsstat som har identifierat en kritisk entitet av särskild europeisk betydelse som en kritisk entitet enligt artikel 6.1 tillhandahålla kommissionen viss information i enlighet med artikel 18.3 (jfr även skäl 36). Det rör sig om relevanta delar av riskbedömningen av kritiska entiteter (a), en förteckning över relevanta åtgärder som vidtagits i enlighet med artikel 13 (b), och tillsyns- eller efterlevnadskontrollåtgärder, inbegripet bedömningar av efterlevnad eller utfärdade förelägganden, som dess behöriga myndighet har vidtagit enligt artiklarna 21 och 22 med avseende på den kritiska entiteten (c).

I artikel 18.4 och 18.5 i direktivet finns bestämmelser om rapportering av slutsatser, om experter i det rådgivande uppdraget och om säkerhetsgodkännande av experterna. Där anges också att programmet för varje rådgivande uppdrag ska anordnas i samråd med deltagarna och i överenskommelse med den medlemsstat som har identifierat en kritisk verksamhetsutövare av särskild europeisk betydelse enligt artikel 6.1.

Enligt artikel 18.7 ska medlemsstaterna säkerställa att kritiska entiteter av särskild europeisk betydelse ger det rådgivande uppdraget åtkomst till uppgifter, system och anläggningar som rör tillhandahållandet av deras samhällsviktiga tjänster som är nödvändiga för utförandet av det berörda rådgivande uppdraget. Rådgivande uppdrag ska enligt artikel 18.8 genomföras i enlighet med tillämplig nationell rätt i den medlemsstat där de äger rum med respekt för den medlemsstatens ansvar för den nationella säkerheten och skyddet av sina säkerhetsintressen. När kommissionen anordnar rådgivande uppdrag ska den, enligt artikel 18.9, bland annat ta hänsyn till rapporterna från inspektioner som kommissionen har genomfört enligt vissa EU-förordningar.

Utredningens förslag i denna del

Utredningen konstaterar att artikel 18 i CER-direktivet i stor utsträckning reglerar kommissionens förfaranden och i övrigt har sådant innehåll att direktivet i denna del kan genomföras på förordningsnivå. Utredningen föreslår dock att det ska införas viss reglering i den nya lagen om rådgivande uppdrag och att det bland annat ska framgå att sådana anordnas av kommissionen och genomförs inom ramen för en tillsyn.

Utredningen föreslår också att det ska införas reglering i lagen som uttrycker att syftet med ett rådgivande uppdrag är att bedöma de åtgärder som har vidtagits av verksamhetsutövaren för att uppfylla skyldigheterna att göra en riskbedömning, vidta åtgärder för motståndskraft, inbegripet genomförande av bakgrundskontroller, samt genomföra incidentrapportering. För att genomföra artikel 18.4 föreslår utredningen att det ska införas en bestämmelse i lagen om att en kritisk verksamhetsutövare av särskild europeisk betydelse på begäran av MCF ska tillhandahålla den riskbedömning som behandlas i avsnitt 8.1 och en förteckning över relevanta vidtagna åtgärder för motståndskraft (jfr avsnitt 8.2). Det utvecklas inte vilka åtgärder som ska anses vara relevanta eller vilken aktör som ska göra bedömningen av relevansen.

Utredningen föreslår att skyldigheten att tillhandahålla informationen ska gälla från och med den dag då verksamhetsutövaren har mottagit kommissionens underrättelse (se avsnitt 7.1). Skyldigheten att tillhandahålla informationen skulle enligt utredningen kunna inträffa innan de tidsfrister som behandlas i avsnitt 6.4 och 8.1 har löpt ut. Om detta skulle inträffa bör MCF enligt utredningens bedömning avvakta med sin begäran om information, eftersom någon skyldighet att vidta åtgärder ännu inte har inträtt.

Tillsynsmyndigheten bör enligt utredningen, inom ramen för tillsyn och sina föreslagna tillsynsbefogenheter, bedöma vilken åtkomst till uppgifter, system och anläggningar som krävs för genomförandet av det rådgivande uppdraget i enlighet med artikel 18.7. Detta innebär enligt utredningen att det inte behöver införas någon särskild skyldighet för den kritiska

verksamhetsutövaren av särskild europeisk betydelse att medverka i det rådgivande uppdraget i enlighet med artikeln. Däremot föreslår utredningen att det ska framgå av regleringen avseende tillsynsmyndighetens uppdrag att tillsynsmyndigheten, utöver att utöva tillsyn över att lagen och föreskrifter som meddelats i anslutning till lagen följs, även inom ramen för tillsyn genomför rådgivande uppdrag.

Utredningen bedömer att artikel 13.4 innebär att kommissionen ska anordna ett rådgivande uppdrag även för en verksamhetsutövare som inte är av särskild europeisk betydelse om en medlemsstat begär det. En sådan begäran kräver dock samtycke från verksamhetsutövaren. Utredningen föreslår att det ska regleras i förordning att ett sådant rådgivande uppdrag endast får anordnas efter samtycke.

Vilken reglering om rådgivande uppdrag bör införas i den nya lagen?

Advokatfirman Kahn Pedersen anser att den av utredningen föreslagna paragrafen som bland annat upplyser om att ett rådgivande uppdrag anordnas av kommissionen bör utgå eftersom den bör vara av informativ art. Regeringen instämmer i att utredningens förslag, av angivet skäl, inte bör genomföras.

Utredningen föreslår, i fråga om genomförandet av artikel 18.7, att det ska framgå av regleringen avseende tillsynsmyndighetens uppdrag att tillsynsmyndigheten inom ramen för tillsyn genomför rådgivande uppdrag. Ett rådgivande uppdrag syftar till att göra en bedömning av om verksamhetsutövaren har uppfyllt sina skyldigheter i enlighet med direktivet och därmed i förlängningen enligt den nya lagen. Mot denna bakgrund bedömer regeringen, i likhet med utredningen, att tillsynsmyndigheten även bör kunna vidta sådana åtgärder som avses i avsnitt 10.2 i samband med ett rådgivande uppdrag och att det inte krävs någon särskild reglering i övrigt för att genomföra artikel 18.7. Eftersom det inte är tillsynsmyndigheten som genomför ett rådgivande uppdrag bör den av utredningen föreslagna bestämmelsen dock omformuleras något. Det bör i stället framgå av lagen att en tillsynsmyndighet inom ramen för tillsyn ska medverka till genomförande av rådgivande uppdrag.

Lagrådet anser att det krävs en omformulering av bestämmelsen om tillsynsmyndighetens uppdrag i aktuell del. Lagrådet föreslår att det ska anges att tillsynsmyndigheten inom ramen för sin tillsyn, om förutsättningarna för det är uppfyllda, ska medverka till att ett sådant rådgivande uppdrag som avses i artikel 18 i CER-direktivet anordnas av kommissionen och att det rådgivande uppdraget därefter genomförs i enlighet med direktivet. Regeringen bedömer att Lagrådets förslag skulle kunna tolkas som att det finns en risk för att ett rådgivande uppdrag anordnas trots att förutsättningarna enligt direktivet inte är uppfyllda och dessutom på ett sätt som inte är förenligt med direktivet. Tillsynsmyndighetens uppdrag är, enligt regeringens synsätt, inte heller att bevaka att uppdraget genomförs i enlighet med direktivet utan att bidra till att det kan genomföras. Regeringen följer därför inte Lagrådets förslag i denna del.

För att genomföra artikel 18.3 i CER-direktivet föreslår utredningen att det ska införas reglering i lagen om att en kritisk verksamhetsutövare av särskild europeisk betydelse på begäran av MCF ska tillhandahålla den

riskbedömning som behandlas i avsnitt 8.1 och en förteckning över relevanta vidtagna åtgärder för motståndskraft (jfr avsnitt 8.2). Utredningens förslag skiljer sig i mindre del åt från utformningen av artikel 18.3 a och 18.3 b.

Regeringen konstaterar att MCF, i utredningens förslag till förordning, inte pekas ut som tillsynsmyndighet. Detta bör vara bakgrunden till att utredningen bedömer att det bör införas en särskild skyldighet att lämna ut uppgifter till MCF i enlighet med artikel 18.3 (jfr resonemanget avseende artikel 18.4). Regeringen konstaterar dock, som utredningen, att den myndighet som ska lämna information till kommissionen enligt artikel 18.3 också behöver få del av uppgifter som inte bör lämnas av verksamhetsutövaren (se artikel 18.3 c). Regeringen bedömer, givet detta och det rådgivande uppdragets syfte, att det framstår som en mer ändamålsenlig lösning att det är tillsynsmyndigheten som i stället inhämtar uppgifter enligt artikel 18.3 a och 18.3 b från den kritiska verksamhetsutövaren inom ramen för sin tillsyn. Tillsynsmyndigheten bör, givet sitt uppdrag, också kunna bidra till att bedöma vilken del av riskbedömningen som är relevant och även vilka uppgifter om åtgärder för motståndskraft som är relevanta. Tillsynsmyndigheten kan därefter lämna uppgifterna vidare till den myndighet som regeringen pekar ut som ansvarig för att lämna uppgifter till kommissionen enligt artikel 18.4. Det bör därmed inte införas någon uppgiftsskyldighet för verksamhetsutövaren i förhållande till MCF i lagen.

Det behöver och bör enligt regeringens mening, och till skillnad från utredningens förslag, inte heller införas någon annan reglering gällande rådgivande uppdrag. Som *Transportstyrelsen* för fram kan ett rådgivande uppdrag bli aktuellt även för en kritisk verksamhetsutövare som inte är av särskild europeisk betydelse. Rådgivande uppdrag som har sin grund i artikel 13.4 kräver dock verksamhetsutövarens samtycke och kopplat till denna artikel krävs därför ingen särskild reglering i lagen.

8 Riskbedömning, åtgärder för motståndskraft och incidentrapportering

8.1 Kritiska verksamhetsutövares riskbedömning

Regeringens förslag

En kritisk verksamhetsutövare ska göra en riskbedömning senast nio månader efter det att verksamhetsutövaren har fått del av beslutet om att denne har identifierats som kritisk verksamhetsutövare.

Riskbedömningen ska dokumenteras och innehålla en redogörelse för alla relevanta risker för en incident.

Riskbedömningen ska uppdateras vid behov och minst vart fjärde år.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela ytterligare föreskrifter om riskbedömningen.

Utredningens förslag

Förslaget från utredningen stämmer i allt väsentligt överens med regeringens. Utredningen föreslår att uttrycken risk och riskbedömning ska definieras i lag. Utredningens förslag till bemyndigande avser föreskrifter, inte ytterligare föreskrifter.

Remissinstanserna

Majoriteten av remissinstanserna tillstyrker eller har inga invändningar mot förslaget. *Advokatfirman Kahn Pedersen* anser att tidsfristen bör räknas från när beslutet om identifiering har fått laga kraft. *Region Norrbotten* och *Umeå kommun* anser att den föreslagna tidsfristen kommer att bli svår att hålla.

Ett flertal remissinstanser, bland andra *Svenskt Näringsliv*, *Transportstyrelsen* och Umeå kommun, för fram att det finns behov av att klargöra vad riskbedömningen ska baseras på, hur riskbedömningen ska genomföras och hur allriskperspektivet ska tillämpas. *Energiföretagen Sverige* och *Vattenfall AB* anser att samma tröskelvärden bör användas vid riskbedömningen som vid identifieringen av kritiska verksamhetsutövare och vid bedömningen av om en incident kan medföra en betydande störning. *Svensk Dagligvaruhandel* och *Svensk Handel* bedömer att en riskbedömning med krav på kontinuitetsbedömning skulle vara mer verkningsfullt än utredningens förslag. *Sveriges universitets- och högskoleförbund (SUHF)* efterfrågar förtydliganden gällande om riskbedömningen ska avse hela verksamheten även om tillhandahållandet av den samhällsviktiga tjänsten utgör en avgränsad och mindre del av verksamheten. *Säffle kommun* vill att uttrycket hot används i sammanhanget eftersom alla händelser som kan föranleda en incident inte är riskbaserade, till exempel när det är fråga om aktörsdrivna hot. *Tech Sverige* anser att det är oklart om riskbedömningen ska fokusera på konsekvenser för själva verksamhetsutövaren eller för samhället.

Flera remissinstanser uttalar sig gällande hur ofta riskbedömningen bör uppdateras. *Affärsverket svenska kraftnät*, *E-hälsomyndigheten, Sveriges metereologiska och hydrologiska institut (SMHI)* och Transportstyrelsen anser att en uppdatering vart fjärde år är för sällan. SMHI för fram att den bortre tidsgränsen riskerar att bli normerande. Svensk Dagligvaruhandel anser att fyra år är en rimlig tidsgräns för uppdatering, förutsatt att det inte inträffar något som föranleder uppdatering innan dess, eftersom ett kortare uppdateringsintervall riskerar att skapa en administrativ börda utan motsvarande mervärde. *Länsstyrelsen i Norrbottens län* anser att uppdateringsintervallet bör harmonisera med vad som gäller för risk- och sårbarhetsanalyser enligt förordningen om statliga myndigheters beredskap. *Säkerhetspolisen* anser att riskbedömningen bör uppdateras minst vartannat år, i enlighet med vad som gäller för en säkerhetsskyddsanalys enligt säkerhetsskyddslagen. Umeå kommun anser att det bör ställas krav på systematik i arbetet med att uppdatera riskbedömningarna för att säkerställa att arbetet påbörjas i tid.

Affärsverket svenska kraftnät, Energiföretagen Sverige och Vattenfall AB för fram att det bör tydliggöras vad som kan föranleda ett behov av att uppdatera riskbedömningen i förtid. Vattenfall AB önskar även ett förtydligande av om det är verksamhetsutövaren eller tillsynsmyndigheten som

ska avgöra när det finns behov av att genomföra en uppdatering av riskbedömningen.

Ett antal remissinstanser, bland andra *Länsstyrelsen i Södermanlands län*, *Malmö kommun* och *Myndigheten för psykologiskt försvar*, resonerar kring förhållandet till de riskbedömningar och analyser som ska genomföras enligt annan reglering, exempelvis de som följer av förordningen om statliga myndigheters beredskap, lagen (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap samt NIS 2-direktivet.

Ett flertal remissinstanser, bland andra *Inspektionen för vård och omsorg (IVO), Länsstyrelsen i Västerbottens län* och Säkerhetspolisen, har synpunkter på utredningens förslag till reglering gällande föreskriftsrätt och resonerar kring hur föreskrifterna ska utformas.

Skälen för regeringens förslag

Riskbedömning enligt direktivet

Artikel 2.7 i CER-direktivet definierar riskbedömning som den övergripande processen för att fastställa arten och omfattningen av en risk genom att identifiera och analysera potentiella relevanta hot, sårbarheter och faror som skulle kunna leda till en incident och genom att utvärdera den potentiella förlusten eller störningen i samband med tillhandahållandet av en samhällsviktig tjänst till följd av den incidenten. Uttrycket risk definieras i artikel 2.6 som risk för förlust eller störning orsakad av en incident, som ska uttryckas som en kombination av omfattningen av förlusten eller störningen och sannolikheten för att incidenten inträffar.

Medlemsstaterna ska enligt artikel 12.1 i direktivet säkerställa att kritiska entiteter gör en riskbedömning inom nio månader från mottagandet av den underrättelse som avses i artikel 6.3 och därefter när det är nödvändigt och minst vart fjärde år. I artikeln anges vidare att riskbedömningen ska göras på grundval av medlemsstaternas riskbedömningar och andra relevanta informationskällor samt att den ska göras för att bedöma alla relevanta risker som kan störa tillhandahållandet av deras samhällsviktiga tjänster.

Riskbedömningen ska enligt artikel 12.2 innehålla en redogörelse för alla relevanta risker för naturolyckor och risker orsakade av människan som skulle kunna leda till en incident. Detta inkluderar risker av sektorsövergripande eller gränsöverskridande slag, olyckor, naturkatastrofer, hot mot folkhälsan och hybridhot samt andra antagonistiska hot, inklusive terroristbrott enligt terrorismdirektivet. Riskbedömningen ska enligt samma artikel beakta den grad till vilken andra sektorer som anges i direktivets bilaga är beroende av den samhällsviktiga tjänst som tillhandahålls av den kritiska entiteten och den grad till vilken den kritiska entiteten är beroende av samhällsviktiga tjänster som tillhandahålls av andra entiteter i sådana andra sektorer, inbegripet i angränsande medlemsstater och tredjeländer i förekommande fall.

Uttrycket incident avser enligt artikel 2.3 i CER-direktivet varje händelse som kan medföra en betydande störning, eller som medför en störning, av tillhandahållandet av en samhällsviktig tjänst, inbegripet när den påverkar de nationella system som skyddar rättsstatens principer. I

artikel 15.1 finns en icke uttömmande uppräkning av vad som ska beaktas vid bedömningen av om en störning är betydande.

Med hänvisning till skyldigheten för medlemsstater att säkerställa att kritiska entiteter gör en riskbedömning bör reglering om detta införas i den nya lagen. Frågan om hur pass detaljerad reglering som bör införas i den nya lagen behandlas nedan.

Riskbedömningens innehåll bör i huvudsak regleras på lägre författningsnivå

Utredningen föreslår att det i den nya lagen ska föreskrivas att riskbedömningen ska innehålla en redogörelse för alla relevanta risker som skulle kunna leda till en incident samt att närmare bestämmelser om hur riskbedömningen ska göras och vad den ska innehålla ska införas på lägre författningsnivå än lag. Flera remissinstanser för fram synpunkter gällande utredningens förslag kring riskbedömningens genomförande och innehåll. Bland andra *Svenskt Näringsliv* framhåller att det bland annat finns behov av att tydliggöra vad riskbedömningen ska baseras på, hur riskbedömningen ska genomföras, hur allriskperspektivet ska tillämpas och att allriskperspektivets innebörd behöver konkretiseras.

Utredningens förslag innebär att skyldigheten att göra en riskbedömning regleras på ett övergripande sätt i den föreslagna lagen. De som kan räknas som kritiska verksamhetsutövare bedriver verksamhet inom vitt skilda sektorer och deras verksamheter kan se mycket olika ut. Det är varken lämpligt eller möjligt att fullt ut, på ett sätt som är relevant för samtliga verksamhetsutövare, i den nya lagen reglera vilka riskbedömningar verksamhetsutövarna bör göra. Regeringen uttryckte i lagrådsremissen, mot denna bakgrund och i likhet med utredningen, att det endast bör föreskrivas i lagen att riskbedömningen ska innehålla en redogörelse för alla relevanta risker som skulle kunna leda till en incident.

Lagrådet anser att den aktuella bestämmelsen bör formuleras på så sätt att riskbedömningen ska innehålla en redogörelse för alla relevanta risker som finns för en incident i stället för alla relevanta risker som skulle kunna leda till en incident. Den i lagrådsremissen föreslagna lydelsen kan enligt Lagrådet uppfattas som något av en pleonasm. Regeringen konstaterar att den i lagrådsremissen föreslagna formuleringen följer formuleringen i artikel 12.2 i CER-direktivet, men har förståelse för Lagrådets synpunkt i denna del. Regeringen bedömer dock att det bör göras en omformulering i förhållande till Lagrådets förslag och att det bör vara tillräckligt att ange att riskbedömningen ska innehålla en redogörelse för alla relevanta risker för en incident.

Regeringen konstaterar att förslaget i denna del, på samma sätt som i artikel 12.2 i CER-direktivet, innebär att allriskperspektivet avgränsas till att avse relevanta risker för en incident, det vill säga en händelse som kan medföra en betydande störning, eller som medför en störning av tillhandahållandet av en samhällsviktig tjänst (se artiklarna 2.3 och 15.1). Detta allriskperspektiv innebär att bland annat omvärldsfaktorer samt den kritiska verksamhetsutövarens individuella och sektorsspecifika förutsättningar är relevanta vid riskbedömningen, inklusive vid bedömningen av vilka risker som är relevanta och som skulle kunna leda till en incident. Med hänsyn till detta och till sektorernas bredd bedömer regeringen att

reglering avseende riskbedömningens genomförande och innehåll, inklusive frågor om eventuella tröskelvärden som nämns av *Energiföretagen Sverige* och *Vattenfall AB*, bör regleras närmare i förordning eller i föreskrifter som meddelas av en myndighet. Riskbedömningen bör bland annat, på sätt som kommer till uttryck i artikel 12.2, ta hänsyn till antagonistiska hot. Det finns, givet den i avsnitt 8.3 föreslagna definitionen av uttrycket incident, inte anledning att låta detta komma till uttryck på sätt som *Säffle kommun* föreslår.

Svensk Dagligvaruhandel och *Svensk Handel* för fram att en riskbedömning med krav på kontinuitetsbedömning skulle vara mer verkningsfullt än direktivets allriskperspektiv och utredningens förslag. Riskbedömningen ska dock enligt artikel 12.2 i direktivet innehålla en redogörelse för alla relevanta risker som skulle kunna leda till en incident. Regeringen konstaterar vidare att CER-direktivet syftar till att stärka kritiska entiteters motståndskraft, vilket i artikel 2.2 definieras som en kritisk entitets förmåga att förebygga, skydda mot, reagera på, stå emot, begränsa, absorbera, anpassa sig till och återhämta sig från en incident. Riskbedömningen är enligt direktivet, och även utredningens förslag, en av grundvalarna för de åtgärder för motståndskraft som en kritisk verksamhetsutövare ska vidta. Med hänsyn till detta, och till föreslagen definition av uttrycket motståndskraft i avsnitt 8.2, bör förmågan att bibehålla kontinuiteten i tillhandahållandet av den samhällsviktiga tjänsten vara en central del av de kritiska verksamhetsutövarnas skyldigheter. Regeringen anser att det inte behöver föreskrivas särskilt att riskbedömningen även syftar till att bidra till sådan kontinuitet.

När det gäller *Tech Sveriges* synpunkt att det är oklart om riskbedömningen ska fokusera på konsekvenser för den kritiska verksamhetsutövaren eller för samhället konstaterar regeringen att den i direktivet angivna kopplingen mellan riskbedömningen och direktivets incidentbegrepp bör innebära att bedömningen ska fokusera på den kritiska verksamhetsutövarens tillhandahållande av en samhällsviktig tjänst. De kritiska verksamhetsutövarnas samlade förmåga att tillhandahålla samhällsviktiga tjänster innebär dock givetvis positiva effekter för samhället i stort.

Gällande till exempel *SUHF:s* fråga om riskbedömningen ska avse hela verksamheten även i fall där tillhandahållandet av den samhällsviktiga tjänsten utgör en avgränsad och mindre del av verksamheten konstaterar regeringen att en verksamhetsutövare som utgångspunkt bör omfattas i sin helhet av regleringen (se avsnitt 5.2). Detta förhållningssätt bör gälla även i förhållande till kravet på att göra en riskbedömning. Riskbedömningens fokus ska enligt artikel 12.2 i CER-direktivet vara på sådant som kan leda till en incident, det vill säga händelser som kan medföra en betydande störning eller som medför en störning av tillhandahållandet av en samhällsviktig tjänst (se artikel 2.3 och 2.5). Det bör därmed vara verksamhetsutövarens ansvar att bedöma hur händelser i samtliga verksamhetsgrenar kan påverka den samhällsviktiga tjänsten.

CER-direktivet ställer inte något krav på att riskbedömningen ska dokumenteras utan anger endast att den ska göras. Med hänsyn till att riskbedömningen föreslås beaktas vid vidtagandet av sådana åtgärder för motståndskraft som behandlas i avsnitt 8.2 och till att tillsynsmyndigheten bör kunna granska huruvida en kritisk verksamhetsutövare har uppfyllt

sina skyldigheter kopplat till riskbedömningen bör det i lagen anges att riskbedömningen ska dokumenteras. I den mån det behövs närmare reglering när det gäller kravet på dokumentation bör detta införas på lägre författningsnivå än lag.

De frågor om föreskriftsrättens fördelning och om föreskrifternas utformning som väcks av bland andra *IVO, Länsstyrelsen i Västerbottens län* och *Säkerhetspolisen* behandlas inte i denna proposition eftersom det rör sig om sådant som inte bör regleras i lag.

Utredningen föreslår att uttrycken risk och riskbedömning ska definieras i lagen och regeringen konstaterar att definitionerna i allt väsentligt motsvarar regleringen i CER-direktivet. Uttrycket risk förekommer dock även i utredningens förslag till reglering gällande sanktionsavgiftens storlek och regeringen har svårt att se att uttrycket, när det används i det sammanhanget, skulle ha samma betydelse som kommer till uttryck i den föreslagna definitionen. Regeringen ser inte heller något behov av att uttrycken definieras i lagen. Det är i stället tillräckligt att det på ett tydligt sätt anges i bland annat författningskommentaren vad uttrycken betyder när de används i lagen.

Riskbedömningens förhållande till andra liknande bedömningar

I artikel 12.2 i CER-direktivet anges att om en kritisk entitet, i enlighet med skyldigheter som föreskrivs i andra rättsakter, har gjort andra riskbedömningar eller utarbetat dokument som är relevanta för dess riskbedömning av kritiska entiteter får den använda dessa bedömningar och dokument för att uppfylla kraven i artikeln. När en behörig myndighet utövar sina tillsynsfunktioner får den enligt samma artikel slå fast att en befintlig riskbedömning som gjorts av en kritisk entitet och som omfattar de risker och den beroendegrad som avses i artikeln helt eller delvis uppfyller berörda skyldigheter.

Regeringen bedömer, i likhet med utredningen, att riskbedömningens förhållande till andra liknande bedömningar inte behöver regleras särskilt i lagen eftersom det oavsett får anses ligga i tillsynsmyndighetens uppdrag att beakta sådana vid bedömningen av om en verksamhetsutövare har uppfyllt kraven på riskbedömning eller inte. Regeringen anser vidare att det inte bör anges vilka andra rättsakter som avses eftersom det som ska bedömas är om den kritiska verksamhetsutövarens riskbedömning som sådan uppfyller kraven, inte vilket regelverk som ligger till grund för den.

Angående de synpunkter om behovet av att samordna, slå ihop eller harmonisera uttryck och metodik i förhållande till andra riskbedömningar som bland andra *Länsstyrelsen i Södermanlands län* och *Malmö kommun* för fram konstaterar regeringen att de uttryck som används i den föreslagna lagen när det gäller riskbedömningen överensstämmer med direktivets utformning. Regeringen bedömer att den föreslagna regleringen är nödvändig för att genomföra direktivet i nationell rätt på ett korrekt sätt. En verksamhetsutövare är dock inte förhindrad att genomföra olika riskbedömningar på ett samordnat sätt förutsatt att kraven i den nya lagen uppfylls.

Enligt artikel 12.1 i CER-direktivet ska medlemsstaterna säkerställa att kritiska entiteter gör en riskbedömning inom nio månader från mottagandet av den underrättelse som avses i artikel 6.3 (se avsnitt 6.4) och därefter när det är nödvändigt och minst vart fjärde år. Riskbedömningen ska enligt samma artikel göras på grundval av medlemsstaternas riskbedömningar (se avsnitt 6.1) och andra relevanta informationskällor, för att bedöma alla relevanta risker som kan störa tillhandahållandet av de kritiska entiteternas samhällsviktiga tjänster. Vid bedömningen av om en ny riskbedömning är nödvändig ska de kritiska entiteterna ta hänsyn till sina specifika omständigheter och utvecklingen av riskerna (skäl 28).

Utredningen föreslår att riskbedömningen ska göras senast nio månader efter att verksamhetsutövaren har fått del av beslutet om att den har identifierats som kritisk verksamhetsutövare och att riskbedömningen ska uppdateras vid behov men minst vart fjärde år. När det gäller tidsfristen inom vilken den första riskbedömningen ska vara genomförd för *Region Norrbotten* fram att den är för kort och *Umeå kommun* anser att kravet vid tidsfristens utgång bör vara att verksamhetsutövaren bedriver det systematiska arbete som krävs. Regeringen konstaterar dock att niomånadersfristen, och kravet på att riskbedömningen ska vara gjord inom denna tid, följer direktivets utformning. Riskbedömningen ska dessutom enligt artikel 13.1 i CER-direktivet ligga till grund för de kritiska entiteternas åtgärder för motståndskraft, och för dessa gäller en tidsfrist om tio månader från och med mottaganden av underrättelsen om identifiering som kritisk entitet (se avsnitt 6.2). Det är därmed inte möjligt att föreskriva en längre frist eller att ange att kravet vid fristens utgång ska avse något annat än riskbedömningens genomförande. Vad som avses med uttrycket har fått del av behandlas i avsnitt 6.4.

Regeringen instämmer i utredningens uppfattning att det bör anges att riskbedömningen ska uppdateras vid behov. Gällande det som *Affärsverket svenska kraftnät, Energiföretagen Sverige* och *Vattenfall AB* för fram om behovet av förtydligande av vad som kan utgöra skäl för uppdatering gör regeringen följande överväganden. Bedömningen gällande behovet av en ny riskbedömning innan den bortre tidsfristen löper ut bör, i enlighet med direktivets skäl 28, göras med hänsyn till den kritiska verksamhetsutövarens specifika omständigheter och utvecklingen av riskerna. Bedömningen bör bland annat utgå från dels den aktuella verksamheten och hur denna utvecklas, dels hur riskerna som sådana utvecklas. Den sammantagna innebörden av dessa kriterier är att riskbedömningen ska hållas aktuell. Regeringen anser inte att bedömningskriterierna i skäl 28 behöver anges i lag eftersom de och kravet på aktualitet får anses följa av uttrycket vid behov. Det är varken lämpligt eller möjligt att fullt ut, på ett sätt som är relevant för samtliga verksamhetsutövare, i den nya lagen reglera vad som utgör skäl för en uppdatering. I den mån det för vissa sektorer finns behov av specifika bedömningskriterier bör dessa anges på lägre författningsnivå än lag.

Advokatfirman Kahn Pedersen för fram att den initiala tidsfristen bör räknas från att beslutet om identifiering har fått laga kraft. Detta eftersom beslut om identifiering bör kunna överklagas och eftersom ett beslut om

inhibition i en sådan process i annat fall blir verkningslöst. Regeringen konstaterar dock att det i direktivet anges att niomånadersfristen ska räknas från och med mottagandet av underrättelsen om identifiering. Den av Advokatfirman Kahn Pedersen föreslagna ändringen skulle därmed innebära att direktivet inte genomförs på ett korrekt sätt. Enligt regeringens mening får en försening av verksamhetsutövarens riskbedömning på grund av en överklagandeprocess avseende ett beslut om identifiering i stället beaktas av tillsynsmyndigheten inom ramen för bedömningen av vilka tillsynsåtgärder som bör vidtas i förhållande till verksamhetsutövaren.

Bland andra Affärsverket svenska kraftnät, *SMHI* och *Säkerhetspolisen* anser att en uppdatering vart fjärde år är för sällan med hänsyn till att de risker och hot som ska bedömas kan utvecklas snabbare än så. Som framgår av direktivet och som utredningen konstaterar aktualiseras dock den bortre tidsfristen om fyra år endast när det inte varit nödvändigt att göra en ny riskbedömning innan dess. Frågan om huruvida en riskbedömning i det enskilda fallet borde ha uppdaterats tidigare kan hanteras inom ramen för tillsynen och det finns inte skäl att korta den bortre tidsgränsen för alla verksamhetsutövare. Regeringen bedömer, till skillnad från SMHI, inte heller att det finns en risk för att den bortre tidsgränsen skulle bli normerande. En underlåtenhet att uppdatera en riskbedömning, trots att behov av detta har funnits, kan på sätt som behandlas i avsnitt 11 leda till ingripanden och i vissa fall till höga sanktionsavgifter.

Säkerhetspolisen för även fram att uppdateringsfrekvensen bör harmoniseras med vad som gäller för en säkerhetsskyddsanalys enligt säkerhetsskyddslagen och att det skulle skapa större tydlighet och incitament att nyttja de synergieffekter som uppstår. *Länsstyrelsen i Norrbottens län* för fram en liknande synpunkt gällande risk- och sårbarhetsanalyser enligt förordningen om statliga myndigheters beredskap. Regeringen konstaterar dock, utöver det som har angetts ovan som skäl mot att göra en ändring i förhållande till utredningens förslag, att fristerna räknas från det att verksamhetsutövaren har identifierats som kritisk respektive från det att verksamhetsutövaren har genomfört sin första riskbedömning. En kortare frist skulle därmed inte innebära någon automatisk synkronisering med till exempel fristen för säkerhetsskyddsanalys enligt säkerhetsskyddslagen. Eftersom en kritisk verksamhetsutövare kan välja att genomföra nya riskbedömningar oftare än vart fjärde år kan en synkronisering med liknande bedömningar i stället uppnås på verksamhetsutövarens initiativ.

8.2 Åtgärder för motståndskraft

Regeringens förslag

En kritisk verksamhetsutövare ska vidta lämpliga och proportionella tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa sin motståndskraft (åtgärder för motståndskraft). Åtgärderna för motståndskraft ska vidtas på grundval av verksamhetsutövarens riskbedömning och annan relevant information samt inkludera åtgärder som är nödvändiga för att

1. förhindra att incidenter inträffar,

2. säkerställa ett tillfredsställande fysiskt skydd av lokaler och kritisk infrastruktur,
3. reagera på, stå emot och begränsa konsekvenserna av incidenter,
4. återhämta sig från incidenter,
5. säkerställa en ändamålsenlig hantering av personalsäkerhet, inbegripet att göra en befattningsanalys och genomföra bakgrundskontroller, och
6. öka kunskapen och medvetenheten om åtgärderna för motståndskraft hos berörd personal.

Verksamhetsutövaren ska upprätta och följa en plan för motståndskraft som beskriver de åtgärder som har vidtagits eller ska vidtas enligt ovan.

En kritisk verksamhetsutövare ska utse en kontaktpunkt för tillsynsmyndigheten.

Uttrycket motståndskraft ska i lagen definieras som förmågan att förebygga, skydda mot, reagera på, stå emot, begränsa konsekvenserna av, absorbera, anpassa sig till och återhämta sig från en incident.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela ytterligare föreskrifter om åtgärder för motståndskraft.

Utredningens förslag

Förslaget från utredningen stämmer delvis överens med regeringens. Utredningen föreslår inte att det ska anges att åtgärderna för motståndskraft ska vara lämpliga. Vidare föreslår utredningen att det ska anges att åtgärderna ska utgå från ett allriskperspektiv. Utredningen föreslår att det ska anges att kritiska verksamhetsutövare ska upprätta och tillämpa en plan för motståndskraft eller ett eller flera likvärdiga dokument. Enligt utredningens förslag ska kritiska verksamhetsutövare utse en samverkansansvarig som utgör kontaktpunkt för berörda myndigheter. Utredningen föreslår inte att bemyndigandet att meddela föreskrifter även ska avse regleringen om kontaktpunkten. Utredningens förslag till bemyndigande avser vidare föreskrifter, inte ytterligare föreskrifter.

Remissinstanserna

Majoriteten av remissinstanserna tillstyrker eller yttrar sig inte särskilt över förslaget. *Region Norrbotten* stödjer förslaget om vilka särskilda skyldigheter som en identifierad verksamhetsutövare ska få enligt utredningens förslag. *Region Östergötland* ställer sig bakom förslaget om krav på proportionerliga åtgärder som utgår från ett allriskperspektiv för att säkerställa motståndskraften och att åtgärderna som har vidtagits eller ska vidtas ska beskrivas i en plan.

Livsmedelsverket, *Svensk Dagligvaruhandel* och *Svensk Handel* anser att det bör krävas att åtgärderna för motståndskraft, utöver att de ska vara proportionerliga, är lämpliga. *Trelleborgs kommun* anser att det behövs en klargörande beskrivning av vad ordet motståndskraft har för innebörd.

Flera remissinstanser har synpunkter på vissa uttryck som används i utredningens förslag. Ett stort antal länsstyrelser, bland andra *Länsstyrelserna i Blekinge län, Uppsala län* och *Västmanlands län,* för fram att uttrycket tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa motståndskraft riskerar att skapa begreppsförvirring jämfört

med andra områden och standarder där sådana åtgärder utgör delmängder av säkerhetsåtgärder och bedömer att ett ensande av uttrycken hade varit att föredra. *Länsstyrelsen i Kalmar län* anser att uttrycken organisatoriska, personrelaterade, tekniska och fysiska åtgärder ska användas eftersom dessa är etablerade inom både privat och offentlig sektor. *Säffle kommun* anser att redan etablerade uttryck bör användas framför introduktion av nya såsom säkerhetsmässiga åtgärder.

Några remissinstanser uttalar sig i fråga om allriskperspektivet. *Energiföretagen Sverige* och *Vattenfall AB* efterfrågar ett förtydligande av vilken riskacceptans som ska gälla och därmed när en riskhanteringsåtgärd blir nödvändig att vidta. *Göteborgs kommun* för fram att uttrycket allriskperspektiv sällan används inom ramen för kommuners arbete med civil beredskap och därför behöver definieras tydligare. Kommunen anser även att allriskperspektivet kan innebära en stor ekonomisk påverkan. Enligt *Netnod* bör regleringen, utöver allriskperspektivet och dess fokus på risker som är ”known knowns”, även beakta ”known unknowns” och till viss del ”unknown unknowns”. Netnod anser även att regleringen borde ge verksamhetsutövare konkreta scenarier att utgå från när de genomlyser sina verksamheter.

Vissa remissinstanser har synpunkter på utredningens förslag om vad åtgärderna ska vara nödvändiga för. Energiföretagen Sverige anser att lagen bör inkludera specifika krav på riskhanteringsåtgärder och tydligt ange nivån för dessa åtgärder för att undvika godtyckliga beslut. *GovSec Sweden AB, LawSec Sweden AB* och *Prolegia Research AB* anser att regleringen om åtgärder för personalsäkerhet är för allmänt hållen och att det bör anges att vikten av en deltagandes lojalitet och pålitlighet från säkerhetssynpunkt samt omständigheter som kan antas innebära sårbarheter i säkerhetshänseende ska beaktas. *Malmö kommun* för fram att det skulle kunna förekomma intressekonflikter kring de åtgärder som kritiska verksamhetsutövare ska vidta, exempelvis när det kommer till att säkerställa ett tillfredsställande skydd av lokaler och kritisk infrastruktur i fall där kommunal mark nyttjas av verksamhetsutövare. *Sveriges meteorologiska och hydrologiska institut (SMHI)* betonar att åtgärder för motståndskraft enligt direktivet ska inkludera åtgärder som är nödvändiga för att bland annat förhindra incidenter från att uppstå, med vederbörlig hänsyn till åtgärder för katastrofriskreducering och klimatanpassning.

Ett par remissinstanser uttalar sig om det av utredningen föreslagna kravet på att en kritisk verksamhetsutövare ska utse en samverkansansvarig. *Läkemedelsverket* för fram att det saknas information gällande vilka krav som ska ställas på verksamhetsutövaren avseende kommunikation med tillsynsmyndigheten om den samverkansansvarige. Säffle kommun önskar att det klargörs om samverkansansvarig är detsamma som inriktning- och samordningskontakt enligt ramverket Gemensamma grunder.

Umeå kommun för fram att krav på enskilda planer riskerar att leda till att innebörden, effekten och behovet av att systematiskt arbeta med planen förbises till förmån för att planen ska existera i någon form.

Några remissinstanser uttalar sig gällande de myndighetsuppdrag som utredningen anser bör beslutas. Malmö kommun är positiv till utredningens förslag att Myndigheten för samhällsskydd och beredskap,

numera Myndigheten för civilt försvar, ska få i uppdrag att tillsammans med tillsynsmyndigheterna se över behovet av att anpassa och komplettera stödmaterial för att detta ska kunna användas av kritiska entiteter. *Nynäshamns kommun* är positiv till utredningens förslag att Försvarshögskolan ska få i uppdrag att ta fram och tillhandahålla en utbildning för de som ansvarar för säkerheten hos kritiska verksamhetsutövare.

Skälen för regeringens förslag

Regleringen i direktivet och utredningens förslag

Enligt artikel 13.1 i CER-direktivet ska medlemsstaterna säkerställa att kritiska entiteter vidtar lämpliga och proportionella tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa sin motståndskraft, på grundval av den relevanta information som tillhandahålls av medlemsstaterna om medlemsstaternas riskbedömning samt resultatet av riskbedömningen av kritiska entiteter, inbegripet åtgärder som är nödvändiga för att

- förhindra incidenter från att uppstå, med vederbörlig hänsyn till åtgärder för katastrofriskreducering och klimatanpassning (a)
- säkerställa ett tillfredsställande fysiskt skydd av deras lokaler och kritiska infrastruktur, med vederbörlig hänsyn till exempelvis stängsel, barriärer, verktyg och rutiner för övervakning av områdesgränser, detektionsutrustning och åtkomstkontroller (b)
- reagera på, stå emot och begränsa konsekvenserna av incidenter, med vederbörlig hänsyn till genomförandet av risk- och krishanteringsförfaranden och protokoll samt varningsrutiner (c)
- återhämta sig från incidenter, med vederbörlig hänsyn till åtgärder för driftskontinuitet och identifiering av alternativa försörjningskedjor, för att återuppta tillhandahållandet av den samhällsviktiga tjänsten (d)
- säkerställa en ändamålsenlig hantering av personalsäkerhet, med vederbörlig hänsyn till åtgärder såsom fastställande av kategorier av personal som utför kritiska funktioner, fastställande av åtkomsträttigheter till lokaler, kritisk infrastruktur och känslig information, inrättande av förfaranden för bakgrundskontroller i enlighet med artikel 14 och fastställande av de kategorier av personer som måste genomgå sådana bakgrundskontroller samt fastställande av lämpliga utbildningskrav och kvalifikationer (e)
- öka medvetenheten om de åtgärder som anges i leden a–e hos berörd personal, med vederbörlig hänsyn till utbildningskurser, informationsmaterial och övningar (f).

Vid tillämpning av artikel 13.1 e ska medlemsstaterna, enligt andra stycket i samma artikel, säkerställa att kritiska entiteter beaktar externa tjänsteleverantörers personal vid fastställandet av kategorier av personal som utför kritiska funktioner.

I direktivets skäl 29 anges att åtgärderna ska vara lämpliga och proportionella i förhållande till de risker som den kritiska entiteten ställs inför. Åtgärderna ska vidtas i syfte att förebygga, skydda mot, reagera på, stå emot, begränsa, absorbera, anpassa sig till och återhämta sig efter en incident. De kritiska entiteterna bör vidta dessa åtgärder i enlighet med

direktivet, men den detaljerade utformningen och omfattningen av åtgärderna bör avspegla de olika risker som varje kritisk entitet har identifierat inom ramen för sin riskbedömning av kritiska entiteter och särdragen hos den entiteten på ett ändamålsenligt och proportionerligt sätt. Kraven på att vidta åtgärder för motståndskraft ska enligt artikel 6.3 gälla från och med tio månader efter dagen för underrättelsen om att entiteten har identifierats som kritisk (se avsnitt 8.2).

I skäl 3 i direktivet nämns bland annat att det finns en ökad fysisk risk på grund av naturkatastrofer och klimatförändringen, som leder till att extrema väderhändelser blir allt vanligare och mer omfattande och medför långsiktiga förändringar i genomsnittliga klimatförhållanden som kan minska kapaciteten, effektiviteten och livslängden för vissa typer av infrastruktur om det inte vidtas klimatanpassningsåtgärder.

Med uttrycket motståndskraft avses enligt artikel 2.2 i direktivet en kritisk entitets förmåga att förebygga, skydda mot, reagera på, stå emot, begränsa, absorbera, anpassa sig till och återhämta sig från en incident. Uttrycket incident avser enligt artikel 2.3 varje händelse som kan medföra en betydande störning, eller som medför en störning, av tillhandahållandet av en samhällsviktig tjänst, inbegripet när den påverkar de nationella system som skyddar rättsstatens principer.

Enligt utredningens förslag ska kritiska verksamhetsutövare vidta tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa sin motståndskraft. Åtgärderna ska utgå från ett allriskperspektiv och vara proportionella i förhållande till risken. De ska vidtas på grundval av verksamhetsutövarens riskbedömning samt annan relevant information och inkludera åtgärder som är nödvändiga för att

1. förhindra incidenter från att uppstå,
2. reagera på, stå emot och begränsa konsekvenserna av incidenter,
3. återhämta sig från incidenter,
4. säkerställa ett tillfredsställande fysiskt skydd av lokaler och kritisk infrastruktur,
5. säkerställa en ändamålsenlig hantering av personalsäkerhet, och
6. öka kunskapen om åtgärderna för motståndskraft hos berörd personal.

Kritiska verksamhetsutövare bör vara skyldiga att vidta åtgärder för att säkerställa sin motståndskraft

Utredningen föreslår att de kritiska verksamhetsutövarna ska vidta åtgärder för att säkerställa sin motståndskraft samt att åtgärderna bland annat ska vara nödvändiga för att uppnå de i artikel 13.1 a–f i CER-direktivet uppräknade syftena. Utredningens uppräkning följer i huvudsak direktivets utformning. I utredningens förslag nämns dock inte de särskilda hänsyn och de exempel på åtgärder som anges i artikel 13.1 a–f. Utredningen anser att åtgärderna för motståndskraft bör regleras närmare i föreskrifter som meddelas av regeringen eller en myndighet.

Regeringen konstaterar att åtgärdernas syfte enligt artikel 13.1 i CER-direktivet bör vara att säkerställa den kritiska entitetens motståndskraft som uttrycket motståndskraft definieras i artikel 2.2. När det gäller definitionen av uttrycket motståndskraft för *Trelleborgs kommun* fram att det behövs en klargörande beskrivning av vad det omfattar. Utredningen berör inte uttrycket närmare. Regeringen konstaterar att uttrycket definieras i

artikel 2.2 i CER-direktivet som en kritisk entitets förmåga att förebygga, skydda mot, reagera på, stå emot, begränsa, absorbera, anpassa sig till och återhämta sig från en incident. När det gäller innebörden av nyss nämnda uttryck, till exempel absorbera, konstaterar regeringen att varken direktivet eller betänkandet innehåller någon klargörande beskrivning av uttryckens innebörd. Det bör inte heller krävas något förtydligande i lagen utan det räcker enligt regeringens mening att konstatera att det handlar om att vidta åtgärder som krävs för att begränsa konsekvenserna av en inträffad incident och för att förhindra en potentiell incident. Regeringen bedömer, i likhet med utredningen, att det finns ett värde i att använda uttrycket motståndskraft i lagen på samma sätt som i CER-direktivet. Regeringen bedömer att definitionen, tillsammans med definitionen av uttrycket incident, ger uttrycket en tillräckligt tydlig innebörd. Regeringen eller den myndighet som regeringen bestämmer bör dessutom, i linje med utredningens förslag, få meddela ytterligare föreskrifter om åtgärderna för motståndskraft.

Innebörden av tekniska, säkerhetsmässiga och organisatoriska åtgärder

Ett stort antal länsstyrelser, däribland *Länsstyrelserna i Blekinge län, Uppsala län* och *Västmanlands län,* invänder mot att uttrycket tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa motståndskraft används i lagen och anser att uttrycket bör anpassas till andra områden och standarder där det mer omfattande uttrycket säkerhetsåtgärder används. Regeringen konstaterar dock att den av utredningen föreslagna formuleringen stämmer överens med direktivet och bedömer att formuleringen bör användas i den nya lagen. Att ensa begreppsanvändningen väger enligt regeringens mening inte tyngre än ett korrekt genomförande av direktivet. Av samma skäl innebär *Länsstyrelsen i Kalmar läns* och *Säffle kommuns* synpunkter, om att andra uttryck bör användas i stället, inte att det finns skäl att frångå utredningens förslag.

Regeringen konstaterar dessutom att närliggande uttryckssätt förekommer i cybersäkerhetslagen. I 2 kap. 3 § cybersäkerhetslagen anges att verksamhetsutövare ska vidta tekniska, driftsrelaterade och organisatoriska åtgärder för att skydda berörda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. Paragrafen genomför artikel 21.1–21.3 i NIS 2-direktivet där motsvarande uttryckssätt finns. I fråga om innebörden av uttrycket tekniska, driftsrelaterade och organisatoriska åtgärder anges i förarbetena till cybersäkerhetslagen att det bland annat kan röra sig om åtgärder till skydd mot obehöriga personer samt till skydd för lokaler och utrustning av betydelse för säkerheten. Det kan också bland annat handla om att verksamhetsutövaren fördelar ansvar, roller och mandat i organisationen samt utarbetar rutiner och genomför uppföljning och utvärdering (se prop. 2025/26:28 s. 244). Motsvarande tolkning bör göras i detta sammanhang. Mer detaljerad vägledning bör ges i förordning eller i föreskrifter som meddelas av en myndighet.

Vad bör åtgärderna inbegripa som ett minimum?

Regeringen gör bedömningen att samtliga krav enligt artikel 13.1–3 i CER-direktivet är att anse som åtgärder för motståndskraft i direktivets mening. Enligt artikel 13.1 ska åtgärderna för motståndskraft inbegripa

åtgärder som är nödvändiga för att uppnå vissa syften och uppfylla vissa mål. *Energiföretagen Sverige* för fram att lagen, till skillnad från utredningens förslag, i stället bör inkludera specifika krav på åtgärder. *GovSec Sweden AB*, *LawSec Sweden AB* och *Prolegia Research AB* anser till exempel att den föreslagna regleringen om åtgärder för personalsäkerhet är för allmänt hållen. Regeringen konstaterar att regleringen kommer att gälla många olika typer av verksamheter och att olika sektorer kan ha olika behov och förutsättningar. Av den anledningen bör mer detaljerad reglering gällande vilka åtgärder som bör vidtas inte införas i lagen.

Åtgärderna för motståndskraft bör i stället, i linje med utredningens förslag men också på ett sätt som i större utsträckning motsvarar direktivets utformning, inkludera åtgärder som är nödvändiga för att förhindra att incidenter inträffar och för att säkerställa ett tillfredsställande fysiskt skydd av lokaler och kritisk infrastruktur. Åtgärder för motståndskraft bör också inbegripa åtgärder som är nödvändiga för att reagera på, stå emot och begränsa konsekvenserna av incidenter samt återhämta sig från incidenter. Åtgärderna bör därutöver inbegripa åtgärder som är nödvändiga för att säkerställa en ändamålsenlig hantering av personalsäkerhet, inbegripet att göra en befattningsanalys och genomföra bakgrundskontroller, och för att öka kunskapen och medvetenheten hos berörd personal om åtgärderna för motståndskraft (se vidare avsnitt 9). Regeringen bedömer, i likhet med utredningen och till skillnad mot *SMHI*, att regleringen i artikel 13.1 i CER-direktivet inte behöver överföras i sin helhet till den nya lagen samt att den närmare preciseringen av de syften och åtgärder som följer av paragrafen bör regleras på lägre författningsnivå än lag. Enligt regeringens bedömning bör de särskilda hänsyn och de exempel som anges i artikel 13.1 ändå beaktas vid tillämpningen av lagen.

Lagrådet uppfattar direktivet som att det ska krävas mera än medvetenhet och kunskap hos personalen om åtgärderna för motståndskraft. I själva verket torde personalens förmåga att delta i åtgärderna vara en avgörande förutsättning för att syftet med lagen ska uppnås. Då räcker det enligt Lagrådet knappast att personalen känner till eller är medveten om vad som krävs i sammanhanget. Lagrådet föreslår mot denna bakgrund att verksamhetsutövaren ska vidta åtgärder som syftar till att öka personalens förmåga att delta i åtgärderna för motståndskraft.

Skyldigheten att vidta åtgärder för motståndskraft gäller för verksamhetsutövaren och inte för personalen. Att öka kunskapen och medvetenheten hos berörd personal innebär dock i sig att man ökar personalens förmåga att bidra till att verksamhetsutövaren kan vidta rätt slags åtgärder. Det är otydligt vilka ytterligare åtgärder som en verksamhetsutövare skulle vara skyldig att vidta om Lagrådets förslag genomförs. Regeringen finner inte heller att det finns skäl att införa en reglering som innebär att man frångår direktivets utformning och utredningens förslag. Regeringen genomför därför inte Lagrådets förslag i denna del.

När det gäller verksamhetsutövarens skyldighet att förhindra att incidenter inträffar handlar det om att vidta åtgärder för att minska risken för att det inträffar en händelse som kan medföra en betydande störning, eller som medför en störning, av tillhandahållandet av den samhällsviktiga

tjänsten. I enlighet med artikel 13.1 bör verksamhetsutövaren inom ramen för denna skyldighet vidta åtgärder för katastrofriskreducering och klimatanpassning. Katastrofriskreducering kan handla om att verksamhetsutövaren investerar i förebyggande åtgärder som i sig skapar ändamålsenlig motståndskraft, till exempel genom att satsa på att förbättra fysiska strukturer genom att förstärka byggnader. Klimatanpassning kan kräva såväl organisatoriska och planeringsmässiga som tekniska och fysiska åtgärder, till exempel robust infrastruktur för energiförsörjning och transporter men också åtgärder som innebär beredskap för exempelvis översvämningsrisk vid extrema skyfall, höga temperaturer, ras, skred och erosion, bränder och vattenbrist.

Lagrådet anser i denna del att skyldigheten bör formuleras som att verksamhetsutövaren ska förebygga att incidenter inträffar. Regeringen, som konstaterar att orden förebygga och förhindra inte är synonymer, bedömer dock att uttrycket förhindra bör användas eftersom det följer CER-direktivets formulering.

I fråga om skyldigheten att säkerställa ett tillfredsställande fysiskt skydd av lokaler och kritisk infrastruktur kan det röra sig om att sätta upp stängsel och andra slags fysiska barriärer, att ha metoder och rutiner för övervakning av olika slags områden samt att använda sig av detektionsutrustning och olika slags åtkomstkontroller, till exempel i form av användarautentisering och behörighetsstyrning.

Att verksamhetsutövaren ska kunna reagera på, stå emot och begränsa konsekvenserna av incidenter bör bland annat inbegripa att ha en förmåga att genomföra risk- och krishanteringsförfaranden på ett ändamålsenligt sätt samt att ha goda rutiner för att hantera incidenter.

När det gäller förmågan och skyldigheten att kunna återhämta sig från incidenter bör verksamhetsutövaren exempelvis vidta åtgärder för driftskontinuitet eller, med ett mer etablerat uttryck, kontinuitetshantering. Kontinuitetshantering innebär att verksamhetsutövaren ska planera för och ha förmåga att upprätthålla sin verksamhet på en acceptabel nivå oavsett vilken störning den utsätts för eller om en kris inträffar. Det kan till exempel röra sig om störningar som innebär att personalen inte kan komma till arbetet, att lokalerna inte går att använda, att strömavbrott inträffar eller att leveranser av viktiga varor och tjänster inte når verksamhetsutövaren. Verksamhetsutövaren kan inom ramen för denna skyldighet bland annat behöva identifiera alternativa försörjningskedjor som krävs för att kunna återuppta tillhandahållandet av en samhällsviktig tjänst. *Lagrådet* föreslår en mindre omformulering i denna del. Regeringen bedömer inte att Lagrådets förslag innebär någon särskild fördel, till exempel i tydlighetshänseende, och genomför därför inte förslaget.

Att säkerställa en ändamålsenlig hantering av personalsäkerhet har en koppling till de förslag som behandlas i avsnitt 9. Det rör sig bland annat om att fastställa kategorier av personal som utför kritiska funktioner och genomförande av bakgrundskontroller samt att fastställa åtkomstkontroll till lokaler, kritisk infrastruktur och känslig information. Verksamhetsutövaren bör också införa ändamålsenliga krav på utbildning och kvalifikationer. Kravet i andra stycket i artikel 13.1 i direktivet, om att de kritiska verksamhetsutövarna bör beakta externa tjänsteleverantörers personal vid fastställandet av kategorier av personal som utför kritiska funktioner, behandlas till viss del i avsnitt 9.1 och 9.2.

Verksamhetsutövarens skyldighet att öka kunskapen och medvetenheten hos berörd personal om ovan nämnda slags åtgärder kan handla om att se till att personalen genomgår utbildning och tar del av informationsmaterial men också om att genomföra eller delta i övningar som ökar kunskapen och medvetenheten. Det kan handla om att verksamhetsutövaren själv anordnar utbildningar och övningar och tar fram informationsmaterial men det kan också handla om att ta del av sådant som anordnas eller tillhandahålls av en extern aktör, till exempel en myndighet.

Som målsättningsbegrepp för åtgärderna för motståndskraft anger både artikel 13.1 i CER-direktivet och utredningen att åtgärderna ska säkerställa motståndskraft och att åtgärder som är nödvändiga för att uppnå angivna syften och uppfylla angivna mål ska vidtas. Varken direktivet eller utredningen går närmare in på vad uttrycken säkerställa och nödvändiga för innebär i fråga om hur långt verksamhetsutövarens skyldigheter sträcker sig. Med hänvisning till kraven på att åtgärderna enligt artikel 13 också ska vara lämpliga och proportionella kan uttrycken dock inte tolkas som att en verksamhetsutövare har en skyldighet att till exempel se till att det aldrig inträffar en incident i verksamheten. Huruvida en verksamhetsutövare har vidtagit tillräckliga åtgärder för motståndskraft får bedömas i varje enskilt fall och blir en fråga för tillsynsmyndigheten och ytterst en domstol.

Lagrådet för fram att det bör anges i lagen att åtgärderna ska syfta till att uppfylla de aktuella målen och uppnå de angivna syftena i stället för att de ska vara nödvändiga för desamma. Förändringen bör enligt Lagrådet ske eftersom den bättre speglar den ambitionsnivå som är avsedd. Regeringen har viss förståelse för Lagrådets synpunkt och tydliggjorde i lagrådsremissen, av samma skäl som Lagrådet för fram och på det sätt som framgår ovan, hur uttrycket nödvändiga för ska tolkas. Uttrycket nödvändiga för används dock i direktivet och det finns en skillnad mellan uttrycken syftar till och nödvändiga för. Regeringen bedömer inte att det finns skäl att avvika från direktivet i denna del och bedömer att ambitionsnivån har tydliggjorts på ett ändamålsenligt sätt. Regeringen följer därför inte Lagrådets förslag i denna del.

Malmö kommun för fram att det skulle kunna förekomma intressekonflikter kring de åtgärder som kritiska verksamhetsutövare ska vidta, exempelvis i samband med åtgärder för skydd av lokaler och kritisk infrastruktur i fall där kommunal mark nyttjas av verksamhetsutövare. Kommunen anser att det är oklart hur samverkan är tänkt att ske och hur tillsynsmyndigheten beaktar detta vid tillsyn. Regeringen konstaterar att kravet på att vidta säkerhetsåtgärder inte innebär en rätt att vidta åtgärder på annans egendom. Vilka åtgärder som kan krävas i enskilda fall av en verksamhetsutövare får, som anges ovan, bedömas av tillsynsmyndigheten och ytterst en domstol.

I artikel 16 i CER-direktivet anges att medlemsstaterna, för att främja en enhetlig tillämpning av direktivet, när det är användbart och utan att föreskriva eller gynna användningen av en viss typ av teknik, ska uppmuntra användningen av europeiska och internationellt erkända standarder och tekniska specifikationer som är relevanta för åtgärder för säkerhet och motståndskraft som är tillämpliga på kritiska entiteter. Detta är inte något som kräver reglering i lag (jfr prop. 2025/26:28 s. 95 f.).

Några remissinstanser, däribland Malmö kommun och *Nynäshamns kommun*, uttalar sig om myndighetsuppdrag som utredningen anser bör beslutas och kring andra åtgärder som faller utanför vad som kan behandlas i denna proposition.

Åtgärderna bör vara lämpliga och proportionella

Artikel 13.1 i CER-direktivet anger att de kritiska entiteternas åtgärder för att säkerställa sin motståndskraft ska vara lämpliga och proportionella. Utredningen bedömer att kravet på lämplighet inte bör framgå av lagen eftersom det anges att åtgärderna ska vara proportionella i förhållande till risken. *Livsmedelsverket*, *Svensk Dagligvaruhandel* och *Svensk Handel* gör en annan bedömning.

Uttrycken lämplighet och proportionalitet avser i regel två olika slags bedömningskriterier i författningssammanhang. Som Livsmedelsverket för fram bör uttrycket lämplighet i detta sammanhang anses innebära att åtgärderna ska vara relevanta och effektiva för att hantera de identifierade riskerna medan proportionalitet avser att åtgärderna ska stå i rimlig proportion till riskens allvarlighetsgrad. Vid bedömningen av om åtgärderna är proportionella ska hänsyn bland annat tas till verksamhetsutövarens grad av riskexponering och storlek samt till sannolikheten för att incidenter inträffar och till incidenternas allvarlighetsgrad, inbegripet deras samhälleliga och ekonomiska konsekvenser. Det kan därmed vara så att en åtgärd är proportionerlig men inte lämplig och vice versa. Även om proportionalitets- och lämplighetsbedömningen i många fall kan ge samma resultat, delar regeringen uppfattningen att det finns en skillnad mellan dessa bedömningar och att båda bedömningarna bör ingå. Detta bör komma till uttryck i lagen.

Det krävs ingen reglering om allriskperspektivet i detta sammanhang

Utredningen föreslår att det ska anges att åtgärderna för att stärka motståndskraft ska utgå från ett allriskperspektiv. Några remissinstanser, bland andra *Göteborgs kommun*, begär förtydliganden och har synpunkter på förslaget i denna del.

Enligt artikel 13.1 i CER-direktivet och enligt utredningens förslag ska åtgärderna för motståndskraft vidtas bland annat på grundval av den kritiska entitetens riskbedömning. Eftersom riskbedömningen i sig, på sätt som behandlas i avsnitt 8.1, föreslås utgå från ett allriskperspektiv är det överflödigt att införa reglering som innebär att även åtgärderna för motståndskraft i sig ska utgå från ett sådant perspektiv. Utredningens förslag i denna del bör därför inte genomföras.

Kritiska verksamhetsutövare bör upprätta en plan för motståndskraft

I artikel 13.2 i CER-direktivet anges att medlemsstaterna ska säkerställa att kritiska entiteter har och tillämpar en plan för motståndskraft eller ett eller flera likvärdiga dokument med en beskrivning av de åtgärder som vidtagits enligt artikel 13.1. Om den kritiska entiteten har utarbetat dokument eller vidtagit åtgärder i enlighet med skyldigheter som anges i andra rättsakter som är relevanta för de åtgärder som avses i artikel 13.1 får den använda dessa dokument och åtgärder för att uppfylla berörda krav. I direktivets skäl 30 anges att för effektivitetens och ansvarsutkrävandets

skull bör de kritiska entiteterna beskriva de åtgärder som de vidtar tillräckligt detaljerat för att dessa syften avseende effektivitet och ansvarsutkrävande ska uppnås, med hänsyn till de identifierade riskerna, i en plan för motståndskraft eller i ett eller flera dokument som är likvärdiga med en plan för motståndskraft, och tillämpa den planen i praktiken.

Utredningens förslag innebär att skyldigheten att upprätta en plan för motståndskraft regleras översiktligt i lagen och att reglering om hur planen ska upprättas och vad den ska innehålla förs in på lägre författningsnivå. Regeringen ställer sig bakom denna utformning av regleringen. Regeringen instämmer även i utredningens uppfattning att det inte behöver regleras särskilt att tillsynsmyndigheten kan bedöma att andra dokument eller åtgärder innebär att den kritiska verksamhetsutövaren uppfyller kravet på en plan för motståndskraft. Det behöver inte regleras i lag att skyldigheten kan avse ett eller flera likvärdiga dokument. När det gäller *Umeå kommuns* synpunkt kring behovet av systematiskt arbete ställer sig regeringen bakom utredningens slutsats att arbetet med att upprätta och uppdatera riskbedömningar, att vidta åtgärder för motståndskraft samt att ta fram planer för motståndskraft innebär att det ställs krav på ett systematiskt arbetssätt.

Kritiska verksamhetsutövare bör utse en kontaktpunkt

Enligt artikel 13.3 i CER-direktivet ska medlemsstaterna säkerställa att varje kritisk entitet utser en sambandsansvarig eller motsvarande som kontaktpunkt med de berörda myndigheterna.

I utredningens förslag anges bland annat att skyldigheten att utse en sambandsansvarig innebär att verksamhetsutövaren ska utse någon som är ansvarig för samverkan med berörda myndigheter. I betänkandet beskrivs den skyldighet som följer av artikel 13.3 som att kritiska verksamhetsutövare ska utse en samverkansansvarig som kontaktpunkt för berörda myndigheter. Innebörden av bestämmelsen bör enligt utredningen förstås som att det är en funktion för samverkan med myndigheter som ska upprätthållas.

Regeringen instämmer i utredningens uppfattning att den skyldighet som följer av artikel 13.3 i CER-direktivet bör regleras i lagen. Regeringen instämmer även i att regleringen bör innebära att kritiska verksamhetsutövare kan välja mellan att peka ut en specifik individ eller en funktion för att fullgöra uppgiften och att verksamhetsutövaren ansvarar för att upprätthålla kontinuitet samt att detta inte behöver anges i lagen. Regeringen konstaterar dock att uttrycken samband och samverkan inte har samma innebörd. Med samband avses något som anknyter eller förbinder vissa företeelser. Samverkan avser i stället gemensamt handlande för ett visst syfte. Den svenska språkversionen av direktivet anger att den sambandsansvarige ska vara en kontaktpunkt med de berörda myndigheterna. I den engelska språkversionen av direktivet används uttrycket liaison, vilket kan översättas till förbindelse eller samband, samt att denna ”liaison officer” ska vara ”the point of contact with the competent authorities”. Regeringen bedömer sammantaget att den funktion som avses i artikel 13.3 tar sikte på samband, inte samverkan. Det bör, enligt regeringens bedömning, vidare vara tillräckligt att i lagen ange att det är en kontaktpunkt som ska utses.

Utredningen föreslår att funktionen ska vara en kontaktpunkt för ”berörda myndigheter”, vilket är motsvarande uttryck som förekommer i artikel 13.3 i CER-direktivet. Uttrycket berörda myndigheter förekommer, förutom i artikel 13.3, i artikel 9.1 i direktivet och avser då situationen att en medlemsstat inrättat mer än en behörig myndighet enligt direktivet och att medlemsstaten i ett sådant fall tydligt ska fastställa uppgifterna för var och en av de berörda myndigheterna. I till exempel den engelska språkversionen används uttrycket competent authorities i artikel 13.3. Regeringen anser att det, vid en systematisk och ändamålsenlig tolkning av direktivet, rätteligen bör vara de behöriga myndigheterna som avses i artikel 13.3, det vill säga den eller de tillsynsmyndigheter som har pekats ut enligt artikel 9 och som ska utöva tillsyn över den reglering som antagits med stöd av direktivet (se vidare avsnitt 10). Det bör därför sammanfattningsvis framgå av lagen att en kritisk verksamhetsutövare ska utse en kontaktpunkt för tillsynsmyndigheten.

Läkemedelsverket för fram att det exempelvis kan vara lämpligt att kräva att kontaktuppgifter till samverkansansvarig ska meddelas tillsynsmyndigheten och att dessa uppgifter ska hållas aktuella. Regeringen instämmer i att det finns behov av ytterligare reglering gällande funktionen som kontaktpunkt, exempelvis vilka kontaktuppgifter som verksamhetsutövarna ska lämna till tillsynsmyndigheterna. Med hänsyn till att förutsättningar och behov kan skilja sig åt mellan sektorerna bör detta dock regleras på lägre författningsnivå än lag. När det gäller *Säffle kommuns* synpunkt, om att kopplingen till ramverket Gemensamma grunder bör tydliggöras, konstaterar regeringen att Gemensamma grunder är ett aktörsgemensamt ramverk för ledning och samverkan. Ramverket hjälper offentliga aktörer att samverka effektivt, dela lägesbilder och skapa en gemensam inriktning och samordning vid samhällsstörningar. Det står en kritisk verksamhetsutövare fritt att peka ut en person eller funktion som kontaktpunkt enligt flera olika regel- och ramverk, förutsatt att detta inte äventyrar det samband som krävs för att upprätthålla en ändamålsenlig kontaktpunkt gentemot tillsynsmyndigheterna på det sätt som krävs enligt den nya lagen.

Lagrådet anser att det bör övervägas om den aktuella paragrafen bör föregås av en paragrafrubrik av lydelsen Kontaktpunkt i stället för att placeras under rubriken Åtgärder för motståndskraft. Lagrådet bedömer att utseendet av en kontaktpunkt inte omedelbart framstår som en åtgärd för motståndskraft. Med hänsyn bland annat till att kravet på att utse en kontaktpunkt regleras i artikel 13.3 i CER-direktivet, vars rubrik är Kritiska entiteters åtgärder för motståndskraft, bedömer dock regeringen att utseendet av en kontaktpunkt bör anses som en åtgärd för motståndskraft. Regeringen genomför därför inte Lagrådets förslag till ändring i denna del.

Regeringens förslag

En kritisk verksamhetsutövare ska till den myndighet som regeringen bestämmer anmäla sådana incidenter som medför eller kan medföra en betydande störning i den kritiska verksamhetsutövarens tillhandahållande av en samhällsviktig tjänst.

Uttrycket incident ska i lagen avse en händelse som kan medföra en betydande störning eller som medför en störning i den kritiska verksamhetsutövarens tillhandahållande av en samhällsviktig tjänst.

En incidentanmälan ska lämnas så snart det kan ske, dock senast 24 timmar efter det att verksamhetsutövaren har fått kännedom om incidenten. Senast en månad efter incidentanmälan ska verksamhetsutövaren lämna en rapport om incidenten till samma myndighet.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela ytterligare föreskrifter om vad som utgör en incident och om incidentrapporteringen.

Utredningens förslag

Förslaget från utredningen stämmer delvis överens med regeringens. Kritiska verksamhetsutövare ska enligt utredningens förslag utan onödigt dröjsmål rapportera incidenter som medför eller kan medföra en betydande störning i tillhandahållandet av samhällsviktiga tjänster. En första rapport ska lämnas inom 24 timmar efter det att verksamhetsutövaren fått kännedom om en incident. En detaljerad rapport ska enligt utredningens förslag lämnas senast en månad efter att den första rapporten lämnades. Utredningen föreslår att bemyndigandet ska innebära rätt att få meddela föreskrifter om vad som utgör en betydande störning och om incidentrapporteringen.

Remissinstanserna

Majoriteten av remissinstanserna tillstyrker eller har inga synpunkter på förslaget. Några remissinstanser för fram synpunkter på definitionen av uttrycket incident. *Försäkringskassan* anser att det bör förtydligas vilka typer av incidenter som omfattas av rapporteringskraven. *Förvaltningsrätten i Linköping* noterar att den föreslagna definitionen av incident inte fullt ut stämmer överens med direktivets definition. *Region Östergötland* och *Stockholm Vatten och Avfall AB* anser att innebörden av uttrycket behöver förtydligas.

Flera länsstyrelser, däribland *Länsstyrelserna i Uppsala län* och *Västra Götalands län*, samt *Vattenfall AB* anser att innebörden av uttrycket kan medföra behöver förtydligas för att undvika tolkningssvårigheter.

Ett antal remissinstanser uttalar sig om tidsfristerna för incidentrapporteringen och om rapporternas innehåll. *Drivkraft Sverige* anser att tidsfristen bör börja löpa först när det står klart att incidenten omfattas av rapporteringskravet. *E-hälsomyndigheten* anser att tiden för att lämna en detaljerad rapport bör ändras från en månad till 30 dagar. *Energiföretagen Sverige* för fram att den initiala incidentrapporteringen bör ske på en

övergripande nivå samt att det bör anges att rapportering ska ske inom 24 timmar när så är möjligt. *Salems kommun*, *Stockholms kommun*, *Säffle kommun* och *Växjö kommun* resonerar kring behovet av resurser och utvecklade processer och system för att kunna hålla 24-timmarsfristen. *Region Gotland, Svensk Dagligvaruhandel* och *Svensk Handel* tillstyrker förslaget om en tidsfrist på 24 timmar för den initiala incidentrapporteringen. Vattenfall AB anser att direktivets formulering att incidentrapportering ska ske inom 24 timmar när det är operativt möjligt bör framgå av lagen. *Tranportstyrelsen* anser dock att en sådan reglering skulle leda till tolkningssvårigheter.

Affärsverket svenska kraftnät, Länsstyrelsen i Norrbottens län, Svenskt Vatten och Transportstyrelsen för fram att det behöver förtydligas hur förslaget förhåller sig till annan reglering om incidentrapportering, till exempel säkerhetskyddsregleringen.

SJ AB och *Tågföretagen* anser att det bör förtydligas vilken kritisk verksamhetsutövare som ska rapportera en incident och till vem rapporten ska lämnas om incidenten medför eller kan medföra en betydande störning i en sammansatt samhällsviktig tjänst som järnvägstrafik, där flera olika aktörer samspelar under pågående leverans.

Flera remissinstanser har synpunkter på sådant som utredningen föreslår ska regleras på lägre författningsnivå än lag. Bland andra Drivkraft Sverige, Energiföretagen Sverige*, Myndigheten för civilt försvar (MCF)*, *Region Gotland* och Salems kommun uttalar sig om uttrycket betydande störning och anser att innebörden av uttrycket behöver förtydligas. Ett antal remissinstanser, däribland *Pensionsmyndigheten* och *Sveriges meteorologiska och hydrologiska institut* för fram synpunkter gällande föreskriftsrättens fördelning.

Flera remissinstanser, däribland *Livsmedelsverket*, *Luleå kommun*, Länsstyrelsen i Norrbottens län, *Svenskt Vatten* och *Stiftelsen för Internetinfrastruktur* har synpunkter på utredningens förslag till förordning i fråga om att incidentrapporteringen ska ske till MCF och inte till tillsynsmyndigheten.

Skälen för regeringens förslag

Uttrycket incident och incidentrapportering enligt direktivet

Enligt artikel 15.1 i CER-direktivet ska medlemsstaterna säkerställa att kritiska entiteter utan onödigt dröjsmål lämnar in en anmälan till den behöriga myndigheten om incidenter som medför en betydande störning eller kan medföra en betydande störning i tillhandahållandet av samhällsviktiga tjänster. För att fastställa om en störning är betydande ska i synnerhet beaktas antal och andel användare som berörs av störningen, störningens varaktighet och det geografiska område som påverkas av störningen med beaktande av huruvida området är geografiskt isolerat.

Enligt artikel 15.4 ska den berörda behöriga myndigheten, så snart som möjligt efter en incidentanmälan, ge den berörda kritiska entiteten relevant uppföljningsinformation, inklusive information som skulle kunna hjälpa den kritiska entiteten att reagera ändamålsenligt på incidenten i fråga. En incident definieras i artikel 2.3 som varje händelse som kan medföra en betydande störning, eller som medför en störning, av tillhandahållandet av

en samhällsviktig tjänst, inbegripet när den påverkar de nationella system som skyddar rättsstatens principer.

Enligt skäl 33 i direktivet bör en mekanism för anmälan av vissa incidenter inrättas för att göra det möjligt för de behöriga myndigheterna att reagera snabbt och ändamålsenligt på incidenter och få en heltäckande bild av verkningarna, arten och de möjliga konsekvenserna av samt orsaken till incidenter som de kritiska entiteterna hanterar. De kritiska entiteterna bör utan onödigt dröjsmål lämna in en anmälan till de behöriga myndigheterna om incidenter som medför en betydande störning eller kan medföra en betydande störning av tillhandahållandet av samhällsviktiga tjänster. Om detta inte är operativt omöjligt bör de kritiska entiteterna lämna in en första anmälan senast 24 timmar efter det att de har fått kännedom om en incident. Den första anmälan bör endast innehålla den information som är absolut nödvändig för att göra den behöriga myndigheten medveten om incidenten och för att den kritiska entiteten vid behov ska kunna söka hjälp. En sådan anmälan bör om möjligt innehålla information om den förmodade orsaken till incidenten. Medlemsstaterna bör säkerställa att kravet på att lämna in denna första anmälan inte avleder den kritiska entitetens resurser från verksamhet som rör incidenthantering, vilken bör prioriteras. Den första anmälan bör i förekommande fall åtföljas av en detaljerad rapport senast en månad efter incidenten. Den detaljerade rapporten bör komplettera den första anmälan och ge en mer komplett bild av incidenten.

Vad bör räknas som en incident enligt lagen?

Några remissinstanser, till exempel *Försäkringskassan*, efterfrågar en tydligare definition av uttrycket incident. För att undvika att väsentliga händelser förbises eller att det sker en överrapportering ser Försäkringskassan behov av tydliga bestämmelser angående vilka typer av incidenter som omfattas av rapporteringskravet. Utredningen föreslår att definitionen av incident i stort ska följa direktivets definition i artikel 2.3 men att den del i direktivets definition som handlar om påverkan på de nationella systemen som skyddar rättsstatens principer inte ska framgå av lagen. Som *Förvaltningsrätten i Linköping* påpekar innebär detta att den av utredningen föreslagna definitionen inte överensstämmer fullt ut med direktivets definition.

Regeringen ställer sig huvudsakligen bakom utredningens förslag till definition och konstaterar att den av utredningen utelämnade exemplifieringen, oavsett om den anges i lagen eller inte, bör beaktas vid bedömningen av om en händelse utgör en incident. När det gäller definitionen i övrigt bedömer regeringen att varken direktivet eller utredningens förslag är tydligt när det gäller frågan om incidenten ska påverka den kritiska verksamhetsutövarens egna tillhandahållande av en samhällsviktig tjänst eller om det även kan röra sig om en händelse i dennes verksamhet som enbart påverkar en annan verksamhetsutövares tillhandahållande av en samhällsviktig tjänst. Hur uttrycket incident definieras i lagen påverkar, förutom vilka incidenter som ska rapporteras, bland annat vad verksamhetsutövaren ska beakta i sin riskbedömning och vilka åtgärder som verksamhetsutövaren ska vidta som en del av sina åtgärder för motståndskraft. En utebliven incidentrapportering föreslås

kunna leda till ingripanden i form av bland annat höga sanktionsavgifter (se avsnitt 11).

I lagrådsremissen uttryckte regeringen att ett tillägg borde göras i förhållande till utredningens förslag och att direktivets utformning talar för att det ska röra sig om en händelse som påverkar den kritiska verksamhetsutövarens egna tillhandahållande av en samhällsviktig tjänst. Verksamhetsutövare skulle annars i varje enskilt fall behöva göra svåra bedömningar och ha särskilt god insyn i andra aktörers möjligheter att tillhandahålla samhällsviktiga tjänster. Regeringen uttryckte även att såväl artikel 15.1 och 15.4 som skäl 33, som bland annat fokuserar på den kritiska entitetens behov av hjälp att hantera incidenten och att den behöriga myndigheten ska få en heltäckande bild av verkningarna, talade för en sådan tolkning. Om en händelse i den kritiska verksamhetsutövarens verksamheten inte får någon effekt på tillhandahållandet av den egna samhällsviktiga tjänsten utan enbart på någon annan aktörs tillhandahållande av en samhällsviktig tjänst kan verksamhetsutövaren knappast bidra med information som leder till en sådan heltäckande bild. I lagrådsremissen uttryckte regeringen också att det i många fall dessutom bör vara så att den andra aktören har identifierats som en kritisk verksamhetsutövare och därmed själv omfattas av rapporteringsskyldigheten.

Lagrådet anser att det föreslagna tillägget i definitionen av uttrycket incident, som alltså innebär att det ska röra sig om en händelse som påverkar den kritiska verksamhetsutövarens tillhandahållande av en samhällsviktig tjänst, bör utgå. Lagrådet pekar bland annat på att det i den föreslagna regleringen om identifiering av kritiska verksamhetsutövare anges att det ska göras en bedömning av incidentens effekt i förhållande till verksamhetsutövarens tillhandahållande av en eller flera samhällsviktiga tjänster men också i förhållande till tillhandahållandet av andra samhällsviktiga tjänster som är beroende av den eller de samhällsviktiga tjänster som verksamhetsutövaren tillhandahåller. Regeringen konstaterar att den i lagrådsremissen föreslagna konstruktionen innebär en viss överlappning men att en sådan också följer med direktivets utformning. Det bör vidare noteras att uttrycket incident också är av central betydelse för att avgöra vilka risker som ska redovisas i den kritiska verksamhetsutövarens riskbedömning (avsnitt 8.1) och vilka åtgärder för motståndskraft som en kritisk verksamhetsutövare är skyldig att vidta (avsnitt 8.2). En definition som formuleras i enlighet med Lagrådets förslag skulle kunna tolkas som att en kritisk verksamhetsutövare, i bland annat sin riskbedömning, behöver beakta händelser som påverkar eller kan påverka andra verksamhetsutövare på ett sätt som varken skulle vara proportionerligt eller ändamålsenligt. Regeringen bedömer att en i viss mån överlappande reglering är att föredra framför en sådan ordning och följer därför inte Lagrådets förslag om omformulering av definitionen av uttrycket incident.

Utredningen föreslår att regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om vad som utgör en betydande störning och om incidentrapporteringen. Utredningen föreslår att definitionen av uttrycket betydande störning i förordning ska följa direktivets utformning (se artikel 15.1). Utredningen föreslår att definit-

ionen bör kompletteras av föreskrifter meddelade av regeringen eller en myndighet.

Med hänsyn till olikheterna mellan de sektorer, undersektorer och kategorier av entiteter som anges i bilagan till CER-direktivet och som ska omfattas av lagens skyldigheter uttryckte regeringen i lagrådsremissen att närmare reglering i linje med utredningens förslag bör införas på lägre författningsnivå än lag. En sådan ordning innebär att skyldigheterna enligt lagen bättre kan anpassas till olika sektorer och samhällsviktiga tjänster och även till andra omständigheter. Regeringen uttryckte dock att föreskriftsrätten bör avse ytterligare föreskrifter och vad som utgör en incident snarare än vad som utgör en betydande störning.

Lagrådet för fram att det är formellt möjligt att införa ett sådant bemyndigande som regeringen föreslår men anser att definitionen av uttrycket incident bör göras mer detaljerad i lagen eller i författningskommentaren bland annat eftersom bemyndigandet – som Lagrådet har uppfattat det – ska ge regeringen eller den myndighet regeringen bestämmer möjlighet att inte bara precisera vad som utgör en incident utan även att utvidga eller inskränka definitionen. Lagrådet anser att det bör tydliggöras vilken nivå på risken som behövs för att det ska vara fråga om en incident och även i vad mån kravet beträffande risknivån är beroende av omfattningen av den störning som skulle kunna bli resultatet av en incident.

Med hänsyn till att uttrycket incident har en koppling inte endast till vilka incidenter som ska rapporteras utan även bland annat till vilka åtgärder för motståndskraft som en kritisk verksamhetsutövare behöver vidta enligt lagen vidhåller regeringen, trots Lagrådets synpunkter, att föreskriftsrätten i aktuell del bör avse vad som utgör en incident snarare än enbart vad som utgör en betydande störning och att det inte är lämpligt att göra definitionen mer detaljerad i lag. Berörda föreskrifter bör exempelvis kunna avse den närmare innebörden av uttrycket kan medföra och skillnaden mellan uttrycken betydande störning och störning. Föreslaget bemyndigande innebär en möjlighet att meddela ytterligare föreskrifter, det vill säga föreskrifter som kompletterar regleringen i lagen i aktuellt avseende.

Det saknas med hänvisning till förslaget om reglering på lägre författningsnivå anledning att närmare beröra vad uttrycket betydande störning innebär och rapporteringens innehåll. Remissinstansernas synpunkter, däribland *Energiföretagens* och *MCF:s*, kommer därmed inte att behandlas inom ramen för denna proposition. Frågan om föreskriftsrättens fördelning, som bland andra *Pensionsmyndigheten* väcker, kan regleras i förordning och är därför inte heller föremål för behandling i denna proposition. Förhållandet mellan uttrycken betydande störning och betydande störande effekt samt Lagrådets synpunkter när det gäller användningen av uttrycken i lagen behandlas i avsnitt 6.3.

Vilka incidenter bör rapporteras?

Som både direktivet och utredningens förslag anger är rapporteringsskyldigheten knuten till uttrycket betydande störning. I artikel 15.1 i CER-direktivet anges parametrar som i synnerhet ska tas i beaktande vid fastställandet av om en störning är betydande. Med hänsyn till att uttrycket

incident också omfattar händelser som orsakar en störning, jämfört med en betydande störning, faller därmed inte alla incidenter in under rapporteringsskyldigheten.

Som framgår av direktivet gäller skyldigheten att rapportera en incident både när det har inträffat en betydande störning i tillhandahållandet av en samhällsviktig tjänst och när en incident kan medföra en betydande störning. Det behöver alltså inte ha inträffat en betydande störning avseende tillhandahållandet av tjänsten utan det är tillräckligt att en sådan kan uppstå. Det krävs dock en viss sannolikhet för att en betydande störning kan inträffa till följd av incidenten för att verksamhetsutövaren ska vara skyldig att rapportera den.

Lagrådet anser att det i stället bör anges att det rör sig om incidenter som har medfört eller hade kunnat medföra en betydande störning i verksamhetsutövarens tillhandahållande av en samhällsviktig tjänst. Detta skulle dock innebära ett avsteg från formuleringen i direktivet (se artikel 15.1). Därtill bedömer regeringen att det vid rapporteringstillfället kan handla om att bedöma en pågående incident. I en sådan situation handlar det om att pröva om incidenten kan medföra en betydande störning jämfört med att pröva om den kunde ha medfört en sådan. Lagrådets förslag bör därför inte genomföras.

Uttrycket kan medföra, som till exempel *Vattenfall AB* bedömer behöver förklaras närmare, används även i direktivets definition av uttrycket incident. Direktivet innehåller dock inte några närmare bedömningskriterier gällande uttrycket. Kravet på viss sannolikhet bör enligt regeringens mening inte sättas för högt. Regeringen anser att kravet på att rapportera incidenter bör omfatta incidenter som, vid en sådan inledande och preliminär bedömning av bland annat incidentens art, orsak och omfattning samt av verksamhetsutövarens förutsättningar att exempelvis reagera på, stå emot och begränsa konsekvenserna av incidenten, bedöms kunna medföra en betydande störning. Vid bedömningen av om en incident kan medföra en betydande störning bör det även beaktas om den aktuella händelsen typiskt sett hade orsakat en betydande störning om den inte hade avvärjts. I den mån det finns behov av sektorsspecifika kriterier i form av exempelvis tröskelvärden eller modifierade sannolikhetskrav bör sådana, som anges ovan, införas på lägre författningsnivå än lag.

Tidsfrister för rapportering

Enligt artikel 15.1 i CER-direktivet ska medlemsstaterna säkerställa att kritiska entiteter anmäler relevanta incidenter utan onödigt dröjsmål. I samma artikel anges att medlemsstaterna ska säkerställa att de kritiska entiteterna, om det inte är operativt omöjligt för dem, lämnar in en första anmälan inom 24 timmar efter det att de har fått kännedom om en incident. Denna anmälan ska, i förekommande fall, följas av en detaljerad rapport senast en månad därefter. Direktivets skäl 33 anger att den första anmälan endast bör innehålla den information som är absolut nödvändig för att göra den behöriga myndigheten medveten om incidenten och för att den kritiska entiteten vid behov ska kunna söka hjälp. Medlemsstaterna bör säkerställa att kravet på att lämna in denna första anmälan inte avleder den kritiska entitetens resurser från verksamhet som rör incidenthantering, vilken bör prioriteras.

Utredningen föreslår att en första rapport ska lämnas inom 24 timmar efter det att verksamhetsutövaren fått kännedom om en incident och att en detaljerad rapport ska lämnas senast en månad efter att den första rapporten lämnades. Regeringen bedömer att uttrycket första rapport bör ersättas och att det i lagen bör anges att det rör sig om en anmälan av en incident eftersom detta stämmer bättre överens med formuleringen i artikel 15 i CER-direktivet. Utredningen bedömer att det i lagen inte bör anges att verksamhetsutövaren kan avstå från att rapportera inom 24 timmar om det är operativt omöjligt. Detta eftersom det, enligt utredningen, skulle innebära tolkningssvårigheter och att tidskravet riskerar att sättas ur spel. *Transportstyrelsen* instämmer i denna uppfattning men till exempel *Vattenfall AB* för fram att kravet på att det ska vara operativt möjligt att göra en anmälan bör framgå av lagen.

Regeringen bedömer, liksom utredningen, att tidsfristerna för rapporteringen bör följa direktivet. Regeringen bedömer att huvudregeln bör uttryckas som så att en anmälan ska göras så snart det kan ske. Uttrycket så snart det kan ske bör innebära att en anmälan som huvudregel ska göras i omedelbar anslutning till att verksamhetsutövaren får kännedom om en incident. När det gäller den föreslagna tidsfristen för anmälan följer denna direktivets utformning. Att tidsfristen, som bland annat *Salems kommun*, *Säffle kommun* och *Växjö kommun* påpekar, kan vara utmanande att hålla och sannolikt medför behov av effektiva system och processer för incidenthantering innebär inte att det finns möjlighet att frångå direktivet. Det finns därutöver ett värde i att en incident anmäls så fort som möjligt, även om kraven på innehållet i en sådan anmälan bör anpassas för att i möjligaste mån se till att anmälningsskyldigheten inte påverkar verksamhetsutövarens arbete med att hantera incidenten. Om det uppstår en situation då det objektivt inte är möjligt att anmäla en incident bör det inte bli tal om någon ingripandeåtgärd från tillsynsmyndighetens sida på grund av att tidsfristen har överskridits. Det behöver inte införas någon reglering om att kravet på anmälan inte gäller om det är objektivt omöjligt att göra en sådan.

Drivkraft Sverige för fram att fristen bör börja löpa först när verksamhetsutövarens analys befäst att incidenten är av kritisk karaktär. Regeringen konstaterar att direktivet innebär att tidsfristen börjar löpa redan med utgångspunkt i när den kritiska entiteten har fått kännedom om incidenten. Det är förenligt med syftet med anmälan, att snabbt uppmärksamma den mottagande myndigheten på incidenten och ge verksamhetsutövaren möjlighet att vid behov få hjälp, att det inte kan ställas krav på en mer omfattande utredning.

När det gäller *E-hälsomyndighetens* förslag om att tidsfristen för att lämna en rapport bör ändras från en månad till 30 dagar konstaterar regeringen dels att fristen om en månad följer direkt av direktivets utformning, dels att en frist på en månad förenklar tillämpningen eftersom lagen (1930:173) om beräkning av lagstadgad tid då är tillämplig.

Övriga frågor om incidentrapportering

Utredningen bedömer att övriga frågor med koppling till rapporteringen, bland annat innehållet i rapporten och till vilken myndighet rapportering ska ske bör regleras på lägre författningsnivå än lag. Med hänsyn till att

olika sektorer kan ha olika behov och förutsättningar gör regeringen samma bedömning. Synpunkterna från bland annat *Livsmedelsverket* kopplat till hur rapporteringen ska ske behandlas därför inte i denna proposition.

SJ AB och *Tågföretagen* för fram att det bör förtydligas vilken kritisk verksamhetsutövare som ska rapportera en incident och till vem rapporten ska lämnas om incidenten medför eller kan medföra en betydande störning i en sammansatt samhällsviktig tjänst. Enligt regeringens förslag ska en kritisk verksamhetsutövare till den myndighet som regeringen bestämmer rapportera sådana incidenter som medför eller kan medföra en betydande störning i den kritiska verksamhetsutövarens tillhandahållande av en samhällsviktig tjänst. Regeringen konstaterar att detta krav även gäller i förhållande till tjänster som består av flera samverkande delar. Det innebär att varje kritisk verksamhetsutövare som omfattas av rapporteringsskyldigheten ska göra en anmälan och lämna en rapport.

När det gäller *Affärsverket svenska kraftnäts*, *Länsstyrelsen i Norrbottens läns*, *Svenskt Vattens* och *Transportstyrelsens* synpunkter gällande behovet av förtydligande kring hur förslaget förhåller sig till annan reglering om incidentrapportering konstaterar regeringen att varken artikel 1.3 i CER-direktivet eller den föreslagna lagen ger utrymme för undantag från kraven på incidentrapportering på den grunden att det finns bestämmelser med motsvarande verkan i annan reglering (se avsnitt 5.4.2). Den föreslagna lagens krav på att anmäla och rapportera incidenter gäller därför även om det föreligger sådana krav enligt annan reglering. Den föreslagna lagens förhållande till cybersäkerhetslagen behandlas i avsnitt 5.4.2. Gällande Svenskt Vattens synpunkt att rapporteringsskyldigheten kan komma i konflikt med säkerhetsskyddsregleringen konstaterar regeringen att undantag föreslås i avsnitt 5.4.3 gällande verksamhetsutövare som bedriver säkerhetskänslig verksamhet. Skyldigheterna att lämna uppgifter enligt lagen föreslås inte heller gälla uppgifter som är säkerhetsskyddsklassificerade enligt säkerhetsskyddslagen (se avsnitt 5.4.4)

9 Bakgrundskontroll och befattningsanalys

9.1 Skyldigheten att genomföra bakgrundskontroll

Regeringens förslag

En kritisk verksamhetsutövare ska säkerställa att en person som deltar i eller ska delta i verksamheten, i den mån det följer av verksamhetsutövarens befattningsanalys, har genomgått en bakgrundskontroll. Bakgrundskontrollen ska bestå i att personen styrker sin identitet och genomgår en registerkontroll.

Utredningens förslag

Förslaget från utredningen stämmer delvis överens med regeringens. Utredningen föreslår att syftet med en bakgrundskontroll ska anges i lagen. Utredningen föreslår att en person som deltar i eller ska delta i verksamheten, och som har genomgått en bakgrundskontroll, även ska ha bedömts som lämplig för sådant deltagande. Utredningen föreslår vidare att det ska regleras i lagen att endast den som har genomgått bakgrundskontroll och bedömts lämplig ska få anställas eller på annat sätt delta i aktuell verksamhet.

Remissinstanserna

Många remissinstanser är positiva till förslaget om att införa ett system för bakgrundskontroller, däribland *Arbetsgivarverket*, *Livsmedelsverket*, *Post- och telestyrelsen (PTS)*, *Svenskt Vatten* och *Sveriges meteorologiska och hydrologiska institut (SMHI)* samt flera kommuner och regioner. Arbetsgivarverket anser att bakgrundskontroller är viktiga verktyg för att stärka säkerhetsarbetet och minska risken för otillåten påverkan, och framhåller vikten av att statliga arbetsgivare, inte minst mot bakgrund av vilken verksamhet som bedrivs inom sektorn offentlig förvaltning, ges verktyg för att stärka säkerhetsarbetet avseende redan anställda genom exempelvis registerkontroll under anställning. Flera remissinstanser, bland andra *Enköpings kommun* och *Luleå kommun*, bedömer att förslaget kommer att leda till fler administrativa uppgifter, ökade kostnader och en viss integritetspåverkan.

Många remissinstanser yttrar sig särskilt över bakgrundskontrollens föreslagna innehåll och omfattning. Ett större antal remissinstanser, däribland *Affärsverket svenska kraftnät, Finansiell ID-Teknik BID AB (BID), Strålsäkerhetsmyndigheten, Svenskt Näringsliv, Säkerhetsbranschen, Säkerhetspolisen* samt flera länsstyrelser och kommuner, anser att den valda modellen inte är ändamålsenlig och efterfrågar en mer omfattande bakgrundskontroll. *Försäkringskassan* framhåller bland annat att det inte nödvändigtvis är så att de överväganden som gör sig gällande för en lagstiftning med ett brett tillämpningsområde, och som berör många företag och myndigheter, är samma som om det hade gjorts en bedömning för de olika verksamhetsutövarna var för sig. *Gävle kommun* önskar en differentiering i fråga om kravet på förnyad bakgrundskontroll likt säkerhetsskyddslagens olika klasser, där den lägsta klassen innebär kontroll av engångskaraktär eller motsvarande och högre klasser medför kontinuerlig kontroll. *Malmö kommun* bedömer att kravet på bakgrundskontroller i förhållande till uppdragstagare och leverantörer kan behöva regleras vid upphandling och ställer sig frågande till hur kraven kan uppfyllas vid redan ingångna avtal. Bland andra PTS anser att kritiska verksamhetsutövare inom sektorn digital infrastruktur bör omfattas av motsvarande krav på bakgrundskontroller. *Vetenskapsrådet* ställer sig bakom att en mindre ingripande lösning valts än den som gäller enligt säkerhetsskyddslagen och anser att en lämplig avvägning mellan skyddet för den personliga integriteten och behovet av bakgrundskontroll uppnås med förslaget.

Flera remissinstanser, däribland *Energiföretagen Sverige, Göteborgs kommun, Landsorganisationen i Sverige (LO)* och *Transportstyrelsen*,

anser att det är otydligt hur lämplighetskriteriet i utredningens förslag ska tolkas och efterfrågar vägledning. LO anser att det även måste finnas regler för hur beslutsunderlaget ska se ut och för hanteringen av sådana känsliga personuppgifter som kan förekomma. Vidare anser LO att det måste finnas en möjlighet för den enskilde som är föremål för en bakgrundskontroll att överklaga ett beslut som går ut på att denne inte är lämplig. LO påpekar också att det saknas en arbetsrättslig analys i betänkandet. *Almega Säkerhetsföretagen*, *Bevakningsbranschens Yrkes- och Arbetsmiljönämnd (BYA)* och *Svenska Transportarbetarförbundet* bedömer på liknande vis att ett beslut om någons lämplighet bör kunna överklagas.

Några remissinstanser, däribland Energiföretagen Sverige, Göteborgs kommun, *Svensk Dagligvaruhandel* och *Vattenfall AB*, lyfter utmaningen med att kontrollera äktheten av handlingar och bland annat handlingar från andra länder. *Drivkraft Sverige* och *Innovations- och kemiindustrierna i Sverige (IKEM)* önskar ett förtydligande av hur systemet med bakgrundskontroller ska fungera beträffande personer som bor eller är medborgare i ett land utanför EU. Drivkraft Sverige anser att det bör införas en mekanism som gör det möjligt att erkänna eller ge tillgång till bakgrundskontroller som har genomförts i en annan medlemsstat. IKEM ser en risk för att personer med avgörande kompetens, men med medborgarskap i ett land utanför EU, inte kan verka fritt med de ökade kraven på bakgrundskontroll. BID anser att kraven på hur styrkande av identitet ska ske bör kompletteras i föreskrifter på lägre författningsnivå än lag och har synpunkter på vilka identitetshandlingar som bör godtas. Säkerhetspolisen ser utmaningar med att säkerställa identiteter i de fall den prövade har tilldelats ett samordningsnummer.

BID och Malmö kommun föreslår, för att inte urholka uttrycket bakgrundskontroll, att uttrycket registerkontroll ska användas för viss del av kontrollen som ska ske. Göteborgs kommun anser att användningen av uttrycket bakgrundskontroll leder till otydlighet, eftersom det används inom flera olika områden och ofta saknar en definition i lagtext.

Ett antal remissinstanser, däribland Almega Säkerhetsföretagen, BYA och Svenska Transportarbetarförbundet, har synpunkter som gäller utredningens förslag till förordning. Till exempel *Statens energimyndighet (Energimyndigheten)* har synpunkter gällande utredningens förslag om föreskriftsrätt. Flera remissinstanser, däribland *Domstolsverket,* Drivkraft Sverige, Livsmedelsverket, *Region Stockholm* och Transportstyrelsen, vill se en djupare analys av hur den nya lagen förhåller sig till säkerhetsskyddslagen och cybersäkerhetslagen. Bland andra Säkerhetspolisen nämner fler utredningar som rör utökade registerkontroller till skydd för olika verksamheter och framhåller behovet av att ta ett samlat grepp om frågorna.

Skälen för regeringens förslag

Krav på bakgrundskontroll i direktivet kräver lagreglering

Av artikel 13.1 i CER-direktivet följer en skyldighet för medlemsstaterna att säkerställa att kritiska entiteter vidtar tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa sin motståndskraft (se vidare avsnitt 8.2). Detta inbegriper enligt artikel 13.1 e åtgärder som är nödvändiga för att säkerställa en ändamålsenlig hantering av personal-

säkerhet, med vederbörlig hänsyn till åtgärder såsom fastställande av kategorier av personal som utför kritiska funktioner, fastställande av åtkomsträttigheter till lokaler, kritisk infrastruktur och känslig information, inrättande av förfaranden för bakgrundskontroller i enlighet med artikel 14 och fastställande av de kategorier av personer som måste genomgå sådana bakgrundskontroller samt fastställande av lämpliga utbildningskrav och kvalifikationer. Vid fastställandet av kategorier av personal som utför kritiska funktioner ska enligt samma artikel även externa tjänsteleverantörers personal beaktas.

I artikel 14 i CER-direktivet finns bestämmelser om bakgrundskontroller av personer som deltar i en kritisk entitets verksamhet. Artikeln fastställer att medlemsstaterna ska ange de villkor enligt vilka en kritisk entitet, i vederbörligen motiverade fall och med beaktande av medlemsstaternas riskbedömning, får ansöka om bakgrundskontroller av personer som innehar känsliga roller i eller till förmån för den kritiska entiteten, särskilt när det gäller den kritiska entitetens motståndskraft (a) eller som är bemyndigade att direkt eller på distans få tillgång till den kritiska entitetens lokaler eller dess informations- eller kontrollsystem, inbegripet när det gäller den kritiska entitetens säkerhet (b) eller som övervägs för rekrytering till tjänster som omfattas av de kriterier som anges i led a eller b (c). Bakgrundskontrollen ska enligt artikel 14.3 åtminstone bekräfta identiteten på den person som är föremål för bakgrundskontrollen och kontrollera uppgifter ur kriminalregistret för den personen avseende brott som är relevanta för en viss tjänst.

Som utredningen konstaterar lämnar direktivet inte något utrymme för medlemsstaterna att välja om bakgrundskontroller ska införas i nationell rätt eller inte, men direktivet ger visst handlingsutrymme vad gäller kontrollernas innehåll och utformning. För att Sverige ska kunna uppfylla sina skyldigheter enligt CER-direktivet bör det, som utredningen föreslår, i den nya lagen införas viss reglering om bakgrundskontroller.

Vilka uttryckssätt bör användas för de kontroller som ska ske enligt lagen?

Utredningen föreslår att kontroller enligt den nya lagen ska bestå av tre delar: identitetskontroll, kontroll av belastningsregistret i visst avseende och en lämplighetsbedömning. Utredningen föreslår att uttrycket bakgrundskontroll ska användas som ett samlingsbegrepp för identitets- och registerkontrollen. Bland andra *Malmö kommun* föreslår, för att inte urholka uttrycket bakgrundskontroll, att uttrycket registerkontroll i stället ska användas i den nya lagen. Regeringen konstaterar att det inte finns någon enhetlig definition av uttrycket bakgrundskontroll i svensk rätt. Uttrycket används dock ofta för att beskriva kontroller som görs i syfte att till exempel bedöma en persons lämplighet inför en anställning, skydda verksamheter mot infiltration av organiserad brottslighet, motverka penningtvätt eller förhindra att olämpliga personer anställs för arbete med utsatta grupper. En bakgrundskontroll kan exempelvis inkludera styrkande av en persons identitet, kreditupplysning och granskning av ekonomisk historik och bolagsengagemang. Den kan även inkludera en kontroll av uppgifter ur belastningsregistret och misstankeregistret (se dir. 2025:83 s. 2).

Uttrycket bakgrundskontroll förekommer i CER-direktivet och det finns en fördel med att använda det uttrycket även i den nya lagen. Uttrycket bör i den nya lagen användas som ett samlingsbegrepp för den identitetskontroll och registerkontroll som föreslås ske enligt lagen. Eftersom det blir tydligt vad som avses med uttrycket bakgrundskontroll i lagen anser regeringen inte att den omständigheten att uttrycket används i andra sammanhang med annan innebörd talar emot att uttrycket används som *Göteborgs kommun* framför. Det är också ofrånkomligt att vissa uttryck används i olika regleringar med olika innebörd och detta behöver inte innebära någon svårighet i tillämpningen av de olika regelverken.

Lagrådet ställer frågan om vad som ska gälla för bakgrundskontroller av verksamhetsutövaren själv när denne inte är en juridisk person. Lagrådet konstaterar att lagtexten i och för sig inte hindrar att en verksamhetsutövare som är en fysisk person kontrolleras, men det är enligt Lagrådet svårt att se hur det ska gå till i praktiken. Regeringen konstaterar att angiven slags kontroll, för att vara ändamålsenlig, skulle kräva att en extern aktör ansvarar för bakgrundskontrollen av verksamhetsutövaren. En sådan kontroll krävs inte enligt CER-direktivet och föreslås inte heller införas inom ramen för denna proposition (se vidare avsnitt 9.3).

Obligatorisk bakgrundskontroll

Utredningens förslag innebär att det i den nya lagen införs en skyldighet för kritiska verksamhetsutövare att säkerställa att vissa kategorier av personer har genomgått bakgrundskontroll. Artikel 14.1 i CER-direktivet innebär en skyldighet för medlemsstaterna att ange de villkor enligt vilka en kritisk entitet ”får” ansöka om bakgrundskontroller av vissa i direktivet utpekade kategorier av personer. Enligt regeringen är en möjlig tolkning att direktivet endast innebär en skyldighet för medlemsstaterna att tillse att berörda verksamhetsutövare ges möjlighet, men ingen skyldighet, att genomföra sådana kontroller. Mot en sådan tolkning talar dock utformningen av artikel 13.1 e i direktivet.

I artikel 13.1 e listas åtgärder som kritiska entiteter ska vidta för att säkerställa en ändamålsenlig hantering av personalsäkerhet, inbegripet inrättande av förfaranden för bakgrundskontroller i enlighet med artikel 14, och fastställande av de kategorier av personer som måste genomgå sådana bakgrundskontroller. Artikel 13.1 e ger därmed, enligt regeringens mening, inget utrymme för att välja om sådana kontroller ska genomföras. Vidare framgår av direktivet att det är ett växande problem att anställda och uppdragstagare till exempel kan missbruka sina åtkomsträttigheter för skadliga ändamål (skäl 32). Regeringen anser därför att lagen, i likhet med vad utredningen föreslår och trots det som *IKEM* framför i fråga om konsekvenserna för vissa arbetstagare, bör utformas så att kritiska verksamhetsutövare har en skyldighet att säkerställa att bakgrundskontroller har gjorts i vissa fall. I vilka fall bakgrundskontroller ska genomföras bör utgå ifrån den befattningsanalys som behandlas närmare i avsnitt 9.2.

PTS bedömer att kritiska verksamhetsutövare inom den digitala sektorn bör omfattas av krav på bakgrundskontroller. Denna synpunkt bemöts i avsnitt 5.4.1.

Vid all form av bakgrundskontroll aktualiseras en avvägning mellan syftet med bakgrundskontrollen, som är att skydda viss verksamhet, och skyddet för den personliga integriteten hos den individ som kontrolleras. Av artikel 14.2 i CER-direktivet följer att bakgrundskontroller ska vara proportionella och strikt begränsade till vad som är nödvändigt. Där anges vidare att de enbart ska utföras i syfte att utvärdera en potentiell säkerhetsrisk för den berörda kritiska entiteten. Enligt artikel 14.3 ska en bakgrundskontroll åtminstone bekräfta identiteten på den person som är föremål för bakgrundskontrollen och kontrollera uppgifter ur kriminalregistret för den personen avseende brott som är relevanta för en viss tjänst. Regeringen, liksom utredningen, tolkar direktivets krav på proportionalitet som att ingreppet i den enskildes personliga integritet inte ska vara större än vad som behövs för att syftet med bakgrundskontrollen ska kunna uppnås. Detta ansluter till den ordning som redan följer av regeringsformen och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen), vilken gäller som lag i Sverige.

Av 2 kap. 6 § andra stycket regeringsformen följer att var och en gentemot det allmänna är skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. Skyddet enligt 2 kap. 6 § andra stycket regeringsformen är dock inte absolut utan får begränsas genom lag i den utsträckning som medges i 21–24 §§. Begränsningar får göras endast för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle. En begränsning får dessutom aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den och inte heller sträcka sig så långt att den utgör ett hot mot den fria åsiktsbildningen såsom en av folkstyrelsens grundvalar. Begränsningen får inte göras enbart på grund av politisk, religiös, kulturell eller annan sådan åskådning (2 kap. 21 §).

Regleringen i 2 kap. 6 § andra stycket regeringsformen tar sikte på sådana åtgärder som den enskilde själv inte kan få kännedom om eller påverka genom ett krav på frivilligt godkännande. Om åtgärderna förutsätter den enskildes godkännande, kan det intrång som åtgärden innebär normalt inte anses vara av så allvarlig beskaffenhet att det bör omfattas av ett stärkt grundlagsskydd. Kravet på samtycke bör bedömas på samma sätt som motsvarande krav enligt bestämmelsen om förbud mot åsiktsregistrering i 2 kap. 3 § första stycket regeringsformen. Bestämmelsens tillämpningsområde är begränsat till sådana intrång som innebär övervakning eller kartläggning av en enskilds personliga förhållanden (se vidare prop. 2009/10:80 s. 178 f.).

Avgörande för om en åtgärd ska anses innebära övervakning eller kartläggning är inte dess huvudsakliga syfte utan vilken effekt åtgärden har. Vad som avses med övervakning respektive kartläggning får bedömas med utgångspunkt från vad som enligt normalt språkbruk läggs i dessa begrepp. Vid bedömning av vilka åtgärder som kan anses utgöra ett betydande intrång ska både åtgärdens omfattning och arten av det intrång åtgärden innebär beaktas. Bestämmelsen omfattar endast sådana intrång

som på grund av åtgärdens intensitet eller omfattning, eller av hänsyn till uppgifternas integritetskänsliga natur eller andra omständigheter, innebär ett betydande ingrepp i den enskildes privata sfär. (Se prop. 2009/10:80 s. 250)

I artikel 8.1 i Europakonventionen anges att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Inskränkningar i skyddet godtas enligt artikel 8.2 endast om de har stöd i lag och om de i ett demokratiskt samhälle är nödvändiga med hänsyn till vissa uppräknade ändamål, däribland den nationella säkerheten, den allmänna säkerheten eller förebyggande av oordning eller brott. Som utredningen närmare redogör för följer ett skydd mot integritetsintrång av olika slag även av Sveriges övriga internationella åtaganden i fråga om mänskliga rättigheter.

Den bakgrundskontroll som är aktuell i detta lagstiftningsärende innebär enligt regeringens bedömning inte sådan kartläggning eller övervakning av enskilds personliga förhållanden eller ett sådant betydande intrång i den personliga integriteten som avses i 2 kap. 6 § andra stycket regeringsformen. Förslaget innebär därmed inte att det rör sig om en begränsning av skyddet enligt 2 kap. 6 § andra stycket regeringsformen. Det kan, oavsett detta ställningstagande, konstateras att den ordning som föreslås införs för att tillgodose ändamål som bedöms godtagbara i ett demokratiskt samhälle och möter sitt syfte på ett välavvägt sätt. Det rör sig också om en mindre ingripande lösning än den som gäller enligt säkerhetsskyddslagen.

Av 1 kap. 1 § första stycket säkerhetsskyddslagen framgår att lagen gäller för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd (säkerhetskänslig verksamhet). Syftet med lagen i stort är att skydda Sveriges säkerhet. Enligt 3 kap. 1 § samma lag ska den som genom en anställning eller på något annat sätt ska delta i säkerhetskänslig verksamhet säkerhetsprövas. Syftet med säkerhetsprövningen är, enligt 3 kap. 2 § säkerhetsskyddslagen, att klarlägga om en person kan antas vara lojal mot de intressen som skyddas av lagen och i övrigt pålitlig från säkerhetssynpunkt. Vid säkerhetsprövningen ska sådana omständigheter beaktas som kan antas innebära sårbarheter i säkerhetshänseende. Enligt 3 kap. 3 § säkerhetsskyddslagen ska säkerhetsprövningen göras innan deltagandet i den säkerhetskänsliga verksamheten påbörjas och följas upp under den tid som deltagandet i verksamheten pågår.

Säkerhetsprövningen omfattar som utgångspunkt både grundutredning och registerkontroll samt i vissa fall även en särskild personutredning enligt 3 kap. 3 § säkerhetsskyddslagen. Utredningen ska i sistnämnda fall omfatta en undersökning av den kontrollerades ekonomiska förhållanden. Utredningen ska i övrigt ha den omfattning som behövs enligt 3 kap. 17 § säkerhetsskyddslagen. Registerkontrollerna omfattar enligt 3 kap. 13 § säkerhetsskyddslagen både uppgifter ur lagen om belastningsregister och lagen (1998:621) om misstankeregister, samt vissa andra uppgifter. Vid registerkontroll ska enligt 3 kap. 14 § säkerhetsskyddslagen uppgifter löpande hämtas in under den tid deltagandet i den säkerhetskänsliga verksamheten pågår.

Utredningen konstaterar att ett omfattande kontrollsystem enligt den nya lagen, liknande säkerhetsskyddsregleringen, skulle ge goda förutsättningar

för att bedöma sårbarheter, men på bekostnad av den personliga integriteten. Många remissinstanser, däribland *Affärsverket svenska kraftnät* och *Säkerhetspolisen*, anser att den valda modellen inte är ändamålsenlig mot bakgrund av de skyddsintressen som har identifierats av utredningen och efterfrågar en mer omfattande bakgrundskontroll.

Är skyddsintressen mycket starka, till exempel skyddet av Sveriges säkerhet, kan mycket ingripande kontroller anses såväl lämpliga som ändamålsenliga och proportionerliga. Vid kontroller i syfte att skydda Sveriges säkerhet kan det, som utredningen anger, vara nödvändigt att kunna vidta omfattande utredningsåtgärder samt bland annat behandla och bevara en stor mängd personuppgifter. I de fall andra slags prövningar aktualiseras kan individens rätt till skydd för den personliga integriteten vara den tyngst vägande faktorn, och ett kontrollsystem måste då utformas med betydligt mindre ingripande åtgärder.

Regeringen konstaterar, i likhet med utredningen, att det är ett tungt vägande intresse att kritiska verksamhetsutövare kan tillhandahålla sina samhällsviktiga tjänster. Detta intresse är starkt nog för att motivera att skyddet för den personliga integriteten hos den som arbetar eller erbjuds arbete hos den kritiska verksamhetsutövaren får stå tillbaka i vissa fall. Detta gäller dock, som utredningen anger, inte reservationslöst. Endast sådana inskränkningar i den personliga integriteten som är nödvändiga för att verksamhetsutövaren ska kunna bedöma den eventuella risk som personen utgör bör godtas.

Ett minimikrav som ställs i CER-direktivet är att bakgrundskontrollen ska innefatta en identitetskontroll och kontroll av relevanta uppgifter ur kriminalregistret. En utgångspunkt bör vara att en bakgrundskontroll inte ska utformas mer ingripande än vad som är nödvändigt för att uppnå syftet med kontrollen. Som *Försäkringskassan* framhåller är det inte nödvändigtvis så att de överväganden som gör sig gällande för en lagstiftning med ett brett tillämpningsområde, och som berör många företag och myndigheter, är samma som om det hade gjorts en bedömning för de olika verksamhetsutövarna var för sig. Den nya lagen kommer att omfatta många olika sektorer och olika typer av verksamhetsutövare. Enligt regeringen är det inte nödvändigt att införa krav på mer omfattande bakgrundskontroller i förhållande till samtliga som kan vara berörda. *Svenskt Näringsliv* bedömer att behovet av mer utförlig kontroll bör utredas för vissa verksamheter men som organisationen anger bör även beaktas att krav på mer omfattande kontroller innebär fler administrativa uppgifter och ökade kostnader för berörda verksamhetsutövare. Regeringen anser därför, i likhet med utredningen, att en mindre ingripande lösning än den som gäller avseende säkerhetsskydd bör införas i den nya lagen. Som en följd av detta bör systemet avseende bakgrundskontroller i den nya lagen utformas på ett sådant sätt att ingreppet i den personliga integriteten minimeras samtidigt som syftet med bakgrundskontrollen uppnås.

Personen som kontrollen avser bör styrka sin identitet och genomgå registerkontroll

Enligt artikel 14.3 i CER-direktivet ska en bakgrundskontroll åtminstone bland annat bekräfta identiteten på den person som är föremål för

bakgrundskontrollen. I direktivet anges att det för att bekräfta identiteten på en person som är föremål för en bakgrundskontroll är lämpligt att medlemsstaterna kräver ett identitetsbevis såsom pass, nationellt identitetskort eller digitala identifieringsformer, i enlighet med tillämplig rätt (skäl 32).

Som utredningen noterar finns ingen legaldefinition av uttrycket identitet, utan det har givits olika innebörd på olika rättsområden (se prop. 2021/22:276 s. 55). Regeringen gör samma bedömning som utredningen, att uttrycket i CER-direktivets kontext tar sikte på att viss information om en person är att betrakta som objektiv fakta. Denna information bör som absolut minimum avse namn och födelsetid. I likhet med utredningen anser regeringen att ett beviskrav för dessa omständigheter bör sättas relativt högt och ansluta till vad som används i liknande situationer i svensk rätt (se till exempel 6 § andra stycket 2 passlagen [1978:302], 3 § andra stycket 2 förordningen [2005:661] om nationellt identitetskort och 2 § 2 lagen [2015:899] om identitetskort för folkbokförda i Sverige). Som följd anser regeringen, liksom utredningen, att den person som kontrollen avser bör vara skyldig att styrka sin identitet.

Utredningen föreslår att den person som kontrollen avser ska styrka sin identitet genom att visa en giltig och godtagbar identitetshandling. Utredningen bedömer att det, som utgångspunkt, är samma typer av identitetshandlingar som godtas enligt 4 § i Skatteverkets föreskrifter (SKVFS 2009:14) om identitetskort som ska anges utgöra godtagbara identitetshandlingar. Regeringen anser att det är tillräckligt att i lagen ange att den person som kontrollen avser ska styrka sin identitet.

Enligt artikel 14.3 i CER-direktivet ska en bakgrundskontroll vidare åtminstone kontrollera uppgifter ur kriminalregistret för personen i fråga avseende brott som är relevanta för en viss tjänst. Den person som bakgrundskontrollen avser bör därmed också genomgå en registerkontroll. Som utvecklas i avsnitt 9.3 bör en kritisk verksamhetsutövare få tillgång till information i belastningsregistret. Registerkontrollens innehåll och omfattning behandlas i samma avsnitt.

I avsnitt 9.2 föreslås att en befattningsanalys ska utgöra grunden för vilka som ska genomgå bakgrundskontroll. Regeringen vill framhålla att kravet på bakgrundskontroll inför en anställning eller annat deltagande enbart bör omfatta den som erbjuds anställning eller erbjuds att på annat sätt delta inom ramen för en befattning med krav på bakgrundskontroll, och inte alla som har ansökt om anställning eller om att på annat sätt få delta inom ramen för en sådan befattning. För en sådan ordning talar dels integritetsskäl, dels en önskan om att begränsa antalet registerutdrag. Registerkontrollen bör därmed utgöra det sista ledet i rekryteringsförfarandet. Erbjudandet om anställning eller annat deltagande kan och bör lämnas med förbehåll för vad som kan framkomma vid kontrollen.

Det har inte framkommit något behov av ett klassificeringsförfarande och att differentiera kravet på förnyad bakgrundskontroll efter olika klasser som *Gävle kommun* föreslår. Enligt regeringens bedömning kan uppgifter i belastningsregistret vara relevanta för riskbedömningen avseende alla personer som innehar eller kommer att inneha sådana befattningar som upptas i befattningsanalysen (se vidare avsnitt 9.2). Genom förslaget i avsnitt 9.3 om att en förnyad bakgrundskontroll ska göras inte

endast inom två år, utan även när det finns skäl för det, så sker också en viss differentiering.

Några remissinstanser, däribland *Energiföretagen Sverige*, resonerar kring utmaningen med att kontrollera äktheten av handlingar från andra länder. Bland andra *Drivkraft Sverige* önskar ett förtydligande av hur systemet med bakgrundskontroll ska fungera beträffande personer som bor eller är medborgare i ett land utanför EU. Det är inte tydligt om remissinstanserna lyfter problematiken kopplat till kontrollen av identitet eller registerkontrollen. När det gäller kontrollen av identitet finns det utrymme för att inom ramen för den föreskriftsrätt som föreslås i avsnitt 8.2 reglera hur kontrollerna ska ske och bland annat vilka identitetshandlingar som ska godtas. Frågan om vilken myndighet som bör ges föreskriftsrätt, som *Energimyndigheten* och *Livsmedelsverket* tar upp, föreslås inte regleras i lag och behandlas därför inte i denna proposition. Det finns, trots synpunkter från flera remissinstanser och till exempel *BID*, inte anledning att inom ramen för denna proposition närmare beröra utredningens övriga förslag till förordning.

Med anledning av remissinstansernas resonemang om möjligheten att genomföra bakgrundskontroller avseende tredjelandsmedborgare kan nämnas att Sverige sedan länge har ett utbyte av information om brottmålsdomar med andra länder (se vidare avsnitt 9.6). Regeringen kan inte utöka tillgången till uppgifter i andra länders register inom ramen för förslag i denna proposition eller införa en sådan mekanism som Drivkraft Sverige efterfrågar.

Det bör inte införas ett särskilt krav på lämplighetsprövning

I artikel 14.2 i CER-direktivet nämns att syftet med en bakgrundskontroll ska vara att utvärdera en potentiell säkerhetsrisk för den berörda kritiska entiteten. I skäl 32 anges att risken för att anställda och uppdragstagare till exempel missbrukar sina åtkomsträttigheter inom den kritiska entitetens organisation för skadliga ändamål är ett växande problem.

Enligt utredningen handlar bakgrundskontroller enligt direktivet ytterst om att bedöma om en person är lämplig för anställning eller annat slags deltagande genom den aktuella befattningen. Utredningen föreslår därför att det i den nya lagen ska införas ett krav på verksamhetsutövaren att säkerställa att en person bedöms som lämplig för deltagandet. Vidare föreslår utredningen att det ska regleras i lagen att endast den som har genomgått en bakgrundskontroll och har bedömts som lämplig ska få anställas eller på annat sätt delta i berörd verksamhet. Prövningen av någons lämplighet att delta i den aktuella verksamheten utgör enligt utredningen en delmängd av arbetsgivarens bedömning av individens personliga lämplighet enligt arbetsrättsliga regler.

Flera remissinstanser, däribland *Energiföretagen Sverige*, *Göteborgs kommun*, *LO* och *Transportstyrelsen*, anser att det är otydligt hur lämplighetskriteriet i utredningens förslag ska tolkas och efterfrågar vägledning. LO anser att det även måste finnas regler för hur beslutsunderlaget ska se ut och för hanteringen av sådana känsliga personuppgifter som kan förekomma. Vidare anser till exempel LO att det måste finnas en möjlighet för den enskilde som är föremål för en bakgrundskontroll att överklaga ett beslut som går ut på att denne inte är lämplig, och LO påpekar också att

det saknas en arbetsrättslig analys i betänkandet. Regeringen, som konstaterar att utredningen inte för något närmare resonemang när det gäller dessa frågor, gör följande överväganden i fråga om utredningens förslag i denna del.

En grundläggande utgångspunkt är givetvis att endast lämpliga personer deltar i sådan verksamhet som lagen tar sikte på. Regeringen noterar dock att det i CER-direktivet inte anges att de kritiska entiteterna ska säkerställa att en person bedöms som lämplig. Regeringen anser, till skillnad från utredningen, att det inte heller behöver införas något krav på att en kritisk verksamhetsutövare ska säkerställa att en person bedöms som lämplig. Kritiska verksamhetsutövares skyldighet att agera om en person bedöms utgöra en potentiell säkerhetsrisk, till exempel med anledning av förekomst i belastningsregistret, aktualiseras redan genom verksamhetsutövarens skyldighet att vidta åtgärder för motståndskraft, det vill säga lämpliga och proportionella tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa sin motståndskraft (se avsnitt 8.2). Enligt regeringen kan det därtill förväntas att verksamhetsutövaren genomför noggranna rekryteringsprocesser i strävan att bemanna verksamheten med endast lämpliga personer. För att upprätthålla en väl fungerande organisation kan det också förväntas att verksamhetsutövaren leder och fördelar arbetet med samma strävan och därmed gör noggranna överväganden avseende sin bemanning.

En bakgrundskontroll kommer att utgöra ett verktyg för och ett led i den kritiska verksamhetsutövarens bedömning av vilka potentiella säkerhetsrisker som kan finnas kopplat till verksamheten och vilka åtgärder för motståndskraft som krävs. Som utvecklas i avsnitt 9.3 föreslås en kritisk verksamhetsutövare få tillgång till information i belastningsregistret. Att en person förekommer i belastningsregistret bör inte per automatik innebära att personen betraktas som en säkerhetsrisk. På motsvarande vis skulle det kunna föreligga en risk även om en person inte förekommer i belastningsregistret. Verksamhetsutövaren kan komma att behöva ställa uppföljande frågor kopplat till uppgifter som framkommer vid registerkontrollen för att bedöma eventuella säkerhetsrisker. En bedömning av om det föreligger potentiella säkerhetsrisker kopplat till en enskild person förutsätter en helhetsbedömning av den information som verksamhetsutövaren har tillgänglig. Det handlar om uppgifter som verksamhetsutövaren naturligt får del av inom ramen för en normal rekryteringsprocess respektive under pågående anställning.

Det finns olika säkerhetsrisker som kan behöva utvärderas. Den kritiska verksamhetsutövaren kan exempelvis behöva bedöma om det finns en risk för att en enskild person kan missbruka sina åtkomsträttigheter för skadliga ändamål eller om det finns en risk för att personen kan hamna i en intressekonflikt eller bli utsatt för olika påtryckningar på ett sätt som kan skada verksamheten. Den nya lagen kommer att gälla för ett stort antal sektorer och verksamhetsutövare. Hur bedömningen av risker närmare bör göras bör inte regleras i lag utan konkretiseras på lägre författningsnivå, som flera remissinstanser efterfrågar. Detta kan ske med stöd av det bemyndigande som föreslås och behandlas i avsnitt 8.2. Ett exempel på vad som kan föreskrivas är hur man bör bedöma risken för störning i tillhandahållandet av den samhällsviktiga tjänsten. En sådan bedömning kommer i sin tur att vara central för vilka befattningar som ska tas upp i befattnings-

analysen och därmed för vilka personer som ska genomgå bakgrundskontroll (se vidare avsnitt 9.2). Hanteringen av personuppgifter, som LO berör, behandlas i avsnitt 13.2.

Om verksamhetsutövaren identifierar en risk kopplad till en viss person, så följer det av verksamhetsutövarens övergripande ansvar enligt förslaget i avsnitt 8.2 att vidta åtgärder för att minska den risken. Bedömningen av vilka potentiella säkerhetsrisker som finns kopplat till verksamheten och vilka åtgärder för motståndskraft som kan och behöver vidtas, måste göras utifrån den enskilda verksamheten och den befattning som personen har eller är aktuell för. Huruvida en kritisk verksamhetsutövare har vidtagit tillräckliga åtgärder för motståndskraft får bedömas i varje enskilt fall och kan i slutändan bli en fråga för tillsynsmyndigheten eller ytterst en domstol. I sammanhanget kan det även tilläggas att om en arbetstagare visar på exempelvis bristande omdöme, agerar illojalt eller på annat sätt skadar arbetsgivaren kan arbetsrättsliga åtgärder såsom omplacering till annan befattning, eller ytterst uppsägning eller avsked, komma i fråga. Arbetstvister handläggs enligt lagen (1974:371) om rättegången i arbetstvister.

Lagrådet ser det som en brist att det inte finns någon reglering i lagen av vad det ska få för följd om någon anställd som ska kontrolleras vägrar att genomgå kontrollen eller om kontrollen utfaller på sådant sätt att personen måste omplaceras eller avskedas. Åtminstone bör frågan om hur det arbetsrättsliga regelverket förhåller sig till lagförslaget redas ut på ett mer heltäckande sätt än som har skett i lagrådsremissen enligt Lagrådet.

Det finns inte utrymme för att införa någon särskild reglering som ändrar vad som annars gäller ur ett arbetsrättsligt perspektiv inom ramen för denna proposition. Det är inte heller möjligt att på ett heltäckande sätt beskriva vilka omständigheter som skulle kunna aktualiseras och vilka situationer som skulle kunna uppstå i samband med en bakgrundskontroll och hur dessa omständigheter och situationer ska hanteras i varje enskilt fall. Vilka krav som gäller för omplacering, uppsägning och avsked framgår av det arbetsrättsliga regelverket och den rättspraxis som finns på området.

Även redan anställda bör omfattas av bakgrundskontroller

Utredningen anser att artikel 14.1 i CER-direktivet ska tolkas som att den tar sikte både på de personer som vid lagstiftningens ikraftträdande redan har befattningar som omfattas av kravet på bakgrundskontroller, och sådana personer som övervägs för rekrytering till sådana befattningar. Med beaktande av att det i artikel 14.1 a anges att det handlar om personer som ”innehar” känsliga roller, och att det i artikel 14.1 c anges att det även handlar om personer som ”övervägs för rekrytering” anser regeringen att det av direktivet får anses följa att bakgrundskontroller ska genomföras beträffande både personer som har befattningar som omfattas av kravet på bakgrundskontroller och sådana personer som övervägs för rekrytering till sådana befattningar.

Frågan är då, som utredningen lyfter, om det av direktivet också följer att kravet på bakgrundskontroller ska gälla för personer som vid lagstiftningens ikraftträdande redan har befattningar som omfattas av krav på sådana kontroller. Någon uttrycklig reglering av denna fråga finns inte i

direktivet. En restriktiv tolkning av direktivet, som skulle innebära att endast sådana som övervägs för befattningar efter ikraftträdandet ska kontrolleras, är dock enligt regeringens mening inte förenlig med vad som anges om syftet med en bakgrundskontroll i CER-direktivet, nämligen att utvärdera en potentiell säkerhetsrisk. Som exempelvis *Arbetsgivarverket* framhåller är det vidare viktigt att arbetsgivare ges verktyg för att stärka säkerhetsarbetet avseende redan anställda. Detta ställningstagande medför att när lagstiftningen har trätt i kraft bör den kritiska verksamhetsutövaren vara skyldig att genomföra bakgrundskontroller avseende personal, uppdragstagare och andra som redan deltar i verksamheten inom ramen för befattningar med krav på bakgrundskontroll men också sådana personer som övervägs för rekrytering till sådana befattningar.

Malmö kommun bedömer att kravet på bakgrundskontroller i förhållande till uppdragstagare och leverantörer kan behöva regleras vid upphandling och ställer sig frågande till hur kraven kan uppfyllas vid redan ingångna avtal. Regeringen konstaterar att en kritisk verksamhetsutövare inte bör kunna undgå skyldigheterna enligt lagen genom att anlita exempelvis externa leverantörer. Skyldigheten att genomföra bakgrundskontroller kan vidare i vissa fall innebära att verksamhetsutövaren måste vidta åtgärder för att revidera redan ingångna avtal. Det kommer, som konstateras ovan, i slutändan att vara upp till tillsynsmyndigheten eller ytterst en domstol att bedöma om verksamhetsutövaren har vidtagit tillräckliga åtgärder för att uppfylla sina skyldigheter enligt den nya lagen.

Nästa fråga är då om, och i sådana fall när, en förnyad bakgrundskontroll ska göras av anställda och andra som fortsatt deltar i verksamheten. Utredningen anser att det av CER-direktivet får anses följa att även en förnyad bakgrundskontroll ska göras. En motsatt tolkning vore enligt utredningen inte förenlig med direktivets syfte. Regeringen delar den uppfattningen. Även om bakgrundskontroller kommer att innebära fler administrativa uppgifter, ökade kostnader och en viss integritetspåverkan som till exempel *Enköpings kommun* och *Luleå kommun* anger, bedömer regeringen att möjligheten att genomföra förnyade bakgrundskontroller av anställda, och personer som på annat sätt deltar i verksamheten, utgör en förutsättning för en hög personalsäkerhet. En anställning kan pågå under lång tid och omständigheterna kan förändras. En verksamhetsutövare kan därför ha ett befogat intresse av att få information om huruvida en anställd har begått brott som kan ge anledning att ifrågasätta en tidigare gjord bedömning i fråga om den anställde kan utgöra en potentiell säkerhetsrisk eller inte, antingen genom förnyad bakgrundskontroll efter en viss tid eller när det finns skäl för en sådan. Genom att det i lagen anges när en förnyad bakgrundskontroll får och ska göras minskar risken för bristande objektivitet som annars skulle kunna uppstå om verksamhetsutövaren helt fritt skulle få bestämma tidpunkten för en förnyad bakgrundskontroll. Hur ofta en bakgrundskontroll ska få göras behandlas i avsnitt 9.3.

Förhållandet till säkerhetsskyddslagen, cybersäkerhetslagen och annan reglering

Flera remissinstanser, däribland *Domstolsverket*, efterfrågar förtydliganden när det gäller förslagets förhållande till säkerhetsskyddslagen. I avsnitt 5.4.3 föreslås att den nya lagen inte ska gälla för statliga

myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen. Skyldigheterna enligt lagen, bland annat kravet på bakgrundskontroller, föreslås inte gälla för en enskild verksamhetsutövare som bedriver enbart säkerhetskänslig verksamhet eller som erbjuder tjänster enbart till statliga myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet. För andra kritiska verksamhetsutövare som till någon del bedriver säkerhetskänslig verksamhet föreslås skyldigheterna enligt lagen inte gälla för den delen av verksamheten som är säkerhetskänslig. För övriga delar av verksamheten föreslås den nya lagen gälla i sin helhet.

Om det i lag eller annan författning finns bestämmelser som innehåller krav på bakgrundskontroll med minst motsvarande verkan som den nya lagens krav gäller, enligt förslaget i avsnitt 5.4.2, inte kraven i den nya lagen för verksamhetsutövaren. Som framgår av nyss nämnda avsnitt anser regeringen att det inte är görbart att sammanställa samtliga rättsregler som kan anses ha motsvarande verkan. Med hänvisning till de föreslagna undantagen för säkerhetskänslig verksamhet finns det vidare som utgångspunkt ingen anledning att bedöma huruvida säkerhetsskyddsregelverket innebär krav med motsvarande verkan som vissa remissinstanser, däribland *Drivkraft Sverige,* resonerar om. Som exempelvis *Livsmedelsverket* lyfter fram kan det dock uppstå situationer då personal behöver genomgå såväl bakgrundskontroll enligt den nya lagen som säkerhetsprövning enligt säkerhetsskyddslagen. Med hänsyn till att bestämmelserna om bakgrundskontroll enligt den nya lagen och säkerhetsprövning enligt säkerhetsskyddslagen har delvis olika syften, omfattning och tillämpningsområden kan enligt regeringen en sådan ordning inte anses vara obefogad. Det finns inte heller utrymme för att låta säkerhetsskyddslagen vara subsidiär i förhållande till den nya lagen, bland annat eftersom den tar sikte på Sveriges säkerhet.

Region Stockholm vill se ett förtydligande när det gäller förhållandet till cybersäkerhetslagen med anledning av att utredningen anger att uttrycket befattningar även omfattar deltagande i verksamhet som medför så kallad logisk tillgång. Logisk tillgång torde enligt regionen avse endast hantering av it-system. I avsnitt 5.4.2 behandlas den nya lagens förhållande till cybersäkerhetslagen. I cybersäkerhetslagen finns krav på att verksamhetsutövare ska vidta säkerhetsåtgärder som avser personalsäkerhet. Av förarbetena till den lagen framgår att kravet bland annat kan innebära att verksamhetsutövaren genomför olika typer av kontroller exempelvis i form av verifiering av kvalifikationer för att motverka mänskliga misstag eller avsiktligt skadliga handlingar (se prop. 2025/26:28 s. 245). Cybersäkerhetslagen innehåller dock inget krav på bakgrundskontroll som motsvarar CER-direktivets krav. Kravet på bakgrundskontroller enligt den nya lagen bör, som utvecklas i avsnitt 9.2, gälla för befattningar som medför tillgång till sådana system som kan påverka tillhandahållandet av den samhällsviktiga tjänsten, även om deltagandet i verksamheten endast sker på distans. Det bör dock noteras att det i samma avsnitt föreslås att bakgrundskontroller ska göras endast för befattningar där deltagandet i verksamheten innebär möjlighet att orsaka mer än ringa störning.

Regeringen konstaterar att frågan om en sådan översyn som bland andra *Säkerhetspolisen* efterfrågar ligger utanför sådant som kan behandlas inom ramen för denna proposition.

9.2 Befattningsanalysen bör utgöra grunden för vilka som ska genomgå bakgrundskontroll

Regeringens förslag

En kritisk verksamhetsutövare ska göra en analys av vilka befattningar som ska omfattas av krav på bakgrundskontroll (befattningsanalys). Befattningsanalysen ska dokumenteras och innehålla uppgifter om sådana befattningar där deltagande i verksamheten innebär möjlighet att orsaka mer än ringa störning i den kritiska verksamhetsutövarens tillhandahållande av en eller flera samhällsviktiga tjänster.

Befattningsanalysen ska uppdateras vid behov och minst en gång om året.

Utredningens förslag

Förslaget från utredningen stämmer delvis överens med regeringens. Utredningen föreslår att det ska anges i lagen att befattningsanalysen ska utgå från den kritiska verksamhetsutövarens riskbedömning och åtminstone innehålla uppgift om vilka befattningar där deltagande kan orsaka mer än ringa skada på den samhällsviktiga tjänsten.

Remissinstanserna

Post- och telestyrelsen, Sveriges akademikers centralorganisation (Saco) och *Sveriges metereologiska och hydrologiska institut* tillstyrker förslaget. Saco anser att det är nödvändigt med dokumentation för att processen ska bli förutsägbar och rättssäker, och att bedömningen av vilka befattningar som ska omfattas behöver vara så restriktiv som möjlig och i stället kompletteras med andra säkerhetsåtgärder likt åtkomstbegränsning. Ett krav på att det ska röra sig om befattningar där deltagande kan orsaka mer än ringa skada på den samhällsviktiga tjänsten framstår enligt Saco som rimligt. *Stockholms kommun* bedömer att den korta tid som utredningen föreslår för ikraftträdandet av lagen innebär små möjligheter för berörda verksamhetsutövare att dessförinnan, genom olika typer av behörighetsregleringar, minska antalet befattningar som omfattas av krav på bakgrundskontroll på det sätt som nämns i betänkandet. *Svensk Dagligvaruhandel* anser att det är av vikt att en befattningsanalys genomförs men understryker att en indelning av befattningar i sådana där ett deltagande kan orsaka mer än ringa skada på den samhällsviktiga tjänsten och sådana där ett deltagande inte bedöms kunna orsaka sådan skada inte alltid är lika tydlig inom alla sektorer. Enligt Svensk Dagligvaruhandel behöver det lyftas fram mer om indirekt påverkan, då alla med tillgång till en lokal kan göra sig skyldiga till sabotage och därmed bör omfattas av befattningsanalysen.

Flera remissinstanser, däribland *Livsmedelsverket*, *Malmö kommun, Säffle kommun, Transportstyrelsen* och ett flertal av länsstyrelserna, anser att innebörden av uttrycket ringa skada behöver förtydligas.

Några remissinstanser anser att befattningsanalyserna ska genomföras mer sällan än vad som föreslås. *Energiföretagen Sverige* och *Vattenfall AB*

påtalar att säkerhetsskyddslagstiftningen inte innehåller något motsvarande krav på årlig översyn för verksamheter av betydelse för Sveriges säkerhet. Vattenfall AB anser att årlig uppdatering av befattningsanalysen är ett för högt ställt krav och föreslår samma nivå som inom säkerhetsskyddsområdet. *Nynäshamns kommun* är positiv till krav om att kritiska verksamhetsutövare ska göra befattningsanalyser men anser att en sådan ska göras en gång per mandatperiod eller vid behov, såsom vid större omorganisationer. Bland andra *Region Norrbotten* bedömer att det kommer att vara resurskrävande för verksamhetsutövarna att göra befattningsanalysen.

Skälen för regeringens förslag

Det bör införas en skyldighet att göra en befattningsanalys

Givet syftet med en bakgrundskontroll är det, som utredningen samt exempelvis *Saco* anger, centralt att en förteckning tas fram där de befattningar hos den kritiska verksamhetsutövaren som omfattas av kravet på bakgrundskontroller framgår. En sådan skyldighet bör regleras i den nya lagen. Av lagen bör framgå att verksamhetsutövaren är skyldig att göra en befattningsanalys som ska dokumenteras.

Med uttrycket befattning bör enligt utredningen förstås alla typer av roller och funktioner som medför fysisk eller logisk tillgång till en kritisk verksamhetsutövares samhällsviktiga tjänst. Uttrycket avser enligt utredningen både sådana befattningar som anställda innehar och sådana som uppdragstagare och leverantörer anlitas för att fullgöra. Utredningen anger inte vad som avses med logisk tillgång.

Regeringen konstaterar att det av artikel 14.1 i CER-direktivet följer att bakgrundskontroller ska ske av personer som innehar känsliga roller i eller till förmån för den kritiska entiteten, särskilt när det gäller den kritiska entitetens motståndskraft. Av samma artikel följer vidare att bakgrundskontroller ska ske avseende personer som är bemyndigade att direkt eller på distans få tillgång till den kritiska entitetens lokaler eller dess informations- eller kontrollsystem, inbegripet när det gäller den kritiska entitetens säkerhet. Det kan därför, som *Svensk Dagligvaruhandel* resonerar kring, bland annat röra sig om personer som ges tillträde till lokaler där en eller flera samhällsviktiga tjänster bedrivs, eller som får åtkomst till sådana system som kan påverka en eller flera sådana tjänster.

Befattningsanalysen bör innehålla en beskrivning av sådana befattningar som kan påverka den kritiska verksamhetsutövarens tillhandahållande av en eller flera samhällsviktiga tjänster på visst sätt, till exempel eftersom befattningen innebär tillträde eller åtkomst till lokaler, anläggningar eller annan kritisk infrastruktur. Som behandlas i avsnitt 6.3 föreslås uttrycket kritisk infrastruktur definieras på samma sätt i den nya lagen som i CER-direktivet. Med kritisk infrastruktur avses enligt artikel 2.4 i direktivet en tillgång, en anläggning, utrustning, ett nätverk eller ett system, eller en del av en tillgång, en anläggning, utrustning, ett nätverk eller ett system, som krävs för tillhandahållandet av en samhällsviktig tjänst. Således bör även deltagande i verksamheten som endast sker på distans beaktas.

Både sådana befattningar som anställda innehar och sådana som exempelvis uppdragstagare och leverantörer anlitas för att fullgöra bör omfattas av förteckningen. En sådan utformning är enligt regeringen

förenlig med innebörden och utformningen av artikel 13.1 i CER-direktivet, där det anges att medlemsstaterna ska säkerställa att kritiska entiteter, med avseende på personalsäkerhet, beaktar externa tjänsteleverantörers personal vid fastställandet av kategorier av personal som utför kritiska funktioner.

En central fråga att bedöma i befattningsanalysen är vilken påverkan som en person till följd av sin befattning kan ha på den kritiska verksamhetsutövarens tillhandahållande av den samhällsviktiga tjänsten. Verksamhetsutövaren behöver noga analysera vilka befattningar som ska omfattas av kravet på bakgrundskontroller. Analysen bör bygga på den riskbedömning som verksamhetsutövaren ska genomföra enligt förslaget i avsnitt 8.1. Något behov av att ange detta i lagen finns dock inte. Verksamhetsutövaren bör, som utredningen anger, alltid överväga om verksamheten är organiserad på ett optimalt sätt utifrån skyddsbehovet och om alternativa åtgärder till bakgrundskontroller i stället kan vidtas. Genom att vidta andra säkerhetsåtgärder, till exempel tillträdes- och åtkomstbegränsningar, kan antalet befattningar som kan påverka tillhandahållandet av den samhällsviktiga tjänsten minskas som Saco resonerar kring. Regeringen har förståelse för *Stockholms kommuns* ståndpunkt att det i vissa fall kan vara förenat med svårigheter för berörda verksamhetsutövare att före ikraftträdandet av den nya lagen, genom olika typer av tillträdes- och åtkomstbegränsningar, få till stånd en sådan förändring. Utformningen av artikel 13.1 e i CER-direktivet innebär dock att varje verksamhetsutövare som har identifierats som kritisk ska vidta åtgärder för att säkerställa en ändamålsenlig hantering av personalsäkerhet, inbegripet att fastställa åtkomsträttigheter till lokaler, kritisk infrastruktur och känslig information. Frågan om när lagen bör träda i kraft behandlas i avsnitt 15 och regeringen bedömer inte att det finns skäl att skjuta på ikraftträdandet givet vikten av att regleringen kommer på plats så snart som möjligt.

Bakgrundskontroller där deltagandet kan orsaka mer än ringa störning

En bakgrundskontroll medför till sin natur ett antal negativa konsekvenser. Som utvecklas i avsnitt 9.3 föreslås en kritisk verksamhetsutövare inom ramen för bakgrundskontroller få tillgång till information i belastningsregistret. Det kan i samband med anställning eller motsvarande även komma att ställas frågor om innehållet i registerutdraget. Det medför att den kritiska verksamhetsutövaren kan få tillgång till information som kan uppfattas som mycket integritetskränkande för den person som kontrollen avser. Vidare ska uppgifternas relevans bedömas av den anställande eller anlitande verksamheten. Aktiviteten innebär som sådan att tid läggs och kostnader uppstår kopplat till insamling och analys av uppgifter. Även om processen kan genomföras relativt fort innebär den med nödvändighet ytterligare moment i ett rekryteringsärende, vilket kan få negativa konsekvenser för en rekrytering. Bakgrundskontroller under pågående anställning kan också uppfattas som en integritetskränkning. Beroende på utfallet av en sådan kontroll kan den även leda till negativa konsekvenser för den enskilde. Det finns därför, som utredningen anger, goda skäl att begränsa förutsättningarna för när en bakgrundskontroll ska få genomföras.

Regeringen ställer sig bakom ståndpunkten att det bör införas ett kvalificeringskrav som innebär att bakgrundskontroller endast ska genomföras när det är nödvändigt. Det gör även att antalet personer som kan omfattas av kravet på bakgrundskontroller kan hållas lägre. Det leder i sin tur till en minskad administrativ börda för verksamhetsutövarna och att färre personer behöver utsättas för det integritetsintrång som en bakgrundskontroll innebär.

Utredningen föreslår att en bakgrundskontroll endast ska komma i fråga för deltagande som kan orsaka mer än ringa skada på den samhällsviktiga tjänsten. Den mindre olägenhet som kan uppkomma genom att sådana befattningar som endast kan orsaka ringa skada faller utanför skyldigheten att genomföra bakgrundskontroller bedömer utredningen vara hanterbar jämfört med det integritetsintrång som bakgrundskontroller skulle innebära kopplat till dessa befattningar. Den skada som en person till följd av sin befattning har möjlighet att orsaka på den samhällsviktiga tjänsten ska enligt utredningen vara styrande för om befattningen ska omfattas av kravet på bakgrundskontroller, och därmed beaktas i befattningsanalysen. Utredningen föreslår att det uttryck som ska användas är ringa skada, vilket ansluter till etablerad begreppsanvändning inom svensk rätt.

Flera remissinstanser anser att innebörden av uttrycket ringa skada behöver förtydligas. Regeringen konstaterar, som utredningen, att uttrycket används kopplat till säkerhetsskyddsklassificering enligt säkerhetsskyddslagen. Klassificeringen sker efter en bedömning av den skada som ett eventuellt röjande av uppgifterna kan medföra för Sveriges säkerhet (se 2 kap. 5 § säkerhetsskyddslagen). I förarbetena till säkerhetsskyddslagen anges att bedömningen avgörs genom en hypotetisk skadebedömning. Där bedöms vilka konsekvenser ett eventuellt röjande av uppgifterna skulle kunna få för de särskilda skyddsintressen som finns i den aktuella verksamheten. Genom att bedöma eventuella konsekvenser framgår också tydligt vilken risk för skada som finns (se prop. 2017/18:89 s. 66).

Enligt regeringen framstår det dock som mindre lämpligt att använda sig av uttryckssättet ringa skada på den samhällsviktiga tjänsten för att identifiera de befattningar som ska omfattas av kravet på bakgrundskontroller. Givet att åtgärderna i CER-direktivet bland annat syftar till att förebygga och motverka att störningar uppstår i de kritiska verksamhetsutövarnas tillhandahållande av samhällsviktiga tjänster är det mer naturligt att tala om störning, jämfört med skada som säkerhetsskyddslagen tar sikte på. Som en följd av detta föreslår regeringen, till skillnad från utredningen, att bakgrundskontroller ska göras för befattningar där deltagande i verksamheten innebär möjlighet att orsaka mer än ringa störning i den kritiska verksamhetsutövarens tillhandahållande av en eller flera samhällsviktiga tjänster. Sådana befattningar bör därför beaktas i befattningsanalysen. Med ringa störning avses en mycket begränsad störning. Som regeringen anger i avsnitt 9.1 finns ett behov av att konkretisera regleringen men det bör ske på lägre föreskriftsnivå än lag.

Vilken påverkan som en person till följd av sin befattning kan ha på tillhandahållandet av en viss tjänst varierar beroende på verksamheten och tillträdes- och åtkomsträttigheter till lokaler, anläggningar och annan kritisk infrastruktur som informations- och kontrollsystem. En noggrann analys av det deltagande det är fråga om får göras i varje enskilt fall och

för varje verksamhetsutövare. Som framgår av avsnitt 8.2 och 9.1 bör bakgrundskontroller anses vara en åtgärd för motståndskraft enligt artikel 13.1 i CER-direktivet. Genomförandet av bakgrundskontroller omfattas därför också av kravet på lämplighet och proportionalitet som behandlas i avsnitt 8.2.

Befattningsanalysen bör dokumenteras och hållas uppdaterad

Utredningen föreslår att befattningsanalysen ska dokumenteras och hållas uppdaterad, minst en gång om året eller i övrigt när behov uppstår. Detta innebär att befattningsanalysen, som utredningen anger, ska uppdateras vid förändringar som innebär att befattningar bör läggas till eller tas bort.

Regeringen instämmer i utredningens uppfattning att befattningsanalysen bör dokumenteras och att den bör uppdateras. En sådan ordning leder, som *Saco* pekar på, till en ökad förutsägbarhet som är viktigt ur ett rättssäkerhetsperspektiv. Några remissinstanser, däribland *Nynäshamns kommun*, anser att befattningsanalyserna ska genomföras mer sällan och vid behov, såsom vid större omorganisationer. I CER-direktivet anges ingen skyldighet att göra en översyn men regeringen bedömer, utifrån artikel 13.1 e, att en sådan bör krävas. Regeringen menar att det är rimligt att ställa krav på att verksamhetsutövare kontinuerligt och minst en gång om året ser över vilka befattningar som ska omfattas av kravet på bakgrundskontroller och, vid förändringar, uppdaterar befattningsanalysen. Det bör därför, även med beaktande av bland annat *Region Norrbottens* synpunkter, införas ett krav som innebär att befattningsanalysen ska dokumenteras och hållas uppdaterad, minst en gång om året eller i övrigt när behov uppstår.

9.3 Registerkontroll och förnyad bakgrundskontroll

Regeringens förslag

Den person som bakgrundskontrollen avser ska på begäran av den kritiska verksamhetsutövaren visa upp ett utdrag ur belastningsregistret. Utdraget ska inte få vara äldre än sex månader.

En förnyad bakgrundskontroll ska göras när det finns skäl för det, och senast inom två år efter det att den senaste bakgrundskontrollen genomfördes.

Det ska genomföras ändringar i lagen om belastningsregister som möjliggör för den enskilde att begära ut ett begränsat utdrag från belastningsregistret om sig själv.

Utredningens förslag

Förslaget från utredningen stämmer delvis överens med regeringens. Utredningen föreslår att utdraget ska få vara högst ett år gammalt.

Flera remissinstanser har synpunkter på förslaget att den person som kontrollen avser själv ska visa upp ett belastningsregisterutdrag. Ett antal remissinstanser, däribland *Sveriges akademikers centralorganisation (Saco),* tillstyrker förslaget. Saco anser att förslaget innebär den minst ingripande ordningen för den enskilde som då har möjlighet att kontrollera vilka som får ta del av utdraget. *Salems kommun* bedömer att förslaget kommer att mildra verksamhetsutövarens administrativa börda.

Almega Säkerhetsföretagen, Bevakningsbranschens Yrkes- och Arbetsmiljönämnd (BYA) och *Svenska Transportarbetarförbundet* anser dock att det inte är verksamhetsutövaren som bäst kan avgöra om uppgifter som framkommer vid en registerkontroll innebär att en person brister i lämplighet. För enhetlighet och rättssäkra bedömningar anser de att tillsynsmyndigheten bör besluta om den prövades lämplighet, och att kontroller ska kunna ske efter ansökan av en kritisk verksamhetsutövare. Samma remissinstanser anser vidare att Registerkontrolldelegationen vid Säkerhets- och integritetsskyddsnämnden, numera Myndigheten för säkerhet och integritetsskydd, bör kontrollera berörda personer och besluta om uppgifter ska lämnas ut. *Vattenfall AB* påtalar att det av direktivet följer att den kritiska verksamhetsutövaren ska kunna ansöka om bakgrundskontroller och anser att detta bör följa av lagen för ett enhetligt system inom EU.

Bland andra *E-hälsomyndigheten* och *Prolegia Research AB* ser en risk för att förfalskade utdrag används. E-hälsomyndigheten, som i huvudsak tillstyrker utredningens förslag, anser därför att endast digitalt utfärdade och signerade intyg ska användas. *Finansiell ID-Teknik BID AB (BID)* anser att företag som erbjuder tjänster för bakgrundskontroller bör regleras och ackrediteras i särskild ordning och ges rätt att begära ut belastningsregisterutdrag från Polismyndigheten. *Svensk Dagligvaruhandel* anser att förslaget innebär stora risker och en stor belastning för företagen och Polismyndigheten. *Polismyndigheten* har inga synpunkter på förslagen i betänkandet.

Ett antal remissinstanser yttrar sig särskilt över förslaget om förnyade kontroller. *Affärsverket svenska kraftnät* anser att registerutdrag bör uppvisas oftare än inom två år efter det att den senaste registerkontrollen genomfördes. *Landsorganisationen i Sverige (LO)* och Saco anser att förslaget går längre än vad som är nödvändigt enligt direktivet. Saco anser att en förnyad bakgrundskontroll ska göras när det finns skäl för det. *Malmö kommun* anser att det är oklart vad som kan utgöra tillräckliga skäl för att en förnyad bakgrundskontroll ska göras tidigare än två år efter det att den senaste kontrollen genomfördes. Malmö kommun lyfter även möjligheten att utreda om Polismyndigheten kan meddela verksamhetsutövaren att förändringar har skett i belastningsregistret. *SJ AB* och *Tågföretagen* anser att det är otydligt hur sårbarheter ska fångas upp under anställningen.

E-hälsomyndigheten anser att utredningens förslag om att registerutdraget ska få vara högst ett år gammalt innebär en för lång tid. Även *Transportstyrelsen* anser att tidsgränsen för hur gammalt registerutdraget får vara bör kortas och att sex månader är en mer rimlig gräns. Affärsverket

svenska kraftnät pekar på att förslaget innebär att den enskilde kan undgå att behöva uppvisa ett nytt registerutdrag under sammanlagt tre års tid.

Vissa remissinstanser yttrar sig över vilka uppgifter som belastningsregistret ska innehålla. Ett antal remissinstanser, såsom *Länsstyrelsen i Västerbottens län,* Svensk Dagligvaruhandel och *Transportföretagen*, invänder mot förslaget om att ett begränsat registerutdrag ska uppvisas. *Defensify AB* anser att registerutdraget bör omfatta fler brottstyper där dagsböter har dömts ut. *Myndigheten för säkerhet och integritetsskydd* påpekar att utredningens förslag ger verksamhetsutövarna rätt till fler uppgifter ur belastningsregistret än vad som i normalfallet skulle lämnas ut inom ramen för en säkerhetsprövning, och att det saknas tillräckligt utvecklade proportionalitetsbedömningar i fråga om de syften som eftersträvas skulle kunna uppnås med ett mer begränsat utdrag. Saco tillstyrker förslaget om att ett begränsat belastningsregisterutdrag ska visas upp men vill se en ytterligare analys avseende bedömningen att registerutdraget ska innehålla uppgifter om domar där någon annan påföljd än böter har dömts ut. Transportföretagen anser att det vore problematiskt att inkludera misstankeregistret men önskar kunna ta del av uppgifter om åtal har väckts och om medarbetaren förekommer i andra rättsliga sammanhang.

Livsmedelsverket framhåller vikten av tydliga riktlinjer för vilka frågor som är relevanta att ställa kopplat till informationen i belastningsregistret och hur informationen, ur integritetssynpunkt, ska hanteras.

Skälen för regeringens förslag

Utdrag bör endast inhämtas från belastningsregistret

Av artikel 14.3 b i CER-direktivet följer att bakgrundskontrollen ska omfatta uppgifter ur kriminalregistret som är relevanta för en viss tjänst. Det finns, med hänvisning till direktivets krav, två register som kan komma i fråga att inhämta uppgifter från, belastningsregistret och misstankeregistret. I belastningsregistret finns uppgifter om den som har dömts till påföljd för brott. Registret regleras i lagen (1998:620) om belastningsregister och förordningen (1999:1134) om belastningsregister. Där finns bestämmelser om vilka uppgifter som registret ska innehålla och om när uppgifter ur detta ska eller får lämnas ut. Regleringen skiljer sig åt beroende på om den begärande parten är en svensk myndighet, utländsk myndighet, enskild som begär utdrag avseende sig själv eller en enskild som begär ut uppgifter om en annan enskild. Polismyndigheten ansvarar för belastningsregistret och prövar om uppgifter ska lämnas ut. Ändamålet med registret är framför allt, men inte enbart, att ge information om sådana belastningsuppgifter som behövs i de brottsbekämpande myndigheternas och domstolarnas verksamhet. I registret ska bland annat samtliga påföljder för brott, utvisning, förvandlingsstraff för böter, åtalsunderlåtelser samt kontakt- och tillträdesförbud föras in. Uppgifter om den som är dömd i utlandet ska under vissa förutsättningar också föras in i belastningsregistret.

Misstankeregistret syftar till att underlätta tillgången till sådana uppgifter om skälig misstanke om brott som behövs i viss verksamhet hos de brottsbekämpande myndigheterna och domstolarnas verksamhet. Registret har också till ändamål att ge information till myndigheter vid

sådan lämplighetsprövning, tillståndsprövning eller annan prövning som anges i författning. Misstankeregistret innehåller uppgifter om bland annat personer som är skäligen misstänkta för brott enligt brottsbalken eller för annat brott för vilket svårare påföljd än böter är föreskrivet. Registret regleras i lagen om misstankeregistret och förordningen (1999:1135) om misstankeregistret.

Vid en bakgrundskontroll enligt den nya lagen bör det, i enlighet med utredningens förslag, endast få ske en kontroll av innehållet i belastningsregistret. Registret är centralt för registerkontroller eftersom det innehåller en stor andel av de uppgifter som normalt ska eller får kontrolleras enligt flera författningar. Regeringen instämmer i utredningens uppfattning att uppgifter ur misstankeregistret inte bör inhämtas. Ett system för bakgrundskontroll ska utformas så att ingreppet i den personliga integriteten blir välavvägt. Med hänvisning bland annat till den omständigheten att skuldfrågan inte är slutligt prövad bör uppgifter i misstankeregistret inte ingå i bakgrundskontrollen som *Transportföretagen* resonerar kring.

Vem bör ta fram uppgifterna ur belastningsregistret?

Som vissa remissinstanser anger följer det av systematiken i artikel 14 i CER-direktivet att det är den kritiska verksamhetsutövaren som ska kunna ansöka om bakgrundskontroller av vissa personer som deltar i verksamheten. *BID* föreslår införandet av en reglering och system för ackreditering av företag som specialiserar sig på tjänster för bakgrundskontroller. Utredningen föreslår att systemet med registerkontroll ska utföras på ett sådant sätt att den enskilde, på begäran av verksamhetsutövaren, ska kunna begära ut ett utdrag ur belastningsregistret som sedan visas upp för verksamhetsutövaren. Liknande lösningar när det gäller registerkontroller inför anställning förekommer i skollagen (2010:800) och flera liknande författningar med krav på registerkontroll som till exempel lagen (2013:852) om registerkontroll av personer som ska arbeta med barn. Flera remissinstanser är, som redovisas ovan, kritiska mot lösningen och pekar på riskerna med ett sådant system.

Systemet för registerkontroll bör utformas på ett sätt som innebär att integritetsintrånget för den enskilde inte blir större än nödvändigt. Även om det i belastningsregisterregleringen finns exempel på situationer där enskilda har getts rätt att begära uppgifter om andra enskilda kan en sådan lösning enligt regeringen inte anses vara lämplig i detta fall. Den nya lagen kommer att omfatta många olika typer av verksamhetsutövare och beröra ett stort antal arbetsgivare. Beroende på hur dessa har valt att organisera verksamheten kommer ett ännu större antal personer att efter delegation fatta beslut om anställning av personal och annan rekrytering. Av integritetsskäl är det inte möjligt att låta alla dessa begära ut utdrag från belastningsregistret med risk för spridning av uppgifter till andra än den som ska ta emot uppgiften.

En lösning där den som ska kontrolleras begär ut uppgifter om sig själv och visar upp ett utdrag för verksamhetsutövaren för bedömning innebär flera fördelar ur integritetshänseende. Vid ett rekryteringsförfarande ges den enskilde en valmöjlighet; att visa upp utdraget eller att återkalla sin ansökan. Ett annat alternativ, om ett utdrag inte visas upp, är att

verksamhetsutövaren inte anställer den enskilde eftersom en bakgrundskontroll enligt lagen inte har kunnat göras. Om en redan anställd, på uppmaning av verksamhetsutövaren, inte visar upp ett utdrag från belastningsregistret förhindras verksamhetsutövaren att uppfylla sin skyldighet att göra en bakgrundskontroll. Under förutsättning att verksamhetsutövarens bedömning att inkludera befattningen i sin befattningsanalys är korrekt, uppfyller inte verksamhetsutövaren kraven enligt lagen om arbetstagaren har kvar sin befattning. Verksamhetsutövaren behöver därmed vidta åtgärder, vilket kan inbegripa arbetsrättsliga åtgärder. Det behövs med föreslagen lösning inte någon särskild instans, som *Almega Säkerhetsföretagen, BYA och Svenska Transportarbetarförbundet* nämner som ett alternativ, som beslutar om att uppgifter ska lämnas ut till verksamhetsutövaren.

Regeringen konstaterar att det är svårt att finna ett system för registerkontroll som inte påverkar den personliga integriteten eller är förenad med olägenheter av praktisk art, däribland risken för att registerutdragets äkthet skulle kunna ifrågasättas som till exempel *E-hälsomyndigheten* och *Prolegia Research AB* pekar på. Det finns dock inga indikationer på att förfalskade registerutdrag skulle vara ett vanligt förekommande problem vid registerkontroller inom exempelvis skolväsendet (se promemorian Utökade registerkontroller inom utbildningsväsendet och en ny grund för avskiljande av studenter, U2025/01126 s. 86, och även prop. 2006/07:37 s. 20). När det gäller frågan om tillförlitlighet av ett utdrag från belastningsregistret som visas upp kan det även framhållas att Polismyndigheten har en e-tjänst där arbetsgivare kan kontrollera om ett digitalt registerutdrag är äkta och utfärdat av Polismyndigheten. Ett utdrag från belastningsregistret som lämnas i fysisk form och som en enskild begärt ut om sig själv för ändamål kopplat till bland annat skollagen har en vattenstämpel som intygar äktheten.

Regeringen gör bedömningen att det är verksamhetsutövaren som är bäst lämpad att bedöma om det finns säkerhetsrisker exempelvis med anledning av förekomst i belastningsregistret. Alternativet att tillsynsmyndigheten genomför kontrollen och gör bedömningen, som Almega Säkerhetsföretagen, BYA och Svenska Transportarbetarförbundet är inne på, framstår mot den bakgrunden som mindre lämpligt. Utredningen bedömer att en mekanism där tillsynsmyndigheten lämnar ut uppgifter till verksamhetsutövaren som i sin tur gör prövningen också medför nackdelar i integritetshänseende eftersom behandlingen av personuppgifter sker av ytterligare en aktör. En sådan lösning skulle enligt utredningen även väsentligt öka den administrativa bördan för tillsynsmyndigheten. Det framstår enligt regeringen som en rimlig lösning att utforma systemet för registerkontroll i den nya lagen på ett sådant sätt som utredningen föreslår. Föreslagen lösning kan, som *Salems kommun* anger, även förväntas hålla den administrativa bördan för verksamhetsutövaren på en rimlig nivå.

Vissa remissinstanser, som exempelvis E-hälsomyndigheten och *Transportstyrelsen*, anser att utredningens förslag om att registerutdraget ska få vara högst ett år gammal innebär en för lång tid. Transportstyrelsen bedömer att sex månader är en mer rimlig gräns. Regeringen anser att det är viktigt att verksamhetsutövaren får relevant information, och att ett registerutdrag därför inte bör få vara för gammalt, för att verksamhetsutövaren ska kunna göra en bedömning av vilka potentiella säkerhetsrisker

som kan finnas kopplat till verksamheten och vidta de åtgärder för motståndskraft som krävs för att denne ska uppfylla sina skyldigheter enligt lagen. Utdraget bör, för att behålla sin aktualitet, inte vara äldre än sex månader. En sådan ordning stämmer överens med den ordning som gäller för flera andra registerkontrollagar (se till exempel 4 § lagen [2026:44] om registerkontroll vid anställning till ledande befattningar i kommuner, 4 § lagen [2026:43] om registerkontroll vid arbete i hemmet åt äldre personer eller vuxna personer med funktionsnedsättning och 1 § lagen [2010:479] om registerkontroll av personal som utför vissa insatser åt barn med funktionshinder samt även prop. 2025/26:61). Tidsgränsen för hur gammalt ett registerutdrag ska få vara enligt skollagen föreslås även kortas från ett år till sex månader (se prop. 2025/26:174).

Livsmedelsverket framhåller vikten av tydliga riktlinjer för vilka frågor som är relevanta att ställa kopplat till informationen i belastningsregistret och hur informationen, ur integritetssynpunkt, ska hanteras. Som anges i avsnitt 9.1 kan verksamhetsutövaren komma att behöva ställa uppföljande frågor kopplat till uppgifter som framkommer vid registerkontrollen för att bedöma eventuella säkerhetsrisker. Hur bedömningen av risker närmare bör göras bör, som anges i avsnitt 9.1, inte regleras i lag utan konkretiseras på lägre författningsnivå. Frågor om sekretess och personuppgiftsbehandling behandlas i avsnitt 13.

Ett begränsat utdrag bör få inhämtas

Enligt 9 § första stycket lagen om belastningsregister har en enskild rätt att på begäran skriftligen få ta del av samtliga uppgifter ur registret om sig själv. Ett utdrag med samtliga uppgifter kan innehålla information som saknar betydelse för verksamhetsutövarens bakgrundskontroll. Regeringen anser, i likhet med utredningen, att ett fullständigt utdrag vore alltför omfattande i relation till de skyddsintressen som bakgrundskontrollen är tänkt att tillgodose. Som *Saco* understryker är det av stor vikt att inte överflödig information samlas in om den sökande. Det utdrag från belastningsregistret som den sökande ska vara skyldig att hämta in om sig själv bör därför, till skillnad från vad *Transportföretagen* anför, vara begränsat till att avse vissa uppgifter. Som följd av detta bör det, som utredningen föreslår, skapas förutsättningar för den enskilde att begära ut ett utdrag där endast vissa uppgifter redovisas.

Utredningen föreslår att utdraget ur belastningsregistret genom förordningsreglering ska begränsas och att de uppgifter som ska lämnas ut ska vara desamma som när en begäran görs för att en enskild ska kunna ta till vara sin rätt i ett främmande land eller få tillstånd att resa in, bosätta sig eller arbeta där (se vidare 9 § andra stycket 1 lagen om belastningsregister och 22 § första och andra styckena förordningen om belastningsregister). Dessa uppgifter kan enligt utredningen typiskt sett vara relevanta för att bedöma en persons lämplighet att delta i verksamhet där deltagandet kan orsaka mer än ringa skada på den samhällsviktiga tjänsten. *Myndigheten för säkerhet och integritetsskydd* påpekar att utredningens förslag ger verksamhetsutövaren rätt till fler uppgifter än vad som i normalfallet skulle lämnas ut inom ramen för en säkerhetsprövning, och att det saknas tillräckligt utvecklade proportionalitetsbedömningar i fråga om de syften som eftersträvas skulle kunna uppnås med ett mer begränsat

utdrag. Saco vill se en ytterligare analys avseende bedömningen att registerutdraget ska innehålla uppgifter om domar där någon annan påföljd än böter har dömts ut. Frågan om vilka uppgifter som ska omfattas av det utdrag som den enskilde ska vara skyldig att hämta in om sig själv, som till exempel även *Defensify AB* tar upp, behöver och bör dock inte regleras i lag. Regeringen instämmer i utredningens uppfattning att detta i stället bör regleras på förordningsnivå. Närmare överväganden om utdragets innehåll görs därför inte i denna proposition.

När bör en förnyad bakgrundskontroll genomföras?

Vid en avvägning mellan verksamhetsutövarens behov av uppdaterad information och behovet av att minska den administrativa bördan för verksamhetsutövare, samt individens integritetsintresse, bedömer regeringen, i likhet med utredningen och till skillnad från *Affärsverket svenska kraftnät*, *LO* och *Saco*, att en förnyad bakgrundskontroll åtminstone bör göras senast inom två år efter det att den senaste bakgrundskontrollen genomfördes. Den nya lagen bör dock, som utredningen föreslår, också innehålla en skyldighet för verksamhetsutövaren att genomföra en förnyad bakgrundskontroll om det har framkommit skäl som föranleder det.

Flera remissinstanser, till exempel *Malmö kommun*, anser att det är otydligt hur sårbarheter ska fångas upp efter att personen har anställts och vad som kan utgöra tillräckliga skäl för att en förnyad kontroll ska göras tidigare än två år efter det att den senaste kontrollen. Enligt regeringen är det inte möjligt att göra något generellt uttalande om vad som kan utgöra sådana skäl. En bedömning måste göras i varje enskilt fall. Det kan dock exempelvis röra sig om indikationer på att personen inte på ett korrekt sätt förhåller sig till regler och överenskommelser, i fråga om till exempel åtkomstbegränsningar eller tillträde till fysiska lokaler eller it-system, eller att personen har varit frånvarande från arbetet under en längre tid under omständigheter som ger anledning att ifrågasätta skälen för sådan frånvaro.

Utredningen påpekar, som många remissinstanser, att en registerkontroll endast kommer att kunna ha en begränsad påverkan på möjligheten att bedöma risken för infiltration, bland annat därför att en kvalificerad antagonist kan antas undvika att använda sig av individer som förekommer i belastningsregistret. *SJ AB* och *Tågföretagen* anser att det är otydligt hur sårbarheter ska fångas upp under anställningen. Regeringen vill återigen framhålla att resultatet av registerkontrollen inte är den enda aspekten som behöver vägas in vid bedömningen av eventuella säkerhetsrisker. Även annan information som verksamhetsutövaren har tillgänglig behöver beaktas (se vidare avsnitt 9.1). En bakgrundskontroll är dessutom endast en av flera åtgärder för motståndskraft. Malmö kommun lyfter även möjligheten att utreda om Polismyndigheten kan meddela verksamhetsutövaren att förändringar har skett i belastningsregistret. Detta skulle innebära en omfattande skyldighet för Polismyndigheten som går utöver utredningens förslag. Regeringen ser inte heller att en sådan lösning skulle vara förenlig med ett system som i övrigt bygger på att den enskilde ska lämna information om sin förekomst i belastningsregistret.

Regeringens förslag

Vid en bakgrundskontroll ska den kritiska verksamhetsutövaren anteckna om den person som kontrollen avser har styrkt sin identitet och visat upp ett utdrag ur belastningsregistret. Någon annan dokumentation av kontrollen ska inte få göras.

Anteckningar ska bevaras i två år från den dag då bakgrundskontrollen avslutades.

Utredningens förslag

Förslaget från utredningen stämmer i huvudsak överens med regeringens. I utredningens förslag anges inte att någon annan dokumentation om kontrollen inte får göras.

Remissinstanserna

Sveriges akademikers centralorganisation (Saco) tillstyrker förslaget. *Affärsverket svenska kraftnät* anser att verksamhetsutövaren bör ges möjlighet att spara information om datumet för när utdrag ur belastningsregistret inhämtades för att förenkla bedömningen av om det finns skäl att göra en förnyad bakgrundskontroll tidigare än efter två år. *Malmö kommun* anser att förslaget, som innebär att inga anteckningar får göras gällande innehållet, ger upphov till frågor kring spårbarheten kopplat till beslut som tas och hur informationen får användas gällande hanteringen av personens anställning. *Transportstyrelsen* påpekar att det av betänkandet inte framgår om anteckningar ska bevaras även om kandidaten inte anställs. Övriga remissinstanser yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag

Den person som bakgrundskontrollen avser ska enligt förslagen i avsnitt 9.1 och 9.3, efter begäran av verksamhetsutövaren, styrka sin identitet och visa upp ett utdrag ur belastningsregistret. Verksamhetsutövaren bör, som utredningen föreslår, vara skyldig att dokumentera att kontrollen har skett och att göra en anteckning om att den som prövningen avser har styrkt sin identitet och att registerutdraget har visats upp. Det är den enda dokumentationen som bör göras om kontrollen. Det bör inte få föras några anteckningar i övrigt om till exempel registerutdragets innehåll.

Malmö kommun anser att förslaget ger upphov till frågor kring spårbarheten kopplat till beslut som tas och hur informationen får användas när det gäller hanteringen av personens anställning. Regeringen konstaterar att dokumentationen av att ett utdrag ur belastningsregistret har visats upp kommer att vara ett tillräckligt underlag för att vid en tillsyn kunna granska om en registerkontroll skett. Registerkontrollen är en del av bakgrundskontrollen som ska ske enligt regeringens förslag och bakgrundskontroller är i sin tur endast en del av de åtgärder för motståndskraft som verksamhetsutövaren föreslås vara skyldig att vidta (se vidare avsnitt 8.2).

Huruvida en verksamhetsutövare har uppfyllt sina skyldigheter att säkerställa en ändamålsenlig hantering av personalsäkerhet, inbegripet befattningsanalys och bakgrundskontroller, får bedömas i varje enskilt fall utifrån den information som är tillgänglig i tillsynsärendet.

Affärsverket svenska kraftnät anser att verksamhetsutövaren bör ges möjlighet att spara information om datumet för när utdrag ur belastningsregistret inhämtades för att förenkla bedömningen av om det finns skäl att göra en förnyad registerkontroll tidigare än efter två år. I avsnitt 9.3 görs bedömningen att ett utdrag bör få vara högst sex månader gammalt vid uppvisandet och att en förnyad bakgrundskontroll ska göras när det finns skäl för det, men senast inom två år efter det att den senaste bakgrundskontrollen genomfördes. Hur gammalt ett registerutdrag var vid tidpunkten för den senaste kontrollen bör inte i sig påverka bedömningen av när en förnyad bakgrundskontroll ska ske. Det finns därför inte skäl att ge verksamhetsutövaren en sådan möjlighet som föreslås av Affärsverket svenska kraftnät.

Frågan är vilken reglering som bör gälla för bevarandet av den anteckning som verksamhetsutövaren ska vara skyldig att göra. Vissa verksamhetsutövare är skyldiga att registrera och bevara handlingar enligt OSL och arkivlagen (1990:782). Vad som gäller för bevarandet för en aktör som har att tillämpa dessa författningar är således redan reglerat. Samtliga verksamhetsutövare träffas dock inte av angiven regleringen och det bör införas ett bevarandekrav i lagen. Regeringen bedömer, som framgår ovan, att en förnyad bakgrundskontroll för den som är anställd eller på annat sätt deltar i verksamheten ska göras vartannat år. Regeringen konstaterar, i likhet med utredningen, att det inte framkommit några skäl för att anteckningen skulle behöva bevaras längre än så. Bevarandekravet i lagen för verksamhetsutövarna bör därför anges till två år.

Som *Transportstyrelsen* påpekar anger utredningen inte om anteckningar ska bevaras även i de fall kandidaten inte anställs. Enligt regeringen bör bevarandekravet gälla även i dessa fall. Det bör dock framhållas att bakgrundskontrollen enbart bör omfatta den som erbjuds anställning eller erbjuds att på annat sätt delta inom ramen för befattningar med krav på bakgrundskontroll, och inte alla som har ansökt om anställning eller om att på annat sätt få delta i sådan befattning. Registerkontrollen bör därmed utgöra det sista ledet i rekryteringsförfarandet.

Saknas dokumentation om att den som prövningen avser har styrkt sin identitet och visat upp ett utdrag ur belastningsregistret kan det tyda på att någon bakgrundskontroll inte har gjorts. Det kan få till följd att tillsynsmyndigheten ingriper i enlighet med förslagen i avsnitt 11.

9.5 Bakgrundskontroller inför deltagande i viss samverkan enligt direktivet

Regeringens förslag

Regeringen eller den myndighet som regeringen bestämmer ska få genomföra bakgrundskontroll av personer som föreslås delta i ett råd-

givande uppdrag eller företräda Sverige i gruppen för kritiska entiteters motståndskraft enligt artiklarna 18 och 19 i CER-direktivet.

Utredningens förslag

Förslaget från utredningen stämmer delvis överens med regeringens. I utredningens förslag anges även att regeringen eller den myndighet som regeringen bestämmer ska få utfärda säkerhetsgodkännande. Utredningen föreslår även att det i lagen ska införas en bestämmelse om att ett säkerhetsgodkännande ska likställas med en bakgrundskontroll enligt den föreslagna lagen.

Remissinstanserna

Myndigheten för civilt försvar (MCF) ställer sig tveksam till utredningens bedömning att MCF ska få till uppgift att utfärda säkerhetsgodkännande för experter i ett rådgivande uppdrag eftersom det inte är en uppgift som faller inom myndighetens nuvarande ansvarsområde. Enligt MCF vore det lämpligare om godkännandet görs av respektive tillsynsmyndighet alternativt Polismyndigheten eller Säkerhetspolisen. Övriga remissinstanser yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag

I artikel 18 i CER-direktivet finns bland annat bestämmelser om skyldighet för EU-kommissionen att i vissa fall anordna rådgivande uppdrag för att bedöma de åtgärder som en kritisk verksamhetsutövare av särskild europeisk betydelse har vidtagit för att uppfylla sina skyldigheter enligt direktivet och hur ett rådgivande uppdrag ska rapporteras samt bestämmelser om kommissionens yttrande till berörd medlemsstat (se vidare avsnitt 7.2). Enligt artikel 18.7 ska medlemsstaterna säkerställa att kritiska entiteter av särskild europeisk betydelse ger det rådgivande uppdraget åtkomst till uppgifter, system och anläggningar som rör tillhandahållandet av deras samhällsviktiga tjänster som är nödvändiga för utförandet av det rådgivande uppdraget. Enligt artikel 18.5 ska medlemmarna i det rådgivande uppdraget, när så krävs, ha ett giltigt och lämpligt säkerhetsgodkännande. Sverige kan bli behörig att föreslå experter till det rådgivande uppdraget.

Genom artikel 19.1 i CER-direktivet inrättas en grupp för kritiska verksamhetsutövares motståndskraft (CERG). Gruppen ska ge kommissionen stöd samt underlätta samarbete mellan medlemsstaterna och informationsutbyte om frågor som rör direktivet. I artikel 19.2 anges bland annat att gruppen ska bestå av företrädare för medlemsstaterna och kommissionen, vid behov med säkerhetsgodkännande. Utredningen noterar att det inte anges något om behov av säkerhetsgodkännande för den övriga krets av möjliga deltagare i CERG som nämns i artikeln (”andra berörda parter” respektive ”experter från Europaparlamentet”). Utredningen tolkar skrivningen restriktivt och som att säkerhetgodkännande endast ska kunna omfatta företrädare för medlemsstaterna i denna del. I direktivet anges bland annat att avseende CERG bör medlemsstaterna sträva efter att säkerställa att de utsedda företrädarna från deras behöriga myndigheter i gruppen

samarbetar ändamålsenligt och effektivt, inbegripet genom att när så är lämpligt utse företrädare med säkerhetsgodkännande (skäl 37).

Innebörden av uttrycket säkerhetsgodkännande förklaras inte i direktivet och behöver därför tolkas. Syftet med säkerhetsgodkännandet anges inte i direktivet, vilket försvårar tolkningen. Som utredningen konstaterar saknar säkerhetsgodkännande entydig innebörd i svensk rätt och kan ta sikte på godkännande av exempelvis it-system, säkerhetsprodukter eller personal. Den mest närliggande tolkningen är dock, som utredningen anger, att denna del av CER-direktivet tar sikte på personalsäkerhet.

I den engelska språkversionen av direktivet används uttrycket security clearance. Utredningen anser att den etablerade översättningen av security clearance i personalsäkerhetssammanhang är säkerhetsklarering. En avgörande skillnad mellan ett system med säkerhetsklarering och säkerhetsskyddslagens systematik brukar anses vara att den svenska säkerhetsprövningen är knuten till en anställning eller ett deltagande i verksamhet medan kontrollen i ett system med säkerhetsklarering hänför sig till en person (se prop. 2017/18:89 s. 76). På säkerhetsskyddsområdet finns dock ett särskilt system som benämns säkerhetsintyg och som kan utfärdas för en person som har hemvist i Sverige och intyget behövs för vissa ändamål med bäring på säkerhetsskydd (se 5 kap. 1 § säkerhetsskyddslagen). Som utredningen anger är det dock inte säkert att det deltagande som CER-direktivet tar sikte på utgör säkerhetskänslig verksamhet eller verksamhet som bör omfattas av säkerhetsskydd. Som följd framstår det inte som ett tilltalande alternativ att hänvisa till mekanismen för säkerhetsintyg enligt säkerhetsskyddslagen för att tillgodose de behov av säkerhetsgodkännande som omnämns i CER-direktivet. Säkerhetsprövning enligt säkerhetsskyddslagen utgör ett mer omfattande och ingripande verktyg i jämförelse med den bakgrundskontroll som avses i CER-direktivet (se vidare avsnitt 9.1). Regeringen anser, mot denna bakgrund och i likhet med utredningen, att det inte finns skäl att likställa processen för säkerhetsgodkännande med säkerhetsprövning enligt säkerhetsskyddslagen. Regeringen anser, i likhet med utredningen, att systemet för säkerhetsgodkännande i stället lämpligen bör likställas med systemet för bakgrundskontroll.

Utredningen föreslår att det i den nya lagen ska införas en bestämmelse om att ett säkerhetsgodkännande ska anses ha samma innebörd som en bakgrundskontroll enligt den föreslagna lagen. Vidare föreslås att det i lagen ska anges att regeringen får genomföra bakgrundskontroll och utfärda säkerhetsgodkännande för personer som ska företräda Sverige i CERG, och att regeringen eller den myndighet som regeringen bestämmer ska få utfärda säkerhetsgodkännande för personer som föreslås delta i ett rådgivande uppdrag. Utredningen anger inga skäl för att reglera detta i lag.

Enligt regeringens bedömning bör bakgrundskontroller av personer som ska företräda Sverige i CERG regleras i lag eftersom kontrollerna i förlängningen kan påverka enskilda. Utifrån skrivningarna i artiklarna 18.5 och 19.2 bör möjligheten att genomföra bakgrundskontroller göras fakultativ. Det bör således vara upp till regeringen eller den myndighet som regeringen bestämmer att avgöra om en bakgrundskontroll är nödvändig för deltagande. Det behöver inte framgå särskilt av lagen att regeringen eller den myndighet som regeringen bestämmer ska få rätt att utfärda säkerhetsgodkännande. Något behov av att införa en särskild bestämmelse

i den föreslagna lagen om att ett säkerhetsgodkännande ska likställas med en bakgrundskontroll enligt lagen finns inte heller.

9.6 Utbyte av uppgifter ur belastningsregistret mellan medlemsstater

Regeringens förslag

Det ska genomföras ändringar i lagen om belastningsregister som innebär att uppgifter ur belastningsregistret ska få lämnas ut till en annan medlemsstat i EU om begäran görs med stöd av CER-direktivet.

Utredningens förslag

Förslaget från utredningen stämmer överens med regeringens.

Remissinstanserna

Affärsverket svenska kraftnät uttrycker att utredningen inte nämnvärt har tagit den enskildes personliga integritet i beaktande. Övriga remissinstanser yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag

Ecris och Ecris-TCN

Inom EU finns ett informationssystem för utbyte av uppgifter ur kriminalregister (Ecris). Ecris är ett decentraliserat system som baseras på medlemsstaternas nationella kriminalregister. Det är alltså inte fråga om en EU-gemensam databas och systemet innebär inte att medlemsstaterna har direktåtkomst till andra medlemsstaters kriminalregister. Allt utbyte av belastningsuppgifter via Ecris går genom centralmyndigheter som varje medlemsstat har utsett för detta syfte. Förutsättningarna för användningen av systemet regleras i rådets rambeslut 2009/315/RIF av den 26 februari 2009 om organisationen av medlemsstaternas utbyte av uppgifter ur kriminalregistret och uppgifternas innehåll (Ecris-rambeslutet). Ecris-rambeslutet innebär sammanfattningsvis att varje medlemsstat som meddelar en dom mot en annan medlemsstats medborgare ska informera medborgarlandet om domen. Medborgarlandet ska därefter lagra informationen. På så vis får varje medlemsstat samlad information om de egna medborgarnas kriminalhistorik inom EU, vilken ska kunna vidarebefordras vid förfrågningar från andra medlemsstater.

Ecris-rambeslutet har genomförts i svensk rätt genom framför allt ändringar i lagen om belastningsregister och förordningen om belastningsregister. När en enskild begär uppgifter om sig själv i belastningsregistret med stöd av 9 § lagen om belastningsregister ska Polismyndigheten även inhämta uppgifter som finns i kriminalregistret i en annan medlemsstat inom EU, om den enskilde är medborgare där eller om det framkommer att den staten har uppgifter om den enskilde i sitt kriminalregister. Detta gäller enligt 22 § c förordningen om belastningsregister.

EU har även antagit en förordning om inrättande av ett system som ska göra det möjligt för medlemsstaterna att få reda på vilka andra medlemsstater som har uppgifter i sina kriminalregister om en tredjelandsmedborgare. Det rör sig om Europaparlamentets och rådets förordning (EU) 2019/816 av den 17 april 2019 om inrättande av ett centraliserat system för identifiering av medlemsstater som innehar uppgifter om fällande domar mot tredjelandsmedborgare och statslösa personer (Ecris-TCN) för att komplettera det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister och om ändring av förordning (EU) 2018/1726 (EU:s förordning om Ecris-TCN). Driftsättningen av Ecris-TCN pågår.

Rörande användningen av Ecris-TCN följer det av artikel 7.1 i EU:s förordning om Ecris-TCN att Ecris-TCN alltid ska användas när en tredjelandsmedborgare begär uppgifter om sig själv (se prop. 2021/22:172 s. 35). Att Polismyndigheten får använda Ecris-TCN efter en begäran av en enskild om uppgifter om sig själv följer av 3 § lagen (2022:733) med kompletterande bestämmelser till EU:s förordning om Ecris-TCN. Om det av lag eller annan författning följer att ett utdrag ur belastningsregistret ska visas upp eller lämnas, ska Polismyndigheten enligt 6 § lagen med kompletterande bestämmelser till EU:s förordning om Ecris-TCN använda Ecris-TCN även beträffande unionsmedborgare. Med unionsmedborgare avses även svenska medborgare (se prop. 2021/22:172 s. 68).

När det gäller utlämnande av uppgifter ur det svenska belastningsregistret efter en begäran från en annan medlemsstat finns en begränsning i 12 a § första stycket lagen om belastningsregister gällande när uppgifter ur registret får lämnas ut till en utländsk myndighet som har gjort en framställan med stöd av Ecris-rambeslutet för annat ändamål än brottmålsförfaranden. För att utlämnande ska få ske krävs att motsvarande rätt att få del av uppgifterna finns för en svensk myndighet. Det rör sig därmed om ett reciprocitetskrav.

Det krävs en ändring i lagen om belastningsregister för att genomföra CER-direktivet

Av artikel 14.3 i CER-direktivet följer att medlemsstaterna är skyldiga att tillse att bakgrundskontroller som genomförs med stöd av direktivet sker genom användningen av Ecris och Ecris-TCN avseende tredjelandsmedborgare.

Regeringen föreslår att den som omfattas av krav på bakgrundskontroll själv ska inhämta ett utdrag ur belastningsregistret för ändamålet och att den enskilde ska ges en sådan rätt genom en ändring i lagen om belastningsregister (se avsnitt 9.3). Om den enskilde är medborgare i ett annat EU-land eller om det framkommer att en sådan stat har uppgifter om den enskilde i sitt kriminalregister, ska Polismyndigheten även inhämta uppgifter som finns i kriminalregistret i den staten (se 22 c § förordningen om belastningsregister). Ecris kommer alltså att användas vid registerkontroll som sker enligt den nya lagen i detta fall. Även kravet på användning av Ecris-TCN i CER-direktivet är uppfyllt (se 6 § lagen med kompletterande bestämmelser till EU:s förordning om Ecris-TCN). Någon ändrad reglering behövs därmed inte för att uppfylla kraven i artikel 14.3 i CER-direktivet i detta avseende.

Med föreslagen ordning, där det är den enskilde som begär ett utdrag om sig själv, saknas dock motsvarande rätt för en svensk myndighet att begära ut samma uppgifter. Som anges ovan medför reciprocitetskravet i 12 a § första stycket lagen om belastningsregister att en sådan rätt krävs för ett utlämnande till en annan medlemsstat. Det bör därför trots *Affärsverket svenska kraftnät*s invändningar, som utredningen anger och direktivet kräver, införas en ny möjlighet att lämna ut uppgifter ur belastningsregistret efter en begäran från en annan medlemsstat om begäran görs med stöd av CER-direktivet och även om motsvarande rätt saknas för en svensk myndighet.

De tidsfrister som gäller vid utbyte av uppgifter ur belastningsregistret kräver ingen ytterligare reglering

Av artikel 14.3 i CER-direktivet följer vissa tidsfrister som hänvisar till Ecris-rambeslutet respektive EU:s förordning om Ecris-TCN. Av artikeln följer att de centralmyndigheter som avses i artikel 3.1 i Ecris-rambeslutet och i artikel 3.5 i EU:s förordning om Ecris-TCN ska besvara begäran om utbyte av uppgifter ur kriminalregister inom tio arbetsdagar från och med den dag då begäran togs emot i enlighet med artikel 8.1 i Ecris-rambeslutet. Som utredningen noterar hänvisar tidsfristen för besvarandet av en begäran om utbyte av uppgifter enligt artikel 8.1 i Ecris-rambeslutet i sin tur till artikel 6.1 i samma rambeslut. Den senare artikeln reglerar den situationen att centralmyndigheten får rikta en begäran till en annan medlemsstats centralmyndighet, när en begäran kommer in om uppgifter som finns i den medlemsstatens kriminalregister. En sådan begäran ska av centralmyndigheten i den anmodade medlemsstaten besvaras inom tio arbetsdagar.

Situationer där en enskild ansöker om att få ut uppgifter om sig själv i kriminalregistret och centralmyndighetens rätt eller skyldighet att i sådana situationer rikta en begäran om ett utdrag ur kriminalregistret och om uppgifter ur kriminalregistret till en annan medlemsstats centralmyndighet regleras, som utredningen anger, av artikel 6.2 och 6.3 i Ecris-rambeslutet. I sådana situationer gäller en längre svarsfrist på 20 dagar enligt artikel 8.2 i samma rambeslut. Att Polismyndigheten i egenskap av utpekad centralmyndighet i Sverige har att beakta vissa tidsfrister vid besvarandet av en begäran om uppgifter ur kriminalregistret från en centralmyndighet i en annan medlemsstat följer redan av Ecris-regelverken. Det krävs därför, som utredningen anger, ingen ytterligare reglering i denna del.

10 Tillsyn

10.1 Tillsynsmyndigheterna ska pekas ut i förordning

Regeringens förslag

Den eller de myndigheter som regeringen bestämmer ska vara tillsynsmyndighet.

En tillsynsmyndighet ska utöva tillsyn över att lagen och föreskrifter som har meddelats i anslutning till lagen följs. Tillsynsmyndigheten ska också utöva tillsyn över att sådana rättsakter följs som har antagits med stöd av artikel 13.6 i CER-direktivet.

Utredningens förslag

Förslaget från utredningen stämmer i allt väsentligt överens med regeringens. Utredningen föreslår att det i lagen också ska regleras att tillsynsmyndigheterna ska genomföra rådgivande uppdrag och bidra med underlag till den nationella riskbedömningen. Utredningen föreslår inte att tillsynsmyndigheten ska utöva tillsyn över att sådana rättsakter som har antagits med stöd av artikel 13.6 i direktivet följs.

Remissinstanserna

Vissa remissinstanser, däribland *E-hälsomyndigheten*, *Statskontoret* och *Stiftelsen för Internetinfrastruktur,* är positiva till eller tillstyrker utredningens förslag som innebär att det ska finnas en eller flera tillsynsmyndigheter för varje sektor. *Myndigheten för civilt försvar (MCF), Naturvårdsverket, Sveriges advokatsamfund, Totalförsvarets forskningsinstitut (FOI)* och flertalet länsstyrelser ifrågasätter eller avstyrker emellertid det system för tillsyn som utredningen föreslår och lämnar alternativa förslag om exempelvis en nationell tillsynsmyndighet med ett övergripande ansvar. *Livsmedelsverket* föreslår att tillsynssystemet enligt säkerhetsskyddslagen ska ses över för att undersöka möjligheten att få till stånd ett mer sammanhållet tillsynssystem genom att ge samma myndighet ansvar att utöva tillsyn enligt den nya lagen, säkerhetsskyddslagen och cybersäkerhetslagen.

Flera remissinstanser, som *Affärsverket svenska kraftnät, Innovations- och kemiindustrierna i Sverige (IKEM), Läkemedelsindustriföreningen,* och *Statens Kommuner och Regioner (SKR)* samt flera kommuner och regioner*,* understryker behovet av samordning mellan tillsynsmyndigheterna. Vissa av remissinstanserna, bland andra *Svenskt Näringsliv* och SKR, för fram att det är positivt att utredningen föreslår att det ska införas ett av MCF lett samarbetsforum, vilket ska regleras i förordning.

Ett stort antal remissinstanser, däribland *Drivkraft Sverige*, *Försäkringskassan, Läkemedelsverket,* MCF, *Skatteverket*, *Strålsäkerhetsmyndigheten* och *Sveriges universitets- och högskoleförbund,* yttrar sig över förslaget om vilka myndigheter som föreslås utöva tillsyn över olika sektorer, avgränsningen av tillsynsområden och föreskriftsrätten. *Domstolsverket*

anser att en fragmenterad föreskriftsrätt som utredningens förslag innebär, i och med att respektive tillsynsmyndighet får rätt att meddela föreskrifter för sitt tillsynsområde, kan påverka rättssäkerheten. MCF förordar att myndigheten bemyndigas att meddela övergripande föreskrifter som ska gälla för samtliga sektorer och som ska reglera grundläggande krav på motståndskraft samt säkerhet och ramar för riskanalyser. MCF bedömer att tillsynsmyndigheterna vid behov bör kunna meddela avgränsade kompletterande föreskrifter. *Inspektionen för vård och omsorg (IVO)* anser att bemyndigandefrågan inte är tillräckligt utredd i fråga om vilken myndighet som ska få meddela föreskrifter på området hälso- och sjukvård och efterfrågar ytterligare resonemang i denna del. *Transportstyrelsen* ser ett stort behov av att samordna tillsynen i möjligaste mån, både utifrån verksamhetsutövarnas perspektiv och av effektivitetsskäl.

Vissa remissinstanser, däribland *Malmö kommun, Säkerhets- och försvarsföretagen (SOFF)* och *Teknikföretagen*, understryker vikten av tillsynsmyndighetens rådgivande funktion. *Svenskt Vatten* anser att det är viktigt att tillsynsmyndigheten stödjer kritiska verksamhetsutövare på ett dialog- och förtroendebaserat sätt.

Skälen för regeringens förslag

Av artikel 9.1 i CER-direktivet framgår att varje medlemsstat ska utse eller inrätta en eller flera behöriga myndigheter som ansvariga för den korrekta tillämpningen och, vid behov, efterlevnadskontrollen avseende reglerna i direktivet på nationell nivå. När det gäller de kritiska entiteterna inom de sektorer som anges i punkterna 3 och 4 i tabellen i bilagan till CER-direktivet, vilket är sektorerna bankverksamhet och finansmarknadsinfrastruktur, ska de behöriga myndigheterna i princip vara de behöriga myndigheter som avses i artikel 46 i DORA-förordningen. När det gäller de kritiska entiteterna inom den sektor som anges i punkt 8 i tabellen i bilagan, vilket är sektorn digital infrastruktur, ska de behöriga myndigheterna i princip vara de behöriga myndigheterna enligt NIS 2-direktivet. Medlemsstaterna får dock utse en annan behörig myndighet för de sektorer som anges i punkterna 3, 4 och 8 i tabellen i bilagan till direktivet i enlighet med befintliga nationella ramar. Om medlemsstaterna utser eller inrättar mer än en behörig myndighet ska de tydligt fastställa uppgifterna för var och en av de berörda myndigheterna och säkerställa att de samarbetar effektivt för att fullgöra sina uppgifter enligt direktivet, inbegripet vad gäller utseendet av och verksamheten inom den gemensamma kontaktpunkt som avses i artikel 9.2.

Regeringen har i cybersäkerhetsförordningen pekat ut Statens energimyndighet, Transportstyrelsen, Finansinspektionen, Inspektionen för vård och omsorg, Läkemedelsverket, Livsmedelsverket, Post- och telestyrelsen samt Länsstyrelserna i Norrbottens, Skåne, Stockholms, Västra Götalands, Örebro och Östergötlands län som tillsynsmyndigheter enligt cybersäkerhetslagen. I samband med genomförandet av NIS 2-direktivet bedömde regeringen att det bör finnas flera tillsynsmyndigheter (se prop. 2025/26:28 s. 123 f.). Det angavs att de sektorer som omfattas av cybersäkerhetslagen sträcker sig över många sakområden och har en anknytning till olika myndigheters ansvarsområden enligt andra regelverk. Det bedömdes finnas skäl att hålla samman myndigheternas ansvar så att

de får ett helhetsansvar över berörda områden. Samma skäl för ett delat tillsynsansvar gör sig gällande i detta lagstiftningsärende och regeringen anser därmed, till skillnad från bland andra *MCF* och *Naturvårdsverket*, att det inte bör pekas ut en central tillsynsmyndighet.

Bedömningen av vilka myndigheter som bör utöva tillsyn över den nya regleringen kan variera över tid och regeringen anser att det inte är ändamålsenligt att reglera i lag vilka myndigheter som ska vara tillsynsmyndigheter. Detta bör i stället regleras i förordning. Det bör därför föras in en bestämmelse i lagen om att den myndighet eller de myndigheter som regeringen bestämmer ska vara tillsynsmyndighet samt att tillsynsmyndigheten ska utöva tillsyn över att lagen och föreskrifter som har meddelats i anslutning till lagen följs. Tillsynsmyndigheten bör även utöva tillsyn över att sådana rättsakter som har antagits med stöd av artikel 13.6 i CER-direktivet följs.

Utredningen föreslår att det i lagen även ska regleras att tillsynsmyndigheterna ska genomföra rådgivande uppdrag och bidra med underlag till den nationella riskbedömningen (se artiklarna 5 och 18 i CER-direktivet). I avsnitt 7.2 föreslås att tillsynsmyndigheten ska medverka till att rådgivande uppdrag genomförs. Bidraget till den nationella riskbedömningen behöver, som anges i avsnitt 6.1, inte regleras i lag.

Det som många remissinstanser, bland andra *Drivkraft Sverige*, *Försäkringskassan* och MCF*,* framför i fråga om vilka myndigheter som ska ha tillsynsansvar och avgränsningen av tillsynsområdena mellan tillsynsmyndigheterna är frågor som rör utformningen av reglering på förordningsnivå och dessa frågor behandlas därför inte inom ramen för denna proposition. Det finns inte utrymme för att inom ramen för denna proposition se över tillsynssystemet som *Livsmedelsverket* föreslår. Frågan om vilken eller vilka myndigheter som bör ges föreskriftsrätt, som bland andra *Domstolsverket* väcker, rör på motsvarande sätt reglering på förordningsnivå och behandlas inte heller i denna proposition.

Frågorna om ett samarbetsforum, dialog och samordning mellan tillsynsmyndigheterna samt tillsynsmyndigheternas rådgivande funktion, som till exempel *Malmö kommun*, *Svenskt Näringsliv* och *Transportstyrelsen* berör, är inte heller föremål för behandling i denna proposition. Regeringen konstaterar dock att en myndighet, enligt 6 § myndighetsförordningen, ska verka för att genom samarbete med bland annat andra myndigheter ta till vara de fördelar som kan vinnas för enskilda och för staten som helhet. Enligt 8 § förvaltningslagen ska en myndighet vidare inom sitt verksamhetsområde samverka med andra myndigheter och i rimlig utsträckning hjälpa den enskilde genom att själv inhämta upplysningar eller yttranden från andra myndigheter. Regeringen utgår ifrån att samverkan mellan tillsynsmyndigheterna kommer att fungera väl när det gäller bland annat sådana frågor som behöver hanteras gemensamt.

Regeringens förslag

Den som står under tillsyn ska vara skyldig att på begäran tillhandahålla en tillsynsmyndighet de uppgifter eller handlingar som myndigheten behöver för sin tillsyn.

En tillsynsmyndighet ska ha rätt att i den omfattning som det behövs för tillsynen få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamhet som omfattas av tillsynen.

En tillsynsmyndighet ska få besluta att förelägga verksamhetsutövaren att tillhandahålla uppgifterna eller handlingarna och att ge tillträde. Ett föreläggande ska få förenas med vite. Ett vitesföreläggande ska även få riktas mot staten.

En tillsynsmyndighet ska få begära handräckning av Kronofogdemyndigheten för att genomföra tillsynsåtgärderna. Vid handräckning ska bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande gälla.

Utredningens förslag

Förslaget från utredningen stämmer delvis överens med regeringens. Utredningen föreslår att den som står under tillsyn ska vara skyldig att på begäran tillhandahålla tillsynsmyndigheten information som behövs för den nationella riskbedömningen. Utredningen föreslår att det ska införas en bestämmelse i lagen om att tillsynsmyndigheten ska få bestämma att ett föreläggande ska gälla omedelbart. I utredningens förslag anges inte att ett vitesföreläggande även ska få riktas mot staten.

Remissinstanserna

Majoriteten av remissinstanserna yttrar sig inte särskilt över förslaget. *Myndigheten för civilt försvar (MCF)* anser att det bör förtydligas att i de fall verksamhetsutövaren är en myndighet, region eller kommun ska risk- och sårbarhetsbedömningen enligt förordningen om statliga myndigheters beredskap eller risk- och sårbarhetsanalysen enligt lagen om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap redovisas till tillsynsmyndigheten. *Tech Sverige* betonar vikten av att bland annat rutiner införs för att säkerställa att känslig information som inhämtas av tillsynsmyndigheten kopplat till den nationella riskbedömningen hanteras på ett likadant sätt som incidentrapporter som omfattas av sekretess.

Skälen för regeringens förslag

Tillsynsmyndighetens uppdrag kräver vissa befogenheter

Av artikel 21.1 a i CER-direktivet framgår att medlemsstaterna ska säkerställa att de behöriga myndigheterna, för att bedöma om de entiteter som medlemsstaterna har identifierat som kritiska entiteter enligt artikel 6.1 fullgör de skyldigheter som fastställs i direktivet, har befogenheter och

medel för att genomföra inspektioner på plats av den kritiska infrastruktur och de lokaler som den kritiska entiteten använder för att tillhandahålla sina samhällsviktiga tjänster och tillsyn på distans av de åtgärder som vidtagits av kritiska entiteter i enlighet med artikel 13. Den sistnämnda artikeln behandlar åtgärder för motståndskraft (se vidare avsnitt 8.2). De behöriga myndigheterna ska enligt artikel 21.1 b också ha befogenhet och medel för att utföra eller beställa revisioner av kritiska entiteter.

Medlemsstaterna ska vidare enligt artikel 21.2 a säkerställa att de behöriga myndigheterna har befogenheter och medel för att, när så är nödvändigt för att fullgöra deras uppgifter enligt direktivet, kräva att entiteter enligt NIS 2-direktivet som medlemsstaterna har identifierat som kritiska entiteter inom en rimlig tidsfrist, som fastställs av dessa myndigheter, lämnar den information som är nödvändig för att bedöma om de åtgärder som entiteterna har vidtagit för att säkerställa sin motståndskraft uppfyller kraven i artikel 13. De ska också enligt artikel 21.2 b lämna bevis på att de åtgärderna faktiskt har genomförts, inklusive resultatet av en revision som har utförts av en oberoende och kvalificerad revisor som har valts av entiteten och som har utförts på entitetens bekostnad. När de behöriga myndigheterna begär denna information ska de ange syftet med kravet och specificera vilken information som krävs.

Medlemsstaterna ska enligt artikel 21.4 i direktivet säkerställa att bland annat de befogenheter som anges i artikel 21.1 och 21.2 i direktivet endast kan utövas om de omfattas av lämpliga skyddsåtgärder (se vidare avsnitt 11.2).

Uppgiftsskyldighet för verksamhetsutövaren

Utredningen föreslår att en kritisk verksamhetsutövare ska vara skyldig att tillhandahålla tillsynsmyndigheten den information som myndigheten behöver för sin tillsyn och för den nationella riskbedömningen. Regeringen anser i likhet med utredningen att verksamhetsutövaren bör ha en uppgiftsskyldighet kopplat till den information som tillsynsmyndigheten behöver för sin tillsyn men att uttrycket uppgifter och handlingar bör användas eftersom det tydliggör innebörden av skyldigheten (jfr 3 kap. 3 § cybersäkerhetslagen). Uttrycket handling bör ha samma innebörd som i andra kapitlet tryckfrihetsförordningen och därmed omfatta såväl skriftligt material som material som har lagrats digitalt och som kan läsas, avlyssnas eller på annat sätt uppfattas endast med hjälp av tekniska hjälpmedel.

När det gäller utredningens förslag om att verksamhetsutövaren också ska ha en uppgiftsskyldighet gällande information som behövs för den nationella riskbedömningen gör regeringen följande överväganden. Enligt utredningens förslag ska tillsynsmyndigheten bidra med underlag till den nationella riskbedömningen. Den nationella riskbedömningen behandlas närmare i avsnitt 6.1. Den föreslagna uppgiftsskyldigheten har, enligt regeringens bedömning, ingen koppling till tillsynsmyndighetens uppdrag att utöva tillsyn och regeringen har därför svårt att se att det rör sig om en sådan uppgiftsskyldighet som kan räknas till en tillsynsmyndighets undersökningsbefogenheter. Vidare är den föreslagna uppgiftsskyldigheten allmänt hållen. Det är svårt att bedöma vilken uppgiftsskyldighet som den föreslagna regleringen innebär i detta avseende, bland annat

jämfört med en situation där verksamhetsutövaren ska bidra med information som behövs för tillsyn. Utredningen resonerar inte om vilken information som skulle kunna krävas av verksamhetsutövaren med stöd av regleringen och beskriver inte heller hur behovsbedömningen ska göras. Regeringen konstaterar att 5 § tredje stycket förvaltningslagen visserligen skulle kunna innebära en viss begränsning av vilka uppgifter och handlingar som tillsynsmyndigheten kan begära att få del av med stöd av bestämmelsen. Det har dock, oavsett detta, inte framkommit något särskilt behov av den reglering som utredningen föreslår i denna del. CER-direktivet uppställer till exempel inget krav på att informationen ska lämnas. Utredningens förslag i denna del bör därför inte genomföras.

Eftersom uppgiftsskyldigheten knyts till uppgifter och handlingar som tillsynsmyndigheten behöver för sin tillsyn bör det inte göras något sådant förtydligande som *MCF* efterfrågar. Frågor om sekretess, som *Tech Sverige* väcker, behandlas i avsnitt 13.1.

Tillsynsmyndigheten bör ha viss tillträdesrätt

Utredningen föreslår att tillsynsmyndigheten i den utsträckning som behövs för tillsynen ska ha rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamheten. Motsvarande bestämmelser om tillträdesrätt finns i bland annat 6 kap. 3 § säkerhetsskyddslagen.

Enligt 2 kap. 6 § första stycket regeringsformen är var och en skyddad mot bland annat husrannsakan och liknande intrång. I förarbeten används uttrycket husrannsakan för att beteckna varje av myndighet företagen undersökning av hus, rum eller slutet förvaringsställe oavsett syftet med undersökningen (se prop. 1973:90 s. 246 och prop. 1975/76:209 s. 147). Skyddet mot husrannsakan kan enligt 2 kap. 20 och 21 §§ regeringsformen begränsas genom lag, men en sådan begränsning får endast göras för att tillgodose ändamål som är godtagbara i ett demokratiskt samhälle och får aldrig gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den.

Av artikel 8 i Europakonventionen följer att var och en har rätt till skydd för sitt privat- och familjeliv, sitt hem och sin korrespondens. Inskränkningar i skyddet kan godtas, under förutsättning att de har stöd i lag och är nödvändiga i ett demokratiskt samhälle för att tillgodose något av de i artikeln uppräknade intressena, däribland den nationella säkerheten.

Det är angeläget att tillsynen över såväl offentliga som enskilda verksamhetsutövare fungerar på ett tillfredsställande sätt. Det får förutsättas att en verksamhetsutövare endast undantagsvis kommer att vägra tillträde eftersom en verksamhetsutövare som är föremål för tillsyn i regel kommer att ha ett intresse av att medverka på frivillig väg. Ett effektivt system för tillsyn kan emellertid enligt regeringen inte bygga på antagandet att det alltid finns samförstånd mellan tillsynsmyndigheten och verksamhetsutövaren som är föremål för tillsynen och att verksamhetsutövaren rättar sig efter tillsynsmyndighetens anvisningar. Att tillsynsmyndigheterna kan få tillträde till områden, lokaler och andra utrymmen, inbegripet infrastruktur i enlighet med vad som nämns i artikel 21.1 a, där verksamhet som omfattas av tillsyn bedrivs är av avgörande betydelse för att de ska kunna kontrollera att lagen följs. Tillträdesrätten föreslås inte heller gälla

bostäder. Det bör framhållas att tillsynsmyndigheten är skyldig att i varje enskilt fall göra en bedömning av om en mindre ingripande åtgärd än tillträde kan vidtas i första hand och om undersökningsåtgärden är proportionerlig (se 5 § tredje stycket förvaltningslagen). Med hänsyn till de skyddsvärden som är i fråga och vilken krets som berörs av förslaget, som båda berörs i avsnitt 5, är den av utredningen föreslagna tillträdesrätten en godtagbar inskränkning av enskildas fri- och rättigheter (jfr prop. 2020/21:194 s. 82 f.). Nämnda krav i regeringsformen och Europakonventionen är mot denna bakgrund uppfyllda (jfr även artikel 21.4 i CER-direktivet).

Utredningen anger att tillsynsmyndighetens möjlighet att utföra och beställa revisioner enligt direktivet får anses ingå i uppgiften att bedriva tillsyn och möjligheten att begära in information som behövs för tillsynen samt att få tillgång till områden, lokaler och andra utrymmen som används för verksamhet som omfattas av lagen. Det saknas ledning i direktivet i fråga om vad uttrycket revisioner avser. Regeringen bedömer dock i likhet med utredningen att det är en rimlig tolkning att det inte krävs någon särskild reglering i detta avseende.

Förelägganden som bör kunna förenas med viten

Om en verksamhetsutövare inte samarbetar med tillsynsmyndigheten vid tillsynen bör myndigheten kunna meddela de förelägganden som behövs för att verksamhetsutövaren ska tillhandahålla de uppgifter och handlingar och ge det tillträde som behövs för tillsynen. Tillsynsmyndigheten bör dock som utgångspunkt i första hand eftersträva att verksamhetsutövaren tillhandahåller uppgifterna och handlingarna och ger tillträdet på frivillig väg (se 5 § tredje stycket förvaltningslagen). Tillsynsmyndigheten måste göra en proportionalitetsbedömning i varje enskilt fall.

Föreläggandena bör kunna förenas med vite. Den allmänna regleringen om viten finns i lagen (1985:206) om viten (viteslagen). Ett vitesföreläggande kan som huvudregel inte riktas mot staten. I förarbetena till viteslagen överlämnas frågan om ett vitesföreläggande ska kunna riktas mot staten till rättstillämpningen, dock med kommentaren att sådana viten bör komma i fråga främst i situationer där staten i så utpräglad grad uppträder som privaträttsligt subjekt, till exempel på det marknadsrättsliga området, att det skulle vara onaturligt om vitesmöjligheten inte stod till buds. Vidare uttalas att det utanför det marknadsrättsliga området bör krävas att ett helt speciellt undantagsfall är för handen för att ett vitesföreläggande mot en statlig aktör ska vara godtagbart (se prop. 1984/85:96 s. 99 f.). I likhet med resonemanget som förs i förarbetena till säkerhetsskyddslagen anser regeringen att det finns skäl för att vitesförelägganden ska kunna riktas mot staten även enligt den nya lagen främst eftersom staten, i situationer när ett vitesföreläggande skulle kunna aktualiseras, agerar utanför sin rent offentligrättsliga kapacitet (se prop. 2020/21:194 s. 66 f.). Regeringen bedömer att en statlig myndighet i de flesta fall kommer att följa tillsynsmyndighetens uppmaning på frivillig väg och att tillsynsmyndigheten endast undantagsvis bör behöva förena ett föreläggande med vite. Regeringen anser dock att det finns skäl att införa möjligheten för tillsynsmyndigheten att förena ett föreläggande med vite även mot staten.

Frågor om utdömande av viten ska enligt viteslagen prövas av förvaltningsrätt på ansökan av den myndighet som har utfärdat vitesföreläggandet. Det finns inte anledning att i den nya lagen införa bestämmelser som avviker från viteslagen.

Av artikel 6.1 i Europakonventionen följer bland annat att den som är anklagad för brott har rätt att inte belasta sig själv vid utredningen av anklagelsen, den så kallade passivitetsrätten. En skyldighet att lämna uppgifter och handlingar vid vite kan vara oförenlig med passivitetsrätten. Detta kan innebära att ett föreläggande om att tillhandahålla uppgifter eller handlingar inte bör förenas med vite om det rör en överträdelse som kan jämföras med en brottsanklagelse i Europakonventionens mening. Tillsynsmyndigheterna är skyldiga att vid beslut om vitesförelägganden beakta om ett sådant föreläggande kan vara oförenligt med passivitetsrätten. Skyldigheten att beakta passivitetsrätten gäller även för en domstol som överprövar ett beslut om ett vitesföreläggande.

Utredningen föreslår att tillsynsmyndigheten ska kunna besluta om att ett föreläggande enligt lagen ska gälla omedelbart. Av 35 § tredje stycket förvaltningslagen följer att en myndighet får verkställa ett beslut omedelbart om ett väsentligt allmänt eller enskilt intresse kräver det. Myndigheten ska dock, enligt samma bestämmelse, först noga överväga om det finns skäl att avvakta med att verkställa beslutet på grund av att beslutet medför mycket ingripande verkningar för någon enskild, att verkställigheten inte kan återgå om ett överklagande av beslutet leder till att det upphävs eller någon annan omständighet. Mot bakgrund av möjligheter som förvaltningslagen ger i detta avseende i förhållande till enskilda bedömer regeringen att det inte behöver införas någon sådan bestämmelse som utredningen föreslår.

Handräckning av Kronofogdemyndigheten

Tillsynsmyndigheterna bör i första hand försöka förmå berörd verksamhetsutövare att tillhandahålla uppgifter och handlingar och ge tillträde på frivillig väg (se 5 § tredje stycket förvaltningslagen). Om en verksamhetsutövare, trots förelägganden, vägrar att ge tillsynsmyndigheten uppgifter och handlingar eller tillträde, kan dock tvångsåtgärder behöva användas.

Tillsynsmyndigheterna kommer inte att ha befogenheter att vidta tvångsåtgärder. Det finns inte anledning att anta att det kommer att finnas risk för hot eller handgripligheter i samband med utförandet av en tillsynsmyndighets uppdrag. De eventuella hinder som kan uppstå får i stället antas vara av fysiskt art. För att tillsynsmyndigheten i en sådan situation ska kunna få tillgång till uppgifter och handlingar och få tillträde bör myndigheten kunna begära handräckning av Kronofogdemyndigheten. Det bör därför, som utredningen föreslår, införas en bestämmelse om att tillsynsmyndigheten ska ha rätt att begära sådan handräckning.

Det bör framgå av lagen att bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande gäller vid handräckning.

11 Ingripanden

11.1 En reglering liknande den som gäller NIS 2-direktivet bör införas

Regeringens bedömning

Regleringen för ingripanden enligt den nya lagen bör utformas på ett liknande sätt som i cybersäkerhetslagen.

Överträdelser av bestämmelser i lagen bör inte vara straffsanktionerade. En tillsynsmyndighet bör i stället kunna besluta om administrativa sanktioner.

Utredningens bedömning

Bedömningen i betänkandet stämmer överens med regeringens.

Remissinstanserna

Majoriteten av remissinstanserna yttrar sig inte över bedömningen. *Salems kommun* anser att det är positivt att lagstiftningen gällande NIS 2- och CER-direktiven stämmer överens eftersom det underlättar för verksamhetsutövarna.

Skälen för regeringens bedömning

Av artikel 22 i CER-direktivet följer en skyldighet för medlemsstaterna att fastställa regler om sanktioner för överträdelse av de nationella åtgärder som antagits enligt direktivet och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. Det lämnas åt medlemsstaterna att i övrigt avgöra utformning av sanktionerna, inklusive om de ska utgöras av administrativa sanktioner eller straffrättsliga påföljder.

Regeringen gav gällande genomförandet av NIS 2-direktivet uttryck för att administrativa sanktioner på ett bättre sätt kan göra att syftet med sanktionsbestämmelserna uppnås, nämligen att säkerställa att verksamhetsutövare uppfyller de skyldigheter som cybersäkerhetslagen innebär för dessa (se prop. 2025/26:28 s. 143 f.). Regeringen anser, likt utredningen, att de ingripandemöjligheter som införs till följd av CER-direktivet bör vara administrativa och utformas på ett liknande sätt som regleringen i cybersäkerhetslagen.

11.2 Vilka överträdelser bör kunna leda till ingripanden?

Regeringens förslag

En tillsynsmyndighet ska ingripa om en verksamhetsutövare har åsidosatt sina skyldigheter att göra en anmälan, göra en riskbedömning, vidta

åtgärder för motståndskraft eller rapportera incidenter enligt lagen eller enligt föreskrifter som har meddelats i anslutning till lagen.

Tillsynsmyndigheten ska också ingripa om verksamhetsutövaren har åsidosatt sina skyldigheter enligt sådana rättsakter som har antagits med stöd av artikel 13.6 i CER-direktivet.

Utredningens förslag

Förslaget från utredningen stämmer i allt väsentligt överens med regeringens. Utredningen föreslår inte att tillsynsmyndigheten ska kunna ingripa om verksamhetsutövaren har åsidosatt sina skyldigheter enligt rättsakter som har antagits med stöd av artikel 13.6 i direktivet.

Remissinstanserna

Majoriteten av remissinstanserna tillstyrker eller yttrar sig inte över förslaget. *Naturvårdsverket* ifrågasätter av proportionalitets- och resurseffektivitetsskäl om det är lämpligt att göra tillsynsinsatser obligatoriska. *Transportstyrelsen* anser att det bör finnas en generell rätt för tillsynsmyndigheterna att ingripa vid överträdelser, liknande regleringen i 6 kap. 6 § säkerhetsskyddslagen.

Skälen för regeringens förslag

Utan att det påverkar möjligheten att ålägga sanktioner i enlighet med artikel 22 i CER-direktivet får de behöriga myndigheterna enligt artikel 21.3 i direktivet, efter de tillsynsåtgärder som avses i artikel 21.1 eller den bedömning av information som avses i artikel 21.2, beordra de berörda kritiska entiteterna att vidta de åtgärder som är nödvändiga och proportionella för att avhjälpa konstaterade överträdelser av direktivet, inom en rimlig tidsfrist som fastställs av de myndigheterna, och att lämna information om de åtgärder som har vidtagits till de myndigheterna (jfr avsnitt 10.2). Sådana förelägganden ska enligt artikel 21.3 framför allt ta hänsyn till hur allvarlig överträdelsen är.

Medlemsstaterna ska enligt artikel 21.4 i direktivet säkerställa att de befogenheter som anges i artikel 21.1–21.3 i CER-direktivet endast kan utövas om de omfattas av lämpliga skyddsåtgärder. Sådana skyddsåtgärder ska särskilt garantera att befogenheterna utövas på ett objektivt, öppet och proportionerligt sätt och att de berörda kritiska entiteternas rättigheter och legitima intressen, såsom skyddet av handels- och affärshemligheter, skyddas på vederbörligt sätt, däribland rätten att höras, rätten till försvar och rätten till rättslig prövning inför en oberoende domstol.

Av artikel 22 i CER-direktivet följer en skyldighet för medlemsstaterna att fastställa regler om sanktioner för överträdelse av de nationella åtgärder som antagits enligt direktivet och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande.

De överträdelser som bör kunna föranleda ingripanden enligt lagen är underlåtenhet att göra en anmälan för vissa kritiska verksamhetsutövare (avsnitt 7.1) och att göra en riskbedömning (avsnitt 8.1). Även underlåtenhet att vidta åtgärder för motståndskraft (avsnitt 8.2), inbegripet att

bland annat upprätta och tillämpa en plan för motståndskraft, göra en befattningsanalys som ska dokumenteras samt genomföra bakgrundskontroller (avsnitt 9), bör kunna föranleda ingripanden. Detsamma bör gälla för underlåtenhet att rapportera vissa incidenter (avsnitt 8.3).

Regeringen konstaterar att utredningens förslag om ingripanden gäller i förhållande till samtliga skyldigheter som följer av lagen och därmed finns en sådan generell rätt att ingripa genom åtgärdsföreläggande som *Transportstyrelsen* nämner. Tillsynsmyndigheten bör dock också kunna ingripa om verksamhetsutövaren har åsidosatt sina skyldigheter enligt sådana rättsakter som har antagits med stöd av artikel 13.6 i CER-direktivet (se avsnitt 10.1).

Tillsynsmyndigheten bör enligt utredningen vara skyldig att ingripa mot aktuella slags överträdelser. Detta bidrar enligt utredningens mening till likabehandling. *Naturvårdsverket* ifrågasätter om det är lämpligt att göra ingripanden obligatoriska. Eftersom flera olika slags ingripandemöjligheter föreslås införas anser regeringen inte att det finns något som talar emot ett obligatoriskt ingripande vid angivna slags överträdelser (se vidare avsnitt 11.3). Ett obligatoriskt ingripande vid överträdelser gäller enligt cybersäkerhetslagen och bör gälla även enligt den nya lagen (se vidare prop. 2025/26:28 s. 146).

11.3 Vilka möjligheter till ingripande bör finnas?

Regeringens förslag

Ingripande ska ske genom ett beslut om föreläggande, ett beslut om sanktionsavgift eller genom ett beslut om anmärkning. En anmärkning ska beslutas om tillsynsmyndigheten inte finner skäl att ingripa mot en överträdelse på något annat sätt.

Tillsynsmyndigheten ska få avstå från att ingripa om överträdelsen är ringa eller ursäktlig, eller om det annars med hänsyn till omständigheterna vore oskäligt att ingripa.

Utredningens förslag

Förslaget från utredningen stämmer överens med regeringens.

Remissinstanserna

Majoriteten av remissinstanserna tillstyrker eller har inga invändningar mot förslaget. *Affärsverket svenska kraftnät* för fram att det är viktigt att tillsynsmyndigheterna samverkar med varandra i de fall flera tillsynsmyndigheter utövar tillsyn och överväger ingripandeåtgärder mot samma verksamhetsutövare. *Drivkraft Sverige* anser att sanktionerna är otydliga och att dessa bör vara tydligt definierade och rimligt utformade. *Sveriges advokatsamfund* anser att regleringens huvudsyfte, att så långt som det är möjligt motverka att fel eller brister uppkommer, inte uppnås på ett effektivt sätt genom ingripanden i efterhand mot verksamhetsutövarna. Det bör enligt samfundet övervägas att ge tillsynsmyndigheterna möjligheter att ingripa mot verksamhetsutövares brister i det systematiska

och riskbaserade arbetet, för att säkerställa deras motståndskraft, samt fokusera tillsynen på detta område. Det bör enligt samfundet även uttryckligen anges att tillsynsmyndigheterna i enlighet med proportionalitetsprincipen ska välja en mindre ingripande åtgärd och att strängare åtgärder förbehålls de särskilt allvarliga fallen.

Länsstyrelsen i Västerbottens län anser att resonemanget kring vad som kan utgöra ringa överträdelser bör utvecklas ytterligare. Länsstyrelsen påpekar att utredningens förslag tar sikte på ofrivilliga överträdelser men anser att en ringa överträdelse till sin betydelse är en mindre allvarlig överträdelse, inte en ofrivillig överträdelse.

Skälen för regeringens förslag

Ingripandeåtgärder enligt den nya lagen

Regeringen bedömer, i likhet med utredningen, att tillsynsmyndigheten bör få ingripa genom att besluta om föreläggande eller om sanktionsavgift eller genom att göra en anmärkning. Detta motsvarar i allt väsentligt ordningen som gäller enligt 4 kap. 1 § andra stycket cybersäkerhetslagen. *Drivkraft Sverige* utvecklar inte på vilket sätt de föreslagna sanktionerna skulle vara otydliga. Regeringen bedömer dock inte att det krävs förtydliganden i fråga om vilka ingripanden som kan vidtas med stöd av lagen.

Det bör enligt *Sveriges advokatsamfund* uttryckligen anges att tillsynsmyndigheterna i enlighet med proportionalitetsprincipen ska välja en mindre ingripande åtgärd och att strängare åtgärder förbehålls de särskilt allvarliga fallen. Att tillsynsmyndighetens åtgärd ska vara proportionerlig kommer till uttryck i 5 § tredje stycket förvaltningslagen. Det behöver inte särskilt framgå av lagen att tillsynsmyndigheterna ska beakta proportionaliteten i de åtgärder som de vidtar inom ramen för sin tillsyn och vid ingripanden. En anmärkning bör beslutas om något annat ingripande inte görs, givet att tillsynsmyndigheten inte väljer att helt avstå från ett ingripande.

Som Sveriges advokatsamfund påpekar bör fokus i första hand vara att motverka att fel och brister uppstår. Ett föreläggande kan exempelvis syfta till att verksamhetsutövaren ska vidta mer effektiva och ändamålsenliga åtgärder för motståndskraft, vilket bidrar till ett skydd mot incidenter. Förelägganden ger också möjligheter att ingripa vid brister i det systematiska och riskbaserade arbetet och det behöver inte införas någon särskild reglering i detta avseende.

Möjlighet att avstå från ingripande

Enligt artikel 4.1 i sjunde tilläggsprotokollet till Europakonventionen får ingen lagföras eller straffas på nytt i en brottmålsrättegång i samma stat för ett brott för vilket han redan blivit slutligt frikänd eller dömd i enlighet med lagen och rättegångsordningen i denna stat (dubbelbestraffningsförbudet) (jfr även artikel 50 i Europeiska unionens stadga om de grundläggande rättigheterna). Enligt utredningen är det motiverat att införa en ventil som kan tillämpas om dubbelbestraffningsförbudet aktualiseras men även i andra situationer när ett ingripande skulle medföra oskäliga konsekvenser för verksamhetsutövaren, exempelvis om samma

incident redan har lett till kännbara sanktioner enligt något annat regelverk utan att dubbelbestraffningsförbudet aktualiseras.

Regeringen konstaterar att en tillsynsmyndighet enligt 4 kap. 1 § tredje stycket cybersäkerhetslagen får avstå från ett ingripande om någon annan tillsynsmyndighet har vidtagit åtgärder mot verksamhetsutövaren med anledning av överträdelsen och dessa åtgärder bedöms tillräckliga. Utformningen av undantaget enligt lagen som genomför CER-direktivet bör dock enligt utredningens mening i stället göras på ett liknande sätt som gäller på finansmarknadsområdet. Detta medför enligt utredningens förslag att undantag får ske om en överträdelse är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna vore oskäligt att besluta om en sanktion. Enligt utredningen bör det framhållas att oskälighet eller ursäktlighet inte kan anses föreligga om överträdelsen har uppstått till följd av omständigheter som ligger inom verksamhetsutövarens kontrollsfär, exempelvis hänförligt till rutiner, tid och prioriteringar. En ringa eller ursäktlig överträdelse skulle enligt utredningen kunna anses föreligga om överträdelsen berott på någon omständighet som verksamhetsutövaren varken kunnat eller borde ha förutsett eller kunnat påverka. Undantaget tar enligt utredningen sikte på situationer där ett ingripande exempelvis skulle anses strida mot dubbelbestraffningsförbudet eller anses oskäligt på grund av en annan myndighets ingripande mot samma överträdelse eller händelse. Det kan enligt utredningen röra sig om såväl en svensk som utländsk tillsynsmyndighets ingripande.

Liknande reglering som utredningen föreslår finns i till exempel 11 § lagen (2024:500) med kompletterande bestämmelser till EU:s dataförvaltningsförordning. Tillsynsmyndigheten får avstå från att ta ut en sanktionsavgift enligt den lagen, helt eller delvis, om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut avgiften. Ett skäl att sätta ned en avgift enligt lagen kan vara att leverantören av dataförmedlingstjänster eller en vidareutnyttjare har gjort allt som rimligen kan krävas för att förhindra den uppkomna skadan. Befrielse kan också övervägas när det är fråga om engångsföreteelser som inte ger intryck av att vara särskilt allvarliga och som inte har fått några uppenbara, eller i vart fall inte avsevärda, negativa konsekvenser. I bagatellartade fall bör någon avgift inte utgå. En sanktionsavgift bör vidare kunna sättas ned helt eller delvis om exempelvis en leverantör av dataförmedlingstjänster eller en vidareutnyttjare drabbas av flera sanktionsavgifter vid samma prövningstillfälle och den samlade reaktionen skulle bli alltför betungande. Det bör dock inte anses oskäligt att ta ut en sanktionsavgift enbart på grund av att överträdelsen exempelvis berott på att en leverantör av dataförmedlingstjänster eller en vidareutnyttjare inte känt till reglerna eller på grund av dålig ekonomi, tidsbrist eller bristande rutiner. Frågan om en avgift ska sättas ned ska avgöras efter en helhetsbedömning utifrån omständigheterna i det enskilda fallet. Möjligheten att sätta ned avgiften är en undantagsbestämmelse och bör tillämpas restriktivt. (Se vidare prop. 2023/24:73 s. 45 och 66)

Regeringen uttryckte i lagrådsremissen att utredningens förslag gällande undantagets utformning i stort bör genomföras trots att det skiljer sig åt från cybersäkerhetslagens utformning. Regeringen angav att skillnaden inte får någon praktisk betydelse. I lagrådsremissen uttryckte regeringen dock att det fanns skäl, som *Länsstyrelsen i Västerbottens län* anser, att gå

in närmare på vad som bör anses utgöra ringa överträdelser enligt den nya lagen. Som länsstyrelsen nämner finns det anledning att göra skillnad på ofrivilliga överträdelser och ringa överträdelser. Som länsstyrelsen resonerar kring bör uttrycket ringa i detta sammanhang ta sikte på överträdelser som är mindre allvarliga, till exempel en överträdelse som inte har fått några uppenbara negativa konsekvenser. Ursäktlighet bör i detta sammanhang innebära en möjlighet att beakta om en överträdelse är föranledd av ett beteende som av särskilda omständigheter är att betrakta som mindre klandervärt än annars. Så kan till exempel vara fallet om verksamhetsutövaren har gjort det som rimligen kan krävas för att förhindra en överträdelse. Förslaget ger också utrymme för att beakta om det på annat sätt skulle vara oskäligt med ett ingripande. I lagrådsremissen angavs även att en tillsynsmyndighet bör kunna avstå från ett ingripande om verksamhetsutövaren drabbas av flera sanktionsavgifter vid samma prövningstillfälle för olika slags överträdelser och den samlade reaktionen skulle bli alltför betungande. Tillsynsmyndigheten kan också, som angavs i lagrådsremissen, till exempel avstå från att ingripa om ett ingripande skulle riskera att bryta mot dubbelbestraffningsförbudet.

Lagrådet anser att en motsvarande regel som i cybersäkerhetslagen, om att tillsynsmyndigheten får avstå från ingripande om någon annan tillsynsmyndighet har vidtagit åtgärder mot verksamhetsutövaren med anledning av överträdelsen och dessa åtgärder bedöms tillräckliga, bör införas även i den nya lagen. Lagrådet anser vidare att det som anges i lagrådsremissen i fråga om när det är möjligt att avstå från ingripande är alltför kortfattat för att kunna utgöra en nöjaktig vägledning vid tillämpningen.

Regeringen bedömer inte att det finns skäl att göra någon ändring i förhållande till lagrådsremissens respektive utredningens förslag i fråga om undantagets utformning och vidhåller att skillnaden i förhållande till cybersäkerhetslagen inte får någon praktisk betydelse. Regeringen genomför därför inte Lagrådets förslag i denna del. Motsvarande resonemang om undantagets tillämplighet finns i till exempel förarbetena till lagen med kompletterande bestämmelser till EU:s dataförvaltningsförordning (se vidare prop. 2023/24:73 s. 45 och 66). Regeringen bedömer inte att det krävs något tillägg i denna del.

En myndighet ska, enligt 6 § myndighetsförordningen, verka för att genom samarbete med bland annat andra myndigheter ta till vara de fördelar som kan vinnas för enskilda och för staten som helhet. Enligt 8 § förvaltningslagen ska en myndighet vidare inom sitt verksamhetsområde samverka med andra myndigheter och i rimlig utsträckning hjälpa den enskilde genom att själv inhämta upplysningar eller yttranden från andra myndigheter. Regeringen utgår ifrån att samverkan mellan tillsynsmyndigheterna, som *Affärsverket svenska kraftnät* resonerar kring, kommer att fungera väl när det gäller bland annat sådana frågor som behöver hanteras gemensamt.

11.4 Förelägganden vid behov

Regeringens förslag

Tillsynsmyndigheten ska få besluta de förelägganden som behövs för att en kritisk verksamhetsutövare ska fullgöra sina skyldigheter att göra en anmälan, göra en riskbedömning, vidta åtgärder för motståndskraft eller rapportera incidenter enligt lagen eller enligt föreskrifter som har meddelats i anslutning till lagen. Tillsynsmyndigheten ska också få besluta de förelägganden som behövs för att en kritisk verksamhetsutövare ska fullgöra sina skyldigheter enligt sådana rättsakter som har antagits med stöd av artikel 13.6 i CER-direktivet.

Ett föreläggande ska få förenas med vite. Ett vitesföreläggande ska även få riktas mot staten.

Utredningens förslag

Förslaget från utredningen stämmer i allt väsentligt överens med regeringens. Utredningen föreslår att det ska införas en bestämmelse i lagen om att tillsynsmyndigheten ska få bestämma att ett föreläggande ska gälla omedelbart. I utredningens förslag anges inte att ett vitesföreläggande även ska få riktas mot staten.

Remissinstanserna

Majoriteten av remissinstanserna tillstyrker eller yttrar sig inte över förslaget. *Energiföretagen Sverige* för fram att vitesförelägganden kan vara ett effektivt verktyg för att säkerställa att nödvändiga åtgärder vidtas. Energiföretagen Sverige anser att vitesbeloppet bör vara proportionerligt i förhållande till risken och kostnaden för att genomföra åtgärderna. *Stockholms kommun* för bland annat fram att förelägganden bör utfärdas med en tidsfrist som är relevant i förhållande till den risk eller skada som bristen medför eller kan komma att medföra.

Skälen för regeringens förslag

I enlighet med förslaget i avsnitt 11.3 bör en tillsynsmyndighet få ingripa genom föreläggande. Tillsynsmyndigheten bör få besluta de förelägganden som behövs för att verksamhetsutövaren ska fullgöra de skyldigheter som anges i avsnitt 11.2. *Stockholms kommun* för bland annat fram att förelägganden bör utfärdas med en tidsfrist som är relevant i förhållande till den risk eller skada som bristen medför eller kan komma att medföra. Det finns dock ingen anledning att närmare reglera tidsfrister kopplat till förelägganden i lagen.

Föreläggandena bör kunna förenas med vite. Ett sådant bör, av samma skäl som anges i avsnitt 10.2, även få riktas mot staten. Allmänna bestämmelser om viten finns, som anges i samma avsnitt, i viteslagen. *Energiföretagen Sverige* anser att vitesbeloppet bör vara proportionerligt i förhållande till risken och kostnaden för att genomföra åtgärderna. När vite föreläggs med stöd av viteslagen, ska det enligt 3 § den lagen, fastställas till ett belopp som med hänsyn till vad som är känt om adressatens

ekonomiska förhållanden och till omständigheterna i övrigt kan antas förmå honom att följa det föreläggande som är förenat med vitet. Regeringen anser, i likhet med utredningen, att viteslagens bestämmelser bör vara tillämpliga gällande sådana förelägganden som meddelas med stöd av den nya lagen. Skyldigheten att beakta passivitetsrätten vid förelägganden behandlas i avsnitt 10.2.

Lagrådet anser att förhållandet till passivitetsrätten bör regleras i lagen. Regeringen konstaterar att sådan reglering inte förekommer i andra motsvarande regleringar och inte heller krävs för att en myndighet vid beslut om föreläggande ska vara skyldig att beakta passivitetsrätten. Lagrådets förslag i denna del genomförs därför inte.

Utredningen föreslår att det ska införas en bestämmelse om att tillsynsmyndigheten ska få bestämma att ett föreläggande ska gälla omedelbart. Mot bakgrund av möjligheterna som förvaltningslagen ger i detta avseende i förhållande till enskilda, och som redogörs för i avsnitt 10.2, bedömer regeringen att det inte behöver införas någon sådan bestämmelse som utredningen föreslår.

11.5 Sanktionsavgifter

11.5.1 När bör en sanktionsavgift få tas ut?

Regeringens förslag

Tillsynsmyndigheten ska få besluta att ta ut en sanktionsavgift av en verksamhetsutövare om verksamhetsutövaren har åsidosatt sina skyldigheter att göra en anmälan, genomföra en riskbedömning, vidta åtgärder för motståndskraft eller rapportera incidenter enligt lagen eller enligt föreskrifter som har meddelats i anslutning till lagen. Tillsynsmyndigheten ska också få ta ut en sanktionsavgift av en kritisk verksamhetsutövare som har åsidosatt sina skyldigheter enligt sådana rättsakter som antagits med stöd av artikel 13.6 i CER-direktivet.

Utredningens förslag

Förslaget från utredningen stämmer överens med regeringens.

Remissinstanserna

Advokatfirman Kahn Pedersen anser att det bör det tydliggöras att det är tillsynsmyndigheten som har bevisbördan för att en överträdelse har skett, dess allvar och för övriga omständigheter som ska beaktas i fråga om sanktionsavgiftens storlek. Advokatfirman anser även att beviskravet bör lagregleras. Advokatfirman betonar vidare vikten av en tydlig reglering. *Luleå kommun* och *Stockholms Hamn AB* anser att tillsynsmyndigheterna bör prioritera att verka för förändring genom förelägganden. Luleå kommun förordar att tillsynsmyndigheterna initialt har en mer stödjande roll jämfört med att direkt besluta om sanktionsavgift. *Malmö kommun* är positiv till utredningens förslag om att det inte ska vara obligatoriskt för

tillsynsmyndigheten att ta ut sanktionsavgift. Övriga remissinstanser yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag

I svensk rätt finns sanktionsavgifter på många områden. Sanktionsavgifter är till skillnad från vitessanktionerade åtgärdsförelägganden i huvudsak en tillbakaverkande sanktion som är handlingsdirigerande genom att verka avskräckande. Om en sanktionsavgift riskerar att innebära en kostnad eller förlust som är lika stor som eller större än den besparing som görs genom att regelverket inte följs, skapar avgiften ett incitament att undvika överträdelser. Till skillnad från NIS 2-direktivet innehåller CER-direktivet inte några bestämmelser om vilka överträdelser som ska leda till sanktionsavgift (jfr prop. 2025/26:28 s. 167 f.). Regeringen bedömer dock att sanktionsavgift bör kunna aktualiseras om verksamhetsutövaren har åsidosatt sina skyldigheter att göra en anmälan, genomföra en riskbedömning, vidta åtgärder för motståndskraft eller rapportera incidenter enligt lagen eller enligt föreskrifter som har meddelats i anslutning till lagen (se avsnitt 7.1 och 8.1–8.3). Tillsynsmyndigheten bör också kunna ingripa med en sanktionsavgift om verksamhetsutövaren har åsidosatt sina skyldigheter enligt sådana rättsakter som har antagits med stöd av artikel 13.6 i CER-direktivet.

Det är, som utredningen föreslår, lämpligt att det är en tillsynsmyndighet som ska kunna pröva och besluta om sanktionsavgifter. Det är tillsynsmyndigheterna som genom sin sakkunskap kommer att ha eller kommer att kunna skaffa sig bäst förutsättningar för att bedöma om en överträdelse har skett. Om en tillsynsmyndighet fattar beslut om sanktionsavgift, kan det dessutom antas att handläggningen i regel blir snabbare än om en domstol skulle fatta beslut efter ansökan av myndigheten. Genom regeringens förslag i avsnitt 12 om att ett beslut om sanktionsavgift ska kunna överklagas till domstol tillgodoses också rättssäkerhetsaspekterna för den som blir föremål för en sanktionsavgift och det kommer också att bildas domstolspraxis till vägledning för tillsynsmyndigheternas kommande beslut.

Systemet bör, som utredningen bedömer, bygga på ett strikt ansvar. Detta innebär att avgiften ska kunna tas ut oberoende av om överträdelsen har varit uppsåtlig eller berott på oaktsamhet. Strikt ansvar innebär emellertid inte, som *Malmö kommun* nämner, att sanktionsavgift ska tas ut vid varje överträdelse. Det bör ankomma på tillsynsmyndigheten att bedöma om en överträdelse ska leda till en sanktionsavgift i det enskilda fallet (jfr till exempel prop. 2022/23:116 s. 123).

Lagrådet anser att det, som i cybersäkerhetslagen, bör framgå av den nya lagen vilka omständigheter som ska anses tala för att en sanktionsavgift ska tas ut. Regeringen anser inte att detta är nödvändigt av följande skäl. För det första bör det beaktas att den nya lagen, till skillnad mot cybersäkerhetslagen, föreslås innehålla reglering om endast tre olika slags ingripandeåtgärder. Ingripande föreslås kunna ske genom ett beslut om föreläggande som kan förenas med vite, ett beslut om sanktionsavgift eller ett beslut om anmärkning. En anmärkning ska, enligt förslaget i avsnitt 11.3, beslutas endast om tillsynsmyndigheten inte finner skäl att ingripa mot en överträdelse på något annat sätt, det vill säga genom ett beslut om

föreläggande eller ett beslut om sanktionsavgift. Möjligheten att helt avstå från ett ingripande behandlas i samma avsnitt.

Som konstateras ovan och har konstaterats i flera andra lagstiftningsärenden är en sanktionsavgift, till skillnad från ett föreläggande som förenas med vite, i huvudsak en tillbakaverkande sanktion som är handlingsdirigerande genom att verka avskräckande (se till exempel prop. 2020/21:194 s. 89). Om en sanktionsavgift riskerar att innebära en kostnad eller förlust som är lika stor som eller större än den besparing som görs genom att regelverket inte följs, skapar avgiften ett incitament att undvika överträdelser. En verksamhetsutövare kan, av bland annat affärsmässiga skäl, ha incitament att vilja undvika en situation då ett beslut om anmärkning fattas. Ett beslut om anmärkning kan i sig därmed också verka avskräckande och anses vara en tillbakaverkande sanktion. Ett beslut om anmärkning får dock inte samma slags direkta effekter som ett beslut om sanktionsavgift.

Regeringen bedömer att det inte finns någon risk för att en tillsynsmyndighet skulle besluta om en sanktionsavgift i en situation då det hade varit mer ändamålsenligt och dessutom tillräckligt att besluta om ett vitesföreläggande eller en anmärkning (jfr 5 § tredje stycket förvaltningslagen). Det bör dessutom noteras att det finns ett stort antal lagar som är utformade på liknande sätt som regeringen föreslår i detta lagstiftningsärende, till exempel lagen (2018:1698) om domstolarnas behandling av personuppgifter inom brottsdatalagens område, lagen (2022:368) om nationella järnvägssystem och lagen (2026:966) om utsedda verksamhetsställen och rättsliga ombud för inhämtning av elektroniska bevis. Sammanfattningsvis bör Lagrådets förslag i denna del inte genomföras.

Lagrådet anser även att det finns ett behov av en sammanhållen lagstiftning som behandlar de övergripande materiella och processuella förutsättningarna för sanktionsavgifter. Regeringen kan, liksom Lagrådet, konstatera att det finns ett stort antal författningar som innehåller olika typer av system för sanktionsavgifter. Det finns emellertid inte utrymme för att inom ramen för detta lagstiftningsärende göra en sådan översyn som Lagrådet nämner.

Regeringen bedömer att tillsynsmyndigheten bör kunna besluta om sanktionsavgift även om den tidigare har ingripit på något annat sätt (se dock om dubbelbestraffningsförbudet i exempelvis avsnitt 11.3). I enlighet med bland annat 5 § tredje stycket förvaltningslagen ska beslut som tillsynsmyndigheten fattar vara proportionerliga. *Luleå kommun* och *Stockholms Hamn AB* anser att tillsynsmyndigheterna bör prioritera att verka för förändring genom förelägganden. Regeringen bedömer, som anges ovan, att det inte finns någon risk för att en tillsynsmyndighet kommer att besluta om sanktionsavgift som förstahandsalternativ i en situation då det hade varit tillräckligt att besluta om ett föreläggande. Tillsynsmyndigheten bör dock också kunna besluta om sanktionsavgift utan att ha ingripit tidigare om det är motiverat i det enskilda fallet.

Regeringen konstaterar, som *Advokatfirman Kahn Pedersen*, att tillsynsmyndigheten kommer att ha ansvar för att visa att en överträdelse har skett. När det gäller frågan om vilket beviskrav som gäller konstaterar regeringen att det i förvaltningsprocessen inte finns något för alla situationer gällande beviskrav utan att beviskravet varierar med hänsyn till sakens beskaffenhet (se till exempel HFD 2013 ref. 61). Beviskrav i

förvaltningsmål bör dock, för det fall aktuell reglering inte ger någon ledning i frågorna, ses i ljuset av 8 § förvaltningsprocesslagen (1971:291) där det anges att det är domstolens ansvar att varje mål blir så pass utrett som dess beskaffenhet kräver.

Utredningen föreslår inte att det ska regleras i lagen vilket beviskrav som gäller. Någon sådan reglering finns inte heller i till exempel säkerhetsskyddslagen, cybersäkerhetslagen eller lagen (2023:560) om granskning av utländska direktinvesteringar. Regeringen bedömer att det inte bör regleras särskilt vilket beviskrav som gäller i aktuella ärenden. Det blir i stället ytterst upp till en domstol att vid ett överklagande avgöra huruvida det är utrett att en överträdelse har skett. Den reglering som föreslås i denna proposition motsvarar sådan som finns på andra områden, till exempel cybersäkerhetslagen. Regeringen kan därför inte se att det i övrigt skulle krävas några förtydliganden, som Advokatfirman Kahn Pedersen resonerar kring, för att generella krav på förutsebarhet ska vara uppfyllda.

11.5.2 Sanktionsavgiftens storlek

Regeringens förslag

För enskilda verksamhetsutövare ska sanktionsavgiften bestämmas till lägst 5 000 kronor och till högst det högsta av 2 procent av verksamhetsutövarens totala globala årsomsättning under närmast föregående räkenskapsår, och ett belopp i kronor motsvarande 10 000 000 euro.

För offentliga verksamhetsutövare ska avgiften bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor.

Utredningens förslag

Förslaget från utredningen stämmer i allt väsentligt överens med regeringens. Utredningen föreslår att maximibeloppen ska anges enbart i euro när det är fråga om enskilda verksamhetsutövare. I utredningens förslag anges inte att det ska röra sig om närmast föregående räkenskapsår.

Remissinstanserna

Majoriteten av remissinstanserna tillstyrker förslaget eller har inga synpunkter på förslaget. *Advokatfirman Kahn Pedersen* förordar att det tydliggörs att sanktionsavgifter i den övre halvan av det föreslagna beloppsintervallet endast bör komma i fråga för mycket allvarliga överträdelser. *Energiföretagen Sverige* ser en risk för att flera tillsynsärenden inom samma koncern kan resultera i ackumulerade vites- eller sanktionsbelopp överstigande 2 procent av den globala årsomsättningen samt att sanktionerna kan bli oproportionerliga och riskera företagens konkurrensvillkor. *Luleå kommun* påpekar att tillsyn kan initieras både enligt den nya lagen och cybersäkerhetslagen och bedömer att sanktionsavgift inom närbesläktade områden måste beaktas. Luleå kommun bedömer också att sanktionsavgifter kan få icke ändamålsenliga effekter för små och medel-

stora verksamheter. *Rymdstyrelsen* anser att sanktionsavgifterna bör anges i svenska kronor.

Malmö kommun är positiv till att sanktionsavgiftens storlek för offentliga verksamhetsutövare är på samma nivå som i cybersäkerhetslagen. *Säffle kommun* ser det som positivt att man inför sanktionsavgifter men anser att avgifterna ska rymmas inom befintliga budgetramar.

Några remissinstanser har synpunkter i fråga om hur verksamhetsformen kan påverka sanktionsavgiftens storlek. Malmö kommun och *Svenskt Vatten* för fram att utredningens förslag innebär att kommunala bolag kan vara enskilda verksamhetsutövare medan kommunalförbund räknas som offentliga verksamhetsutövare. Remissinstanserna anger att detta är problematiskt eftersom ett kommunalt bolag då kan få högre sanktionsavgifter än ett kommunalförbund, trots att skillnaden mellan dessa aktörer kan vara enbart verksamhetsformen. *Region Stockholm* är av samma åsikt och för fram att valet av förvaltningsform för en uppgift som endast det allmänna kan vara huvudman för inte bör vara avgörande för sanktionsavgiftens storlek.

Skälen för regeringens förslag

I CER-direktivet saknas angivelser om sanktionsavgifternas storlek men utredningen föreslår att liknande reglering som finns i cybersäkerhetslagen bör införas i den nya lagen (se 4 kap. 10 § 1 och 3 cybersäkerhetslagen). Att använda samma beräkningsgrund och maximibelopp skulle, som utredningen resonerar om, kunna bidra till att skapa en enhetlig praxis för närliggande regelverk. Regeringen anser därför att utredningens förslag i denna del bör genomföras. I likhet med *Rymdstyrelsen* anser regeringen att sanktionsavgifterna bör anges i svenska kronor. Det bör, i förhållande till utredningens förslag, anges att det är närmast föregående räkenskapsår som är av intresse vid bedömningen (jfr prop. 2025/26:28 s. 169 f. och artikel 34.4 i NIS 2-direktivet). Uttrycket tar, som *Lagrådet* efterfrågar ett förtydligande om, sikte på det räkenskapsår som är närmast föregående sett till när bedömningen av sanktionsavgiftens storlek görs. Det finns flera exempel på regleringar som inte innehåller något förtydligande om detta i lagtexten (se till exempel lagen [2016:429] om tillsyn över företag av allmänt intresse i fråga om revision och cybersäkerhetslagen). Regeringen anser inte att det krävs något förtydligande i lagen och genomför därför inte Lagrådets förslag i denna del.

Några remissinstanser, däribland *Svenskt Vatten*, har synpunkter i fråga om hur verksamhetsformen kan påverka sanktionsavgiftens storlek. Regeringen anser att det inte skulle vara rimligt att göra skillnad på kommunala bolag och de företag som i övrigt räknas som verksamhetsutövare när det gäller vilken sanktionsavgift som kan aktualiseras. Sådan skillnad görs inte heller i cybersäkerhetslagen.

Energiföretagen Sverige anser att det finns en risk för att flera tillsynsärenden aktualiseras inom samma koncern och bedömer att förslaget kan få oproportionerliga effekter. Enligt regeringens mening ska separata bedömningar göras för varje rättssubjekt, det vill säga för varje juridisk person, i fråga om det bedriver sådan verksamhet som omfattas av lagen och därmed även i fråga om vilken sanktionsavgift som ska utgå för

det fall en sådan beslutas (jfr prop. 2025/26:28 s. 52). Det är därmed också det enskilda rättssubjektets globala årsomsättning, det vill säga intäkter från försäljning av varor och tjänster mätt över hela världen, som är av relevans vid fastställande av sanktionsavgiftens storlek. För det fall flera verksamhetsutövare inom samma koncern gör sig skyldiga till överträdelser av den nya lagen bör det inte tas någon hänsyn till den sammanlagda påverkan på koncernen. Utrymmet för att avstå ingripande i form av till exempel beslut om sanktionsavgift med hänvisning till att sanktionsavgift har beslutats för samma överträdelse eller att en sanktionsavgift skulle vara oskälig, som *Luleå kommun* resonerar om, behandlas i avsnitt 11.3.

Säffle kommun anser att sanktionsavgifterna ska rymmas inom befintliga budgetramar. Vilka omständigheter som bör beaktas särskilt vid bestämmande av sanktionsavgiftens storlek behandlas i avsnitt 11.5.3. Belopp i den övre delen av de föreslagna beloppsintervallen bör, som *Advokatfirman Kahn Pedersen* anger, komma i fråga endast för mycket allvarliga överträdelser (jfr till exempel prop. 2022/23:116 s. 129).

11.5.3 Omständigheter att särskilt beakta vid bestämmande av sanktionsavgiftens storlek

Regeringens förslag

När sanktionsavgiftens storlek bestäms ska särskild hänsyn tas till

1. den skada eller risk för skada som har uppstått till följd av överträdelsen,
2. om den kritiska verksamhetsutövaren tidigare har gjort sig skyldig till en överträdelse, och
3. den ekonomiska fördel som överträdelsen har inneburit för verksamhetsutövaren.

Utredningens förslag

Förslaget från utredningen stämmer i allt väsentligt överens med regeringens. I utredningens förslag anges att särskild hänsyn ska tas till de kostnader som den kritiska verksamhetsutövaren har undvikit till följd av överträdelsen i stället för den ekonomiska fördel som överträdelsen har inneburit för denne.

Remissinstanserna

Majoriteten av remissinstanserna tillstyrker eller yttrar sig inte över förslaget. *Energiföretagen Sverige* önskar ett förtydligande av hur storleken på viten och sanktionsavgifter fastställs och hur det påverkar ett mindre dotterbolag inom en större koncern. *Malmö kommun* instämmer i uppfattningen att omständigheterna i det enskilda fallet ska avgöra sanktionsavgiftens storlek och att den kritiska verksamhetsutövarens ekonomiska styrka ska påverka bedömningen. *Naturvårdsverket* anser att den föreslagna bestämmelsen bör ses över eftersom den innebär ett stort tolkningsutrymme, vilket kan leda till svårigheter att avgöra graden av

vållande och därmed även sanktionsavgiftens storlek. Naturvårdsverket anser att det bör övervägas om tillsynsmyndigheten ska ansöka hos en domstol om att få sanktionsbeloppet fastställt. *Salems kommun* lyfter fram att en kommun kan bedriva flera kritiska verksamheter som tillhör flera olika sektorer. Eftersom sektorerna omfattas av olika tillsynsområden bör man vid bestämmande av eventuella sanktionsavgifter ta hänsyn till den nämnd som den kritiska offentliga verksamheten tillhör, inte till kommunen i stort. Till exempel *Säkerhetspolisen* anser att det bör övervägas om det vid bedömningen av sanktionsavgiftens storlek även ska beaktas vad verksamhetsutövaren har gjort för att överträdelsen ska upphöra och för att begränsa dess verkningar.

Skälen för regeringens förslag

CER-direktivet saknar, till skillnad från NIS 2-direktivet, bestämmelser om vad som ska beaktas vid bestämmande av sanktionsavgiftens storlek (jfr prop. 2025/26:28 s. 150 f.). Utredningen anser att samtliga relevanta omständigheter bör beaktas när en sanktionsavgifts storlek ska bestämmas i det enskilda fallet. Detta bör dock inte anges i lagen enligt utredningen. I stället anser utredningen att vissa omständigheter som ska beaktas i försvårande riktning särskilt bör anges i lagen.

Enligt utredningens bedömning finns det skäl att ta särskild hänsyn till den skada eller risk för skada som har uppstått till följd av överträdelsen, tidigare överträdelser och kostnader som har undvikits till följd av överträdelsen. Det bör enligt utredningen noteras att uppräkningen inte är uttömmande, utan att flera av de omständigheter som nämns i utredningens delbetänkande kan vara av relevans för bedömningen, exempelvis hur lång tid en överträdelse har pågått.

Vid valet av ingripande enligt 4 kap. 2 § cybersäkerhetslagen ska hänsyn tas till hur allvarlig överträdelsen är, hur länge den har pågått och den skada eller risk för skada som uppstått till följd av överträdelsen. Vid bedömningen ska särskilt beaktas om verksamhetsutövaren tidigare har gjort sig skyldig till en överträdelse, vad verksamhetsutövaren har gjort för att förhindra eller minska skadan, om överträdelsen har varit uppsåtlig eller berott på oaktsamhet, och den ekonomiska fördel som överträdelsen har inneburit för verksamhetsutövaren. Vad avser omständigheten att verksamhetsutövaren tidigare har gjort sig skyldig till en överträdelse så bör det vid bedömningen bland annat vägas in tiden mellan den tidigare och den aktuella överträdelsen och om överträdelserna är likartade (se prop. 2025/26:28 s. 258).

Regeringen bedömde vid införandet av cybersäkerhetslagen att det inte skulle vara ett alternativ att enbart beakta ovan angivna omständigheter kopplat till överväganden om sanktionsavgift (se vidare prop. 2025/26:28 s. 150 f.). Omständigheterna ansågs vara relevanta att beakta vid valet av ingripande. Regeringen uttryckte i lagrådsremissen, eftersom färre alternativ för ingripanden föreslås finnas enligt den nya lagen än enligt cybersäkerhetslagen, att det finns skäl att utforma regleringen i den nya lagen på ett annat sätt. Regeringen angav dock att de omständigheter som ska beaktas särskilt bör formuleras om för att bättre stämma överens med utformningen av cybersäkerhetslagen.

Lagrådet anser att det framstår som ologiskt att ange vad som särskilt ska beaktas vid bedömningen när det inte finns någon grundbestämmelse om vilka omständigheter som det mera allmänt ska tas hänsyn till. Lagrådet har också synpunkter på de omständigheter som ska beaktas särskilt enligt förslaget. Det borde enligt Lagrådet snarare vara nivån på bristerna i åtgärderna för motståndskraft som skulle spela särskild roll vid avgörandet av sanktionsavgiftens storlek än omfattningen av en inträffad skada eller vilken risk för skada som har uppstått. Hur stor skadan i ett enskilt fall blir, eller hur stor risken för skada bedöms vara, kan enligt Lagrådet inte sällan ha mera med slumpen att göra än vara avhängigt nivån på den försummelse som har bidragit till skadan eller skaderisken. Lagrådet anser vidare att det inte går ihop att hänsyn ska tas till om verksamhetsutövaren tidigare har gjort sig skyldig till en överträdelse. Uttrycket gjort sig skyldig till innefattar enligt Lagrådet att verksamhetsutövaren har ådragit sig någon form av skuld men i författningskommentaren anges att verksamhetsutövarens större eller mindre skuld inte har någon betydelse när en sanktionsavgift ska beslutas. Beträffande det som sägs om att särskild hänsyn ska tas till den ekonomiska fördel som överträdelsen har inneburit för verksamhetsutövaren, påpekar Lagrådet att det långt ifrån är givet att ett åsidosättande av något åliggande enligt lagen leder till någon ekonomisk fördel.

Som anges i avsnitt 11.5.1 bör vissa grundläggande omständigheter beaktas vid bedömningen av om en sanktionsavgift ska tas ut. Regeringen konstaterar att motsvarande reglering som föreslås i lagrådsremissen, som anger endast vilka omständigheter som särskilt ska beaktas när sanktionsavgiftens storlek bestäms, finns i flera andra lagar (se till exempel lagen om utsedda verksamhetsställen och rättsliga ombud för inhämtning av elektroniska bevis). När det gäller vilka omständigheter som ska beaktas särskilt enligt förslaget i lagrådsremissen konstaterar regeringen att även dessa har motsvarigheter i andra lagar (se till exempel säkerhetsskyddslagen och lagen om granskning av utländska direktinvesteringar). Regeringen finner inte anledning att göra någon ändring med anledning av Lagrådets synpunkter i denna del. Regeringen vill också framhålla att det på goda grunder finns skäl att anta att en verksamhetsutövare som till exempel avstår från att vidta åtgärder för motståndskraft kan få en ekonomisk fördel av sin underlåtenhet eftersom sådana åtgärder kan innebära kostnader.

Flera remissinstanser, bland andra *Säkerhetspolisen,* anser att andra omständigheter än de som utredningen nämner bör kunna påverka bedömningen av sanktionsavgiftens storlek. Regeringen instämmer i den uppfattningen men konstaterar, i likhet med utredningen, att uppräkningen i den nya lagen inte är uttömmande. Det finns därmed utrymme att beakta fler och andra omständigheter vid bedömningen. Regeringen anser dock, till skillnad från *Naturvårdsverket*, inte att detta innebär ett för stort tolkningsutrymme. Varför det enligt regeringens bedömning är godtagbart att en tillsynsmyndighet beslutar om en sanktionsavgift, jämfört med en domstol, behandlas i avsnitt 11.5.1. *Energiföretagen Sverige* önskar ett förtydligande av hur storleken på viten och sanktionsavgifter fastställs och hur det påverkar ett mindre dotterbolag inom en större koncern. Dessa frågor behandlas i avsnitt 11.4 och 11.5.1.

Salems kommun lyfter fram att hänsyn bör tas till vilken nämnd som den kritiska verksamheten tillhör. Lagen föreslås gälla för en kommun som helhet om kommunen identifieras som kritisk (se avsnitt 5.2). Det finns ingen anledning att göra något ytterligare förtydligande i lagen i fråga om vilken del av kommunerna som ett eventuellt beslut om sanktionsavgift ska riktas till (jfr prop. 2025/26:28 s. 169).

11.5.4 Förfarandet vid beslut om sanktionsavgift

Regeringens förslag

En sanktionsavgift ska inte få beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

En sanktionsavgift ska få beslutas endast om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum. Ett beslut om sanktionsavgift ska delges.

En sanktionsavgift ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet. Om sanktionsavgiften inte betalas i rätt tid, ska tillsynsmyndigheten lämna den obetalda avgiften för indrivning. Det ska tas in en bestämmelse i lagen som upplyser om att bestämmelser om indrivning finns i lagen om indrivning av statliga fordringar m.m.

Sanktionsavgiften ska tillfalla staten.

En sanktionsavgift ska falla bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

Utredningens förslag

Förslaget från utredningen stämmer i allt väsentligt överens med regeringens. Utredningen föreslår att det ska införas en bestämmelse som innebär att ett beslut om sanktionsavgift ska få verkställas enligt utsökningsbalken.

Remissinstanserna

Majoriteten av remissinstanserna tillstyrker eller yttrar sig inte över förslaget. *Affärsverket svenska kraftnät* lyfter fram att tillsynsmyndighetens möjligheter att ingripa mot allvarligare fall kan begränsas genom den mycket korta preskriptionstid som föreslås. Den utredning som krävs i allvarligare typer av ärenden kan ta lång tid att få fram. Affärsverket svenska kraftnät föreslår därför att en sanktionsavgift ska få beslutas om den som anspråket har riktas mot getts tillfälle att yttra sig inom fem år från det att överträdelsen ägde rum.

Skälen för regeringens förslag

Rätten att yttra sig och om delgivning av beslut om sanktionsavgift

Den som riskerar att påföras en sanktionsavgift bör ges tillfälle att yttra sig innan tillsynsmyndigheten fattar beslut om en sådan avgift. Verksamhetsutövaren ges därigenom möjlighet att till exempel påtala eventuella felaktigheter och omständigheter som kan utgöra skäl för att helt eller delvis efterge avgiften.

På grund av sanktionsavgiftens ingripande natur bör det finnas en bortre tidsgräns för när en sanktionsavgift ska få beslutas. Utredningen anser att en sanktionsavgift bör få beslutas endast om den som anspråket riktas mot har getts tillfälle att yttra sig inom två år från överträdelsen. *Affärsverket svenska kraftnät* föreslår att en tidsfrist om fem år. Regeringen konstaterar att utredningens förslag motsvarar exempelvis säkerhetsskyddslagens utformning och den reglering som finns i cybersäkerhetslagen och bedömer att samma ordning bör gälla enligt den nya lagen.

Om kommunikation enligt 25 § förvaltningslagen inte har skett med den som avgiften ska tas ut av inom angiven tid, får en sanktionsavgift därmed inte tas ut. Det är tillsynsmyndighetens ansvar att kontrollera att kommunikation har skett. Ett beslut om en sanktionsavgift är en särskilt ingripande åtgärd. Sådana beslut bör därför delges den avgiftsskyldige enligt delgivningslagen (2010:1932).

Betalning, indrivning och preskription

En sanktionsavgift bör tillfalla staten. Det bör också föreskrivas att avgiften ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om avgiften har fått laga kraft eller inom den längre tid som anges i beslutet. Om sanktionsavgiften inte betalas i tid, bör myndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m.

Utredningen föreslår att det ska införas en bestämmelse som innebär att ett beslut om sanktionsavgift ska få verkställas enligt utsökningsbalken. Genom en lagändring som trädde i kraft den 1 september 2022 får de aktuella besluten med stöd av 3 kap. 1 § första stycket 6 a utsökningsbalken verkställas enligt samma balk även utan en sådan bestämmelse som utredningen föreslår (se prop. 2021/22:206). Utredningens förslag i denna del bör därför inte genomföras.

Som utredningen bedömer bör möjligheten att kräva in en beslutad sanktionsavgift falla bort i den utsträckning som verkställighet inte har skett inom fem år från det att beslutet fick laga kraft. Kravet att ett beslut om sanktionsavgift ska delges innebär att beslutet får laga kraft tre veckor efter det att den avgiftsskyldige har delgetts beslutet.

Dubbelbestraffningsförbudet och hinder mot beslut om sanktionsavgift

Som har konstaterats i flera lagstiftningsärenden får straff, i den mening som avses i Europakonventionen, anses omfatta vite (jfr avsnitt 11.3). Om ett vite har dömts ut, bör det därför inte vara möjligt att besluta om en sanktion, varken administrativ eller straffrättslig, för samma sak. Den avgörande tidpunkten för när sådant hinder uppkommer bör vara när det inleds en domstolsprocess angående frågan om att döma ut vite. Ett

föreläggande om vite bör därför inte hindra ett senare ingripande med sanktionsavgift så länge som en myndighet inte har ansökt om utdömande av vitet. När tillsynsmyndigheten har ansökt om att vitet ska dömas ut bör myndigheten dock vara förhindrad att besluta om en sanktionsavgift för en överträdelse som omfattas av vitesföreläggandet. En bestämmelse om detta bör tas in i den nya lagen.

12 Överklagande

Regeringens förslag

Beslut enligt lagen ska få överklagas till allmän förvaltningsdomstol.

Den beslutande myndigheten ska vid ett överklagande vara motpart i domstolen.

Det ska krävas prövningstillstånd vid överklagande till kammarrätten.

Utredningens förslag

Förslaget från utredningen stämmer i allt väsentligt överens med regeringens. Utredningen föreslår att även beslut enligt anslutande föreskrifter ska få överklagas.

Remissinstanserna

Majoriteten av remissinstanserna tillstyrker eller yttrar sig inte över förslaget. *Advokatfirman Kahn Pedersen* instämmer i utredningens uppfattning att beslut om att en verksamhet omfattas av den föreslagna lagen ska kunna överklagas och inhiberas. *Länsstyrelsen i Västra Götalands län* och *Sveriges advokatsamfund* för fram att ett överklagande som gäller en tillsynsmyndighets beslut om att identifiera en verksamhetsutövare som kritisk bör handläggas med förtur.

Skälen för regeringens förslag

Rätten att överklaga beslut

Enligt 40 § förvaltningslagen överklagas beslut till allmän förvaltningsdomstol och prövningstillstånd krävs vid överklagande till kammarrätten. Enligt 41 § samma lag får ett beslut överklagas om det kan antas påverka någons situation på ett inte obetydligt sätt. Det är beslutets faktiska verkningar som avgör om det är överklagbart och prövningen av om ett visst beslut kan antas påverka någons situation utgår från en objektiv bedömning som tar sikte på beslutets faktiska verkningar, främst i förhållande till dennes personliga eller ekonomiska situation (se prop. 2016/17:180 s. 332).

Enligt 42 § förvaltningslagen får ett beslut överklagas av den som beslutet angår, om det har gått honom eller henne emot. Rätten att överklaga förutsätter att beslutet antingen påverkar klagandens rättsliga ställning eller rör ett intresse som han eller hon har och som erkänts av rättsordningen. Exempelvis kan det vara fråga om att den beslutande

myndigheten ska ta hänsyn till intresset vid sin materiella prövning av ärendet. I vissa fall har även den som har ett beaktansvärt intresse i saken fått överklaga beslutet. Avgörande för rätten att överklaga är med andra ord den effekt som beslutet får för den som vill överklaga.

Artikel 6 i Europakonventionen ställer krav på att en enskild ska ha rätt till en rättvis domstolsprövning vid prövning av hans eller hennes civila rättigheter och skyldigheter.

Myndigheter utgör inte några självständiga juridiska personer utan agerar som företrädare för staten. De kan därför i princip inte föra talan mot varandra. Statliga myndigheter anses inte utan författningsstöd kunna överklaga beslut av en annan myndighet, om inte myndigheten i fråga företräder ett rent privaträttsligt intresse.

Överklagandemöjligheter enligt den nya lagen

Beslut enligt den nya lagen bör kunna överklagas till den förvaltningsrätt inom vars domkrets ärendet först prövats. Denna ordning överensstämmer med huvudregeln i 14 § andra stycket lagen (1971:289) om allmänna förvaltningsdomstolar. Rätten till överklagande bör gälla för både offentliga och enskilda verksamhetsutövare. Den beslutande myndigheten bör i båda fallen vara motpart till klaganden och detta bör anges i den nya lagen eftersom 7 a § förvaltningsprocesslagen endast reglerar vem som är motpart vid överklagande av enskilda. Förvaltningsrättens avgörande bör kunna överklagas till behörig kammarrätt. Prövningstillstånd bör krävas vid sådant överklagande.

Advokatfirman Kahn Pedersen bedömer att ett beslut om att identifiera en verksamhetsutövare som kritisk bör kunna inhiberas. *Länsstyrelsen i Västra Götalands län* och *Sveriges advokatsamfund* bedömer att överklaganden av nämnda slags beslut bör handläggas med förtur. Det är, som utredningen anger, domstolen i fråga som prövar ett yrkande om inhibition och om det finns skäl att handlägga ett ärende med förtur (se lagen [2009:1058] om förtursförklaring i domstol).

13 Sekretess och personuppgiftsbehandling

13.1 Ändrad reglering i offentlighets- och sekretesslagen

Regeringens förslag

Det ska genomföras en ändring i offentlighets- och sekretesslagen (OSL) som innebär att sekretess ska gälla för uppgift i en incidentrapport som lämnas enligt den nya lagen samt för uppgift om vilka åtgärder som en verksamhetsutövare har vidtagit till följd av incidenten, om det inte står klart att uppgiften kan röjas utan att den rapporterande verksamhetsutövarens framtida verksamhet skadas eller syftet med vidtagen åtgärd motverkas. Sekretessen ska gälla i högst fyrtio år.

Det ska också föras in en ny sekretessbrytande bestämmelse i OSL som innebär att det internationella samarbetet inte ska hindra att Myndigheten för civilt försvar (MCF) i egenskap av gemensam kontaktpunkt enligt artikel 9 i CER-direktivet lämnar en uppgift till en tillsynsmyndighet enligt den nya lagen, om uppgiften behövs för att tillsynsmyndigheten ska kunna fullgöra sitt uppdrag. Sekretessen ska inte heller hindra att en tillsynsmyndighet lämnar en uppgift till MCF, om uppgiften behövs för att MCF ska kunna fullgöra sitt uppdrag som gemensam kontaktpunkt. En uppgift ska få lämnas endast om intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.

Det ska föras in en bestämmelse i den nya lagen som upplyser om att den myndighet som regeringen bestämmer ska vara gemensam kontaktpunkt enligt CER-direktivet.

Regeringens bedömning

Rätten att meddela och offentliggöra uppgifter bör inte ha företräde framför den tystnadsplikt som följer av sekretessen för uppgift i en incidentrapport som lämnas enligt den nya lagen och för uppgift om vilka åtgärder som en verksamhetsutövare har vidtagit till följd av incidenten.

Utredningens förslag och bedömning

Förslaget från utredningen stämmer delvis överens med regeringens. I utredningens förslag anges att den nya sekretessbestämmelsen ska gälla utöver sekretessen i 18 kap. 8 § OSL. Utredningen föreslår att sekretessen ska gälla om det inte står klart att uppgiften kan röjas utan att den rapporterande verksamhetsutövarens verksamhet skadas eller de åtgärder som vidtagits motverkas. Utredningen föreslår att sekretessen i det internationella samarbetet inte ska hindra att Myndigheten för samhällsskydd och beredskap, numera Myndigheten för civilt försvar (MCF), lämnar en uppgift som avses där till tillsynsmyndigheten enligt den nya lagen, om uppgiften behövs för att tillsynsmyndigheten ska kunna fullgöra sitt uppdrag. Utredningen föreslår att detsamma ska gälla när en tillsynsmyndighet lämnar sådana uppgifter till MCF. Utredningen föreslår att sekretess ska gälla för uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men och uppgiften förekommer i angelägenhet som rör bakgrundskontroll enligt den nya lagen om motståndskraft hos kritiska verksamhetsutövare. Utredningen föreslår en tystnadsplikt för uppgifter som förekommer i angelägenhet som rör bakgrundskontroller hos enskilda. Utredningen föreslår ingen upplysningsbestämmelse i den nya lagen. Utredningen gör samma bedömning som regeringen i fråga om rätten att meddela och offentliggöra uppgifter.

Remissinstanserna

Flera remissinstanser, bland andra *Försvarets radioanstalt (FRA)*, *Livsmedelsverket*, *Länsstyrelsen i Stockholms län*, *Post- och telestyrelsen, Stiftelsen för internetinfrastruktur* och *Tranportstyrelsen* tillstyrker förslaget om att en ny sekretessbestämmelse bör införas för att skydda uppgifter i incidentrapporterna.

Affärsverket svenska kraftnät föreslår att den nya sekretessbestämmelsen ska utvidgas till att också omfatta anmälningar om säkerhetshotande händelser enligt säkerhetsskyddsförordningen (2021:955). *Integritetsskyddsmyndigheten (IMY)* anser att förslaget bör utvidgas till att även omfatta personuppgiftsincidentanmälningar eftersom samma uppgifter om en incident annars kommer att få olika starkt skydd beroende av om de lämnas till IMY i form av en personuppgiftsincidentanmälan eller till en tillsynsmyndighet enligt den nya lagen. *Svensk Dagligvaruhandel* och *Svensk Handel* anser att de föreslagna ändringarna även bör omfatta tillsynsmyndigheternas rapporter. *Tech Sverige* anser att ett verktyg med tillhörande processer och rutiner ska införas för att kunna säkerställa att uppgifter som tillsynsmyndigheterna inhämtar från de kritiska verksamhetsutövarna för att upprätta en nationell riskbedömning hanteras på ett liknande sätt som sekretessen för incidentrapporteringen.

Domstolsverket ifrågasätter bedömningen att befintliga sekretessbestämmelser ger ett tillräckligt skydd för förteckningar över verksamhetsutövare och förordar att frågan utreds vidare. *Länsstyrelsen i Kalmar län* betonar vikten av att förteckningarna över verksamhetsutövare är sekretessbelagda enligt 18 kap. 8 § OSL. *Länsstyrelsen i Västra Götalands län* anser att det finns risk för att praxis kan komma att förändras vad avser tillämpningen av 18 kap. 8 och 13 §§ OSL och menar därför att det finns ett behov av att säkerställa att uppgifter i riskbedömningar och förteckningar över verksamhetsutövare fortsatt ska omfattas av sekretess genom att förtydligande görs i lag.

Svenska Journalistförbundet (Journalistförbundet) och *Svenska Tidningsutgivareföreningen (TU)* avstyrker förslaget om sekretess för uppgifter i incidentrapporter. Enligt Journalistförbundet och TU riskerar förslaget att få en effekt motsvarande absolut sekretess. Om regeringen går vidare med förslaget anser Journalistförbundet och TU att bestämmelsen bör ha ett rakt skaderekvisit för att möjliggöra såväl insyn som skydd för uppgifter. Vad avser förslaget kopplat till meddelarfriheten anser Journalistförbundet och TU att skälen för att inskränka denna inte är tillräckliga. Journalistförbundet noterar även att meddelarfriheten inte är inskränkt avseende incidentrapporter enligt 18 kap. 8 a § OSL.

Livsmedelsverket ställer sig tveksamt till om utredningens förslag om sekretesskydd är tillräckligt i fråga om uppgifter som kan framkomma vid tillsyn och utredning eftersom 30 kap. 23 § OSL endast avser uppgifter som rör affärs- och driftförhållanden och där det kan antas att den enskilde lider skada om uppgiften röjs. Myndigheten bedömer att det behövs en bestämmelse, likt den som föreslås för uppgifter i incidentrapporter och för uppgift om åtgärder, även för uppgifter om tillsyn och utredning.

Transportstyrelsen anser att det är angeläget att beslut vid tillsyn ska kunna beläggas med sekretess eftersom det i besluten bland annat hänvisas till brister som kan vara av sådan art att de bör kunna omfattas av

sekretessen enligt 30 kap. 23 § OSL. Transportstyrelsen anser vidare att tillsynsmyndigheterna behöver kunna dela information mellan sig, både om vilka tillsynsobjekt som faller inom respektive myndighets tillsynsområde och om utfallet vid en tillsyn. Enligt Transportstyrelsen är det tveksamt om generalklausulen i 10 kap. 27 § OSL täcker det behov av informationsdelning som finns och myndigheten menar att det bör övervägas om möjligheterna till utbyte av sekretessbelagda uppgifter mellan tillsynsmyndigheterna kan utökas. Transportstyrelsen anser även att möjligheterna att kunna sekretessbelägga identiteten på tillsynsobjekten i de beslut som fattas bör utredas vidare.

Finansinspektionen instämmer inte i utredningens uppfattning att uppgifter som är sekretessbelagda enligt 15 kap. 1 a § OSL, och som lämnas från en svensk myndighet till en annan, kommer att ha samma sekretessskydd hos den mottagande myndigheten som hos myndigheten som har lämnat uppgifterna vidare. Enligt Finansinspektionen bör det i det fortsatta lagstiftningsarbetet analyseras om sådana uppgifter som kommer att behöva utbytas mellan svenska myndigheter redan ges ett tillräckligt sekretesskydd med stöd av andra bestämmelser i OSL eller om sekretesskyddet behöver regleras särskilt. Även *Skatteverket* ifrågasätter slutsatsen att sekretessen följer med en uppgift som lämnas vidare och anser att räckvidden av 15 kap. 1 a § OSL bör förtydligas.

Göteborgs kommun efterfrågar ett förtydligande i fråga om hur informationsdelning inom en kommun ska kunna ske, då en kommun ur ett sekretessperspektiv består av flera olika självständiga myndigheter.

Ett antal remissinstanser, däribland *Länsstyrelsen i Skåne län* och *Pensionsmyndigheten*, tillstyrker förslaget om sekretess för uppgift som förekommer inom ramen för en bakgrundskontroll. Journalistförbundet och TU, avstyrker dock förslaget, och anser att utredningen mer ingående borde ha beskrivit det regelverk som finns avseende bakgrundskontroller och sekretessbestämmelser kopplade till sådana. TU anser att det är tveksamt om utredningens motivering, som går ut på att motsvarande reglering finns gällande säkerhetsprövning enligt säkerhetsskyddslagen, håller.

Skälen för regeringens förslag och bedömning

Krav på konfidentialitet i direktivet

Utan att det påverkar tillämpningen av artikel 346 i EUF-fördraget ska, enligt artikel 1.4 i CER-direktivet, information som är konfidentiell enligt unionsregler eller nationella regler, såsom regler om affärshemligheter, utbytas med kommissionen och andra relevanta myndigheter i enlighet med direktivet endast när sådant utbyte är nödvändigt för att tillämpa direktivet. Den information som utbyts ska begränsas till vad som är relevant och proportionerligt för ändamålet med utbytet. Vid informationsutbytet ska informationens konfidentialitet och kritiska entiteters säkerhetsintressen och kommersiella intressen bevaras samtidigt som medlemsstaternas säkerhet respekteras.

Ytterligare bestämmelser om konfidentialitet finns i artikel 15.3 i CER-direktivet. Av artikeln följer att gemensamma kontaktpunkter, som skickar eller tar emot information kopplat till incidentrapportering, i enlighet med unionsrätten eller nationell rätt ska behandla den informationen på ett sätt

som respekterar dess konfidentialitet och skyddar den berörda kritiska entitetens säkerhet och kommersiella intressen.

I artikel 18.6 i direktivet anges vidare att EU-kommissionen ska anta en genomförandeakt kopplat till rådgivande uppdrag, med vederbörlig hänsyn tagen till de berörda uppgifternas konfidentialitet och kommersiella känslighet.

Relevanta sekretessbestämmelser

Enligt 2 kap. 2 § tryckfrihetsförordningen får rätten att ta del av allmänna handlingar begränsas endast om det krävs med hänsyn till vissa angivna intressen, till exempel rikets säkerhet eller dess förhållande till annan stat eller mellanfolklig organisation, myndigheters verksamhet för inspektion, kontroll eller annan tillsyn, intresset av att förebygga eller beivra brott eller skyddet för enskildas personliga eller ekonomiska förhållanden. En sådan begränsning ska anges noga i en bestämmelse i en särskild lag eller, om det anses lämpligare i ett visst fall, i en annan lag som den särskilda lagen hänvisar till. Efter bemyndigande i en sådan bestämmelse får regeringen genom förordning meddela närmare föreskrifter om bestämmelsens tillämplighet. Den särskilda lagen är OSL och regeringen har meddelat närmare föreskrifter i offentlighets- och sekretessförordningen (2009:641) (OSF). Av 3 kap. 1 § OSL framgår att det med sekretess i den lagen avses ett förbud att röja en uppgift, vare sig det sker muntligen, genom utlämnande av en allmän handling eller på något annat sätt.

I 15 kap. 1 § OSL regleras den så kallade utrikessekretessen. Enligt paragrafen gäller sekretess för uppgift som rör Sveriges förbindelser med en annan stat eller i övrigt rör bland annat en annan stat, mellanfolklig organisation eller myndighet, om det kan antas att det stör Sveriges mellanfolkliga förbindelser eller på annat sätt skadar landet om uppgiften röjs. Skadebegreppet, det vill säga att ett röjande skulle störa Sveriges mellanfolkliga förbindelser eller på annat sätt skada landet, ska inte ges en vid innebörd.

I 15 kap. 1 a § OSL finns bestämmelser om sekretess i det internationella samarbetet. Av första stycket framgår att sekretess gäller för uppgift som en myndighet har fått från ett utländskt organ på grund av en bindande EU-rättsakt eller ett av EU ingånget eller av riksdagen godkänt avtal med en annan stat eller med en mellanfolklig organisation, om det kan antas att Sveriges möjlighet att delta i det internationella samarbete som avses i rättsakten eller avtalet försämras om uppgiften röjs. Motsvarande sekretess gäller enligt andra stycket för uppgift som en myndighet har inhämtat i syfte att överlämna den till ett utländskt organ i enlighet med en sådan rättsakt eller ett sådant avtal som avses i första stycket. Paragrafen är alltså tillämplig på uppgifter som har tagits emot eller hämtats in som en direkt följd av en EU-rättsakt.

Sekretess för säkerhets- eller bevakningsåtgärd regleras i 18 kap. 8 § OSL. Sekretessen gäller enligt paragrafens första punkt för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärden avser byggnader eller andra anläggningar, lokaler eller inventarier. Sekretessen kan gälla bland annat för uppgifter om instruktioner och tjänstgöringslistor som rör bevakningen av en byggnad.

Sekretessen gäller enligt paragrafens tredje punkt bland annat för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärden avser telekommunikation eller system för automatiserad behandling av information.

Med ordet telekommunikation avses i paragrafen överföring av meddelande med tråd, radio eller en liknande metod. Med uttrycket system för automatiserad behandling av information avses system där datorer, telekommunikation eller annan teknisk utrustning samverkar för att insamla, ordna, bearbeta, söka eller distribuera information. Sekretessen avser bland annat att skydda funktioner för användning av lösenord, loggning och kryptering, installation och konfigurering av brandväggar och antivirusprogram samt administrativa rutiner för till exempel utdelning av lösenord eller bevakning av loggar och larm.

Beskrivningar av hur ett program fungerar i stora drag och vilka typer av uppgifter som bearbetas i ett program bör alltid kunna lämnas utan att uppgifter som omfattas av bestämmelsen behöver röjas. Vidare kan till exempel inte kostnader för införskaffande och installation av ett datorsystem hemlighållas med stöd av bestämmelsen, även om uppgifter i en faktura om vilken typ och/eller version av system som har införskaffats kan komma att hemlighållas (se prop. 2003/04:93 s. 88 f.).

Av 18 kap. 13 § OSL framgår att sekretess gäller för uppgift som hänför sig till en myndighets verksamhet som består i risk- och sårbarhetsanalyser avseende fredstida krissituationer, planering och förberedelser inför sådana situationer eller hantering av sådana situationer, om det kan antas att det allmännas möjligheter att förebygga och hantera fredstida kriser motverkas om uppgiften röjs.

I 35 kap. OSL regleras sekretess till skydd för enskild i verksamhet som syftar till att bland annat förebygga eller beivra brott. Sekretess gäller enligt 35 kap. 1 § OSL för uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men och uppgiften förekommer i bland annat angelägenhet som avser säkerhetsprövning enligt säkerhetsskyddslagen. För uppgift i en allmän handling gäller sekretessen i högst sjuttio år. Syftet med regleringen är att ge ett motsvarande skydd för uppgifter som på annat sätt än genom registerkontroll och särskild personutredning kommer fram vid säkerhetsprövningen (se prop. 2017/18:89 s. 159). Det kan enligt förarbetena vara fråga om uppgifter om personliga och ekonomiska förhållanden som den som kontrollen avser lämnar vid en intervju.

Uppgifter i belastningsregistret omfattas av absolut sekretess enligt 35 kap. 3 § OSL. Uppgifter från registret får därför lämnas ut endast i enlighet med vad som anges i den särskilda registerlagstiftningen, se 6–15 §§ lagen om belastningsregister, och i säkerhetsskyddsregleringen. Den absoluta sekretessens räckvidd begränsas till den registerförande myndigheten, det vill säga Polismyndigheten, och de myndigheterna som har direktåtkomst så länge uppgiften är kvar i registret. När en uppgift tas ut av en myndighet för att användas i den egna verksamheten gäller i stället i förekommande fall sekretess enligt de bestämmelser som gäller för denna verksamhet.

I 19 § lagen om belastningsregister anges att den som med stöd av lagen har fått del av uppgifter om någon annans personliga förhållanden inte obehörigen får röja dessa uppgifter samt att i det allmännas verksamhet tillämpas i stället bestämmelserna i OSL.

Övriga relevanta bestämmelser i OSL

Enligt 8 kap. 1 § OSL får uppgifter som omfattas av sekretess inte röjas för enskilda eller för andra myndigheter, om inte annat anges i OSL eller i lag eller förordning som OSL hänvisar till. En sekretessbrytande bestämmelse är enligt 3 kap. 1 § OSL en bestämmelse som innebär att en sekretessbelagd uppgift får lämnas ut under vissa förutsättningar.

I 8 kap. 3 § OSL finns bestämmelser som reglerar när uppgifter som omfattas av sekretess får röjas för utländska myndigheter och mellanfolkliga organisationer. Enligt paragrafen får en uppgift för vilken sekretess gäller enligt OSL inte röjas för en utländsk myndighet eller en mellanfolklig organisation, om inte utlämnande sker i enlighet med särskild föreskrift i lag eller förordning, eller uppgiften i motsvarande fall skulle få lämnas ut till en svensk myndighet och det enligt den utlämnande myndighetens prövning står klart att det är förenligt med svenska intressen att uppgiften lämnas till den utländska myndigheten eller den mellanfolkliga organisationen.

Av den sekretessbrytande bestämmelsen i 10 kap. 2 § OSL framgår att sekretess inte hindrar att en uppgift lämnas till en enskild eller en annan myndighet, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet.

I 10 kap. 15 a § OSL finns en sekretessbrytande bestämmelse som möjliggör för myndigheter att under vissa förutsättningar lämna uppgifter om enskilda till andra myndigheter, utan hinder av sekretess till skydd för enskilds personliga eller ekonomiska förhållanden som regleras i 21–40 kap. OSL. En förutsättning för att bestämmelsen ska bryta sekretessen är, i nu relevant avseende, att det behövs för att förebygga, förhindra, upptäcka eller utreda fusk och överträdelser av regler, villkor i beslut eller avtal. Enligt bestämmelsens andra stycke gäller vidare att en uppgift inte får lämnas ut om övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut.

Enligt 10 kap. 17 § OSL hindrar sekretess inte att en uppgift lämnas till en myndighet, om uppgiften behövs där för tillsyn över eller revision hos den myndighet där uppgiften förekommer. Om en myndighet i verksamhet som avser tillsyn eller revision, får en sekretessreglerad uppgift från en annan myndighet, blir sekretessbestämmelsen tillämplig på uppgiften även hos den mottagande myndigheten enligt 11 kap. 1 § OSL.

Utlämnande av sekretessbelagda uppgifter kan ske med stöd av generalklausulen i 10 kap. 27 § OSL. En sekretessbelagd uppgift får enligt generalklausulen lämnas till en myndighet, om det är uppenbart att intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.

Enligt 10 kap. 28 § OSL hindrar sekretess inte att en uppgift lämnas till en annan myndighet, om uppgiftsskyldighet följer av lag eller förordning. För att bestämmelsen ska vara tillämplig krävs att uppgiftsskyldigheten har viss konkretion. Uppgiftsskyldigheten kan antingen ta sikte på utlämn-

ande av uppgifter av ett speciellt slag, gälla en viss myndighets rätt att få del av uppgifter i allmänhet eller avse skyldighet för en viss myndighet att lämna andra myndigheter information (se prop. 1979/80:2 Del A s. 322).

Om sekretess gäller enligt 15 kap. 1 a § första eller andra stycket OSL, får de sekretessbrytande bestämmelserna i bland annat 10 kap. 17, 27 och 28 §§ första stycket inte tillämpas. Detta följer av 15 kap. 1 a § tredje stycket OSL.

Genomförandet av NIS 2-direktivet i fråga om sekretess

I propositionen som gäller införandet av cybersäkerhetslagen lämnade regeringen flera förslag och gjorde flera överväganden gällande sekretess kopplat till genomförandet av NIS 2-direktivet (se prop. 2025/26:28 s. 194 f. och jfr även prop. 2025/26:214). Det infördes genom förslagen i propositionen bland annat en ny sekretessbestämmelse i OSL, 18 kap. 8 b §, så att sekretess gäller för uppgift i en incidentrapport som lämnas enligt cybersäkerhetslagen samt för uppgift om vilka åtgärder som verksamhetsutövaren har vidtagit till följd av en incident. Sekretess gäller om det inte står klart att uppgiften kan röjas utan att den rapporterande verksamhetsutövarens framtida verksamhet skadas eller syftet med vidtagen åtgärd motverkas. Sekretessen gäller i högst fyrtio år. Rätten att meddela och offentliggöra uppgifter har, genom en ändring av 18 kap. 19 §, inte företräde framför den tystnadsplikt som följer av sekretessen.

Det fördes också in en ny bestämmelse i OSL, 15 kap. 3 c §, om att sekretessen i det internationella samarbetet inte hindrar att MCF, i egenskap av bland annat gemensam kontaktpunkt enligt NIS 2-direktivet, lämnar en uppgift till en tillsynsmyndighet enligt cybersäkerhetslagen, om uppgiften behövs för att tillsynsmyndigheten ska kunna fullgöra sitt uppdrag enligt den lagen. Sekretessen hindrar inte heller att en tillsynsmyndighet lämnar en uppgift till MCF, om uppgiften behövs för att MCF ska kunna fullgöra sitt uppdrag som bland annat gemensam kontaktpunkt enligt NIS 2-direktivet. En uppgift som omfattas av sekretessen i det internationella samarbetet får lämnas endast om intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda. En ändring av paragrafen, som innebär att FRA anges i stället för MCF i paragrafen, trädde i kraft den 1 juli 2026 (se prop. 2025/26:123).

Det infördes också en paragraf i cybersäkerhetslagen, 1 kap. 17 §, som upplyser om att den myndighet som regeringen bestämmer ska vara bland annat gemensam kontaktpunkt enligt NIS 2-direktivet.

Motsvarande sekretessreglering som den som gäller kopplat till NIS 2-direktivet bör införas

I utredningens slutbetänkande föreslås ändringar i OSL kopplat till både genomförandet av CER-direktivet och NIS 2-direktivet och förslagen är, frånsett förslaget kopplat till bakgrundskontroller, identiska. Den remisskritik som redogörs för ovan gällde förslagen i slutbetänkandet i stort. Remisskritiken har därmed, frånsett den som gäller sekretess och tystnadsplikt kopplat till bakgrundskontroller, bemötts i propositionen som avser genomförandet av NIS 2-direktivet. I propositionen gjorde regeringen bland annat bedömningen att det saknas ett ändamålsenligt sekretesskydd för uppgifter med koppling till en incidentrapport som har

sin grund i NIS 2-direktivet, både med beaktande av 18 kap. 8 § 3 OSL och övrig sekretessreglering (se prop. 2025/26:28 s. 194 f.). Samma bedömning görs i förhållande till den incidentrapportering som har sin grund i CER-direktivet.

Regeringen har, även i förhållande till den reglering som gäller CER-direktivet, förståelse för *TU:s* synpunkt att en sekretessbestämmelse kan innebära att motiverad insyn försvåras i de fall det har skett en incident. Som utredningen resonerar kring bygger ett regelverk som innebär krav på incidentrapportering emellertid på att de aktörer som ska genomföra rapportering har en hög tilltro till systemet och att deras känsliga uppgifter ges ett fullgott skydd hos mottagaren. I annat fall kan rapporter utebli och känsliga uppgifter utelämnas. En sådan utveckling riskerar att motverka syftet med rapporteringen, vilket i slutändan kan leda till att samhället blir mer sårbart. De incidentrapporter som föreslås lämnas kan därtill innefatta uppgifter som vid en första anblick kan framstå som harmlösa, men där det samtidigt kan få stora konsekvenser om uppgifterna röjs. Det kan till exempel röra sig om uppgifter som lämnas i ett tidigt skede där omfattningen av angreppet ännu inte är klarlagt eller uppgifter som ger en antagonistisk aktör en bild av de sårbarheter som finns.

Mot bakgrund av den betydelse som behovet av tilltro till systemet och möjligheten att ge skydd åt känsliga uppgifter har för rapporteringen och med hänsyn till de negativa effekter som ett röjande av uppgifterna kan få anser regeringen att det finns behov av ett erforderligt skydd även för den rapportering som ska ske enligt den lag som genomför CER-direktivet. Intresset av att myndigheterna ska kunna motverka till exempel attacker på kritisk infrastruktur och i förlängningen också bidra till att förebygga och beivra brott samt intresset av att svenska myndigheter kan delta på ett effektivt sätt i det internationella samarbetet enligt CER-direktivet, får enligt regeringen anses väga tyngre än det motstående intresset av insyn i myndigheternas verksamhet.

De överväganden som görs i förarbetena till cybersäkerhetslagen, i fråga om sekretessens föremål, räckvidd och styrka, gör sig gällande även i detta lagstiftningsärende. En ny sekretessbestämmelse som motsvarar den som har införts kopplat till cybersäkerhetslagen bör därför, till skillnad från vad exempelvis *Journalistförbundet* och TU anser, men i likhet med vad utredningen och ett antal remissinstanser föreslår, också ge skydd för uppgifter i en incidentrapport som lämnas enligt den nya lagen och uppgifter om åtgärder som har vidtagits till följd av aktuella incidenter (jfr 18 kap. 8 b § OSL). Sekretessen bör gälla för uppgifter som har lämnats vid de olika delarna av en incidentrapportering, det vill säga både i en anmälan och en rapport (se avsnitt 8.3). Till skillnad från Journalistförbundet och TU anser regeringen också, av samma skäl som anges i förarbetena till cybersäkerhetslagen, att rätten att meddela och offentliggöra uppgifter inte bör ha företräde framför den tystnadsplikt som följer av bestämmelsen (se prop. 2025/26:28 s. 205).

MCF liksom tillsynsmyndigheterna enligt den nya lagen behöver ömsesidigt kunna utbyta sådana uppgifter som härrör från andra EU-medlemsstater och EU:s institutioner oberoende av vilken myndighet som har fått uppgiften. Regeringen konstaterar att den myndighet som är gemensam kontaktpunkt enligt CER-direktivet kan få del av uppgifter med stöd av direktivet som den bör kunna vidarebefordra till tillsynsmyndig-

heterna enligt lagen. Tillsynsmyndigheterna kan också få del av uppgifter med stöd av direktivet som bör kunna vidarebefordras till den myndighet som är gemensam kontaktpunkt. Det rör sig till exempel om uppgifter i incidentrapporter och uppgifter som lämnas inom ramen för rådgivande uppdrag enligt CER-direktivet.

Av artikel 9.2 i direktivet framgår att den gemensamma kontaktpunkten ska ha en sambandsfunktion för att säkerställa gränsöverskridande samarbete. Av skäl 23 framgår vidare att den gemensamma kontaktpunkten vid behov även bör samarbeta och samordna kommunikationen med sin medlemsstats behöriga myndigheter, andra medlemsstaters gemensamma kontaktpunkter och gruppen för kritiska entiteters motståndskraft (CERG). Enligt artikel 9.3 ska den gemensamma kontaktpunkten lämna en sammanfattande rapport till kommissionen och CERG om de anmälningar som de har mottagit, inklusive antalet anmälningar, de anmälda incidenternas art och vilka åtgärder som vidtagits i enlighet med artikel 15.3. Enligt artikel 15.3 ska den behöriga myndigheten på grundval av den information som en kritisk entitet lämnar i en incidentanmälan enligt artikel 15.1, via den gemensamma kontaktpunkten, informera gemensamma kontaktpunkter i andra medlemsstater som påverkas av incidenten på visst angivet sätt. Enligt artikel 11 ska medlemsstaterna när så är lämpligt samråda med varandra om kritiska entiteter i syfte att säkerställa att direktivet tillämpas på ett konsekvent sätt. Av skäl 26 framgår att samråden bör inledas på begäran av en berörd behörig myndighet.

Sekretessen i det internationella samarbetet bör inte heller hindra utbyte av information kopplat till CER-direktivet. En ny sekretessbrytande bestämmelse, motsvarande den bestämmelse som infördes i samband med genomförandet av NIS 2-direktivet, bör införas för att åstadkomma denna ordning (jfr 15 kap. 3 c § OSL). I lagrådsremissen angav regeringen vidare att det bör införas en bestämmelse i den nya lagen som upplyser om att den myndighet som regeringen bestämmer ska vara gemensam kontaktpunkt enligt direktivet (jfr 1 kap. 17 § cybersäkerhetslagen).

Lagrådet anser att det blir egendomligt att riksdagen i lag indirekt anger att det är Myndigheten för civilt försvar som ska utses som gemensam kontaktpunkt enligt den nya lagen när det i den nya lagen inte sägs något annat än att det är den myndighet som regeringen bestämmer som ska vara kontaktpunkt. Paragrafen i OSL bör enligt Lagrådet skrivas om utan att myndigheten anges. Regeringen konstaterar dock att förslaget i lagrådsremissen motsvarar den reglering som har införts kopplat till cybersäkerhetslagen och bedömer inte att det finns anledning att genomföra någon ändring med anledning av Lagrådets förslag.

Utredningens slutsats om att den internationella sekretessen även gäller hos den myndighet som får del av uppgifterna efter vidarebefordran ifrågasätts av *Finansinspektionen* och *Skatteverket*. I förarbetena till 15 kap. 1 a § OSL anges att den aktuella bestämmelsen om sekretess i det internationella samarbetet enbart gäller hos den myndighet som fått uppgiften från ett utländskt organ eller har inhämtat den (se prop. 2012/13:192 s. 30 och prop. 2025/26:28 s. 207). Det behöver följaktligen inte införas en sådan bestämmelse som utredningen föreslår för att möjliggöra sekretessgenombrott för en myndighet som efter vidarebefordran har fått del av uppgifter som omfattas av sekretess i det internationella samarbetet.

Det finns inte heller i detta lagstiftningsärende något utrymme för att föreslå sådana ändringar kopplade till säkerhetsskyddsförordningen och personuppgiftsincidentanmälningar som *Affärsverket svenska kraftnät* och *IMY* föreslår. Detta gäller även i förhållande till de förslag på ändrat regelverk som *Svensk Dagligvaruhandel* och *Svensk Handel* lämnar. *Tech Sverige* anser att ett verktyg med tillhörande processer och rutiner ska införas för att kunna säkerställa att uppgifter som tillsynsmyndigheterna inhämtar från de kritiska verksamhetsutövarna för att upprätta en nationell riskbedömning hanteras på ett liknande sätt som sekretessen för incidentrapporteringen. I avsnitt 10.2 gör regeringen dock bedömningen att utredningens förslag om att den som står under tillsyn ska vara skyldig att på begäran tillhandahålla tillsynsmyndigheten information som behövs för den nationella riskbedömningen inte ska genomföras. Med anledning av vad *Länsstyrelsen i Västra Götalands län* anför vill regeringen framhålla att det inte har framkommit något behov av att göra ändringar i 18 kap. 8 och 13 §§ OSL. Regeringen ser inte att förslaget i denna proposition skulle riskera att påverka hur dessa paragrafer tillämpas.

Informationsutbytet mellan verksamhetsutövare och tillsynsmyndigheter i övrigt

I avsnitt 8.3 föreslås en uppgiftsskyldighet inom ramen för skyldigheterna att genomföra incidentrapportering. I avsnitt 10.2 föreslås vidare en uppgiftsskyldighet för kritiska verksamhetsutövare i förhållande till tillsynsmyndigheten. Införandet av dessa uppgiftsskyldigheter innebär att en uppgift, trots att den omfattas av sekretess hos en offentlig verksamhetsutövare, kan lämnas till en annan myndighet enligt 10 kap. 28 § första stycket OSL. En verksamhetsutövare som omfattas av tillämpningsområdet för OSL har vidare en möjlighet att lämna ut uppgifter med stöd av 10 kap. 17 § samma lag, om uppgiftslämnandet sker inom ramen för tillsyn eller revision. Därtill hindrar sekretess inte att en uppgift lämnas till en enskild eller till en annan myndighet, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet enligt 10 kap. 2 § OSL. Om nämnda bestämmelser inte kan användas, kan frågan om utlämnande av sekretessbelagda uppgifter även prövas utifrån generalklausulen i 10 kap. 27 § OSL. Mot denna bakgrund bedömer regeringen att det inte krävs någon ytterligare sekretessbrytande bestämmelse för att möjliggöra informationsutbyte mellan offentliga verksamhetsutövare och andra myndigheter.

Det bör noteras att om en myndighet i verksamhet som avser tillsyn eller revision, får en sekretessreglerad uppgift från en annan myndighet, blir sekretessbestämmelsen tillämplig på uppgiften även hos den mottagande myndigheten enligt 11 kap. 1 § OSL. Som utredningen anför kan också bestämmelsen om utrikessekretess i 15 kap. 1 § OSL aktualiseras för uppgifter som har tagits emot från EU-kommissionen och andra medlemsstater. Vilket sekretesskydd som uppgifterna får hos den mottagande myndigheten får dock avgöras i varje enskilt fall utifrån den sekretess som gäller hos berörd myndighet.

Huruvida det finns förutsättningar för informationsdelning mellan olika kommunala nämnder med anledning av det regelverk som föreslås i denna proposition, något som *Göteborgs kommun* efterfrågar ett förtydligande

av, får avgöras i varje enskilt fall med beaktande av tillämplig sekretessreglering.

Tillsynsmyndigheternas informationsutbyte i övrigt

Transportstyrelsen anser att det bör övervägas om möjligheterna till utbyte av sekretessbelagda uppgifter mellan tillsynsmyndigheterna kan utökas. Det är inte uteslutet att en tillsynsmyndighet även kan behöva dela med sig av andra uppgifter än sådana uppgifter som omfattas av sekretess i det internationella samarbetet till en annan tillsynsmyndighet.

Sekretess hindrar inte att en uppgift lämnas till en annan myndighet, om det är nödvändigt för att den utlämnande myndigheten ska kunna fullgöra sin verksamhet. Detta framgår av 10 kap. 2 § OSL. Bestämmelsen ska användas med restriktivitet. Regeringen anser dock att en tillsynsmyndighet i vissa fall bör kunna tillämpa paragrafen för utlämnande av uppgifter till en annan tillsynsmyndighet (se prop. 2025/26:28 s. 207). Utlämnande av sekretessbelagda uppgifter kan även ske med stöd av 10 kap. 15 a § första stycket 5 OSL, om det behövs för att förebygga, förhindra, upptäcka eller utreda fusk eller överträdelser av regler, villkor i beslut eller avtal. En uppgift får inte lämnas ut med stöd av bestämmelsen om övervägande skäl talar för att det intresse som sekretessen ska skydda har företräde framför intresset av att uppgiften lämnas ut. Informationsutbyte får ske utifrån tillämpliga bestämmelser och huruvida förutsättningar finns för sådant utbyte med stöd av 10 kap. 2 § OSL, 10 kap. 15 a § OSL, generalklausulen i 10 kap. 27 § OSL eller någon annan bestämmelse, får avgöras i varje enskilt fall.

CER-direktivet kräver, som utredningen nämner, att det finns möjlighet att lämna ut uppgifter som omfattas av sekretess till utländska myndigheter och EU-kommissionen. Som utredningen konstaterar, och lämnar förslag om, kan möjligheten till ett sådant utlämnande regleras i förordning enligt 8 kap. 3 § OSL. Förordningsförslagen är inte föremål för behandling i denna proposition.

Sekretess i övrigt kopplat till tillsyn, förteckningar och riskbedömningar

Utredningen föreslår att det ska regleras i OSF att sekretess även gäller för diarium, ett förslag som enligt *Journalistförbundet* och *TU* är för långtgående. Ett antal remissinstanser betonar vikten av att skydda enskildas affärs- och driftförhållanden i utredning och tillsyn enligt den nya lagen. *Livsmedelsverket* ställer sig till exempel tveksamt till om det finns ett tillräckligt sekretesskydd för uppgifter som kan framkomma vid tillsyn och anser att det behövs en bestämmelse, likt den som föreslås för uppgifter i incidentrapporter och för uppgift om vidtagna åtgärder, även för uppgifter om tillsyn och utredning. Utredningen lämnar ett förslag till ändring av bilagan till OSF i detta syfte, men med begränsningen att sekretessen inte ska gälla för beslut. *Transportstyrelsen* anser att det är angeläget att beslut vid tillsyn ska kunna beläggas med sekretess eftersom det i besluten bland annat hänvisas till brister som kan vara av sådan art att de bör kunna omfattas av sekretess enligt 30 kap. 23 § OSL. Enligt Transportstyrelsen bör även möjligheterna att sekretessbelägga identiteten på tillsynsobjekten i de beslut som fattas utredas vidare.

Enligt 30 kap. 23 § OSL och 9 § OSF gäller sekretess, i den utsträckning som anges i bilagan till förordningen, i en statlig myndighets verksamhet som består i utredning, planering, prisreglering, tillståndsgivning, tillsyn eller stödverksamhet med avseende på produktion, handel, transportverksamhet eller näringslivet i övrigt för bland annat uppgift om en enskilds affärs- eller driftförhållanden, uppfinningar eller forskningsresultat, om det kan antas att den enskilde lider skada om uppgiften röjs. I bilagan till OSF anges dels vad aktuell verksamhet består i, dels vilka särskilda begränsningar i sekretessen som gäller. Varken förslaget om förordningsändringar avseende sekretess hos tillsynsmyndigheterna eller förslaget om sekretess för diarium är dock föremål för denna proposition.

Regeringen bedömer, som utredningen men till skillnad från *Domstolsverket* och *Länsstyrelsen i Kalmar län*, att 18 kap. 8 och 13 §§ OSL utgör tillräckligt skydd för förteckningar avseende verksamhetsutövare och uppgifter i riskbedömningar som ska göras enligt den nya lagen.

Ingen sekretess eller tystnadsplikt för uppgifter kopplade till bakgrundskontroller

Regeringen föreslår i avsnitt 9 att en kritisk verksamhetsutövare ska vara skyldig att genomföra bakgrundskontroller avseende personal, uppdragstagare och andra som deltar i verksamheten. En bakgrundskontroll kan, enligt utredningen, innebära att för den enskilde synnerligen känsliga uppgifter delas med arbetsgivaren eller den som annars ska göra bakgrundskontrollen. I 35 kap. 1 § OSL finns, som redovisas ovan, bland annat en bestämmelse som tar sikte på att skydda uppgifter som förekommer i angelägenhet som avser en säkerhetsprövning enligt säkerhetsskyddslagen. Utredningens bedömning är att uppgifter om bakgrundskontroller bör omfattas av sekretess med stöd av samma paragraf och att detta kan åstadkommas genom att införa en ny bestämmelse i paragrafen. En sådan ordning medför enligt utredningen en tydlighet i fråga om skyddet för uppgifter som framkommer vid bakgrundskontroller. Eftersom bestämmelser om sekretess i OSL endast gäller i det allmännas verksamhet anser utredningen att det även behövs en kompletterande bestämmelse om tystnadsplikt för uppgifter som förekommer i angelägenhet som avser bakgrundskontroller. Utredningen föreslår att en bestämmelse med sådant innehåll införs i den nya lagen om motståndskraft hos kritiska verksamhetsutövare.

Journalistförbundet och *TU* anser att utredningen mer ingående borde ha beskrivit det regelverk som finns avseende bakgrundskontroller och sekretessbestämmelser kopplade till sådana. TU anser att det är tveksamt om utredningens motivering, som går ut på att motsvarande reglering finns gällande säkerhetsprövning, håller. Skillnaderna mellan regeringens och utredningens förslag i fråga om bakgrundskontroller behandlas i avsnitt 9.

Som anges i avsnitt 9.1 används inte uttrycket bakgrundskontroller på ett entydigt sätt i svensk rätt. Frågor om sekretess i samband med vissa slags registerkontroller har dock analyserats i olika sammanhang (se till exempel Ds 2024:24 och SOU 2019:19). I förarbeten har tidigare uttalats att offentlighet i princip bör råda i tjänstetillsättningsärenden inom offentlig verksamhet (se prop. 1979/80:2 Del A s. 201 och prop. 1986/87:3 s. 8). Uppgifter i ett belastningsregisterutdrag som förekommer i ett

anställningsärende saknar normalt sekretesskydd (jfr 35 kap. 1 § 3 OSL). Som redovisas ovan omfattas uppgifter i belastningsregistret enligt 35 kap. 3 § OSL av absolut sekretess. Uppgifter från registret får endast lämnas ut i enlighet med vad som sägs i lagen om belastningsregister och säkerhetsskyddslagen samt tillhörande förordningar. Sekretessen för uppgifter i belastningsregistret gäller så länge uppgifterna finns i registret. Om uppgifter lämnas ut ur registret är sekretessbestämmelser som gäller för registret inte längre tillämpliga på uppgifterna (se prop. 2025/26:61 s. 20). För att sekretess då ska råda krävs att det finns en sekretessbestämmelse som är tillämplig för uppgifterna hos mottagaren.

När en ny sekretessbestämmelse övervägs ska det alltid göras en avvägning mellan sekretessintresset och insynsintresset (se prop. 1979/80:2 Del A s. 75 f.). Genom det förslag som läggs fram i denna proposition kommer enskilda ha möjlighet att få ut ett begränsat utdrag ur belastningsregistret för uppvisande enligt förslaget i avsnitt 9. Förslaget medför således en potentiellt ökad spridning av uppgifter ur registret till en mycket stor krets givet CER-direktivets och den nya lagens tillämpningsområde. Det finns således anledning att överväga om det bör införas något skydd för dessa uppgifter.

Vid bedömningen bör utgångspunkt tas i principen som har gällt sedan länge om att offentlighet i princip ska råda i tjänstetillsättningsärenden inom offentlig verksamhet. Argument för att göra avsteg från den principen skulle kunna vara att uppgifter om brott utgör integritetskänsliga uppgifter och att en sekretessreglering skulle kunna vara ett sätt att skydda dessa uppgifter i den enskildes intresse. Utan ett sekretesskydd respektive tystnadsplikt skulle det kunna tänkas att personer som visserligen är dömda för brott, men ändå skulle kunna vara lämpliga för anställning, avhåller sig från att söka vissa tjänster. Det skulle i sin tur kunna påverka antalet sökande och eventuellt i förlängningen personalförsörjningen inom verksamhet som tillhandahåller samhällsviktiga tjänster.

Som motargument kan dock framhållas att denna möjliga konsekvens motverkas av att registerutdragen är begränsade. Spridningen av uppgifterna påverkas också av att det föreslås att utdrag endast ska visas upp och att verksamhetsutövaren inte får dokumentera eventuella uppgifter i registerutdraget. Det bör även beaktas att någon liknande reglering inte finns avseende registerutdrag som visas upp eller ges in med stöd av skollagen, lagen (2007:171) om registerkontroll av personal vid vissa boenden som tar emot barn, lagen (2010:479) om registerkontroll av personal som utför vissa insatser åt barn med funktionshinder eller lagen om registerkontroll av personer som ska arbeta med barn. Regeringen har vidare gjort bedömningen att det inte krävs några ändrade sekretessregler eller bestämmelser om tystnadsplikt för uppgifter i belastningsregisterutdrag som inhämtas i samband med vissa anställningar inom kommunerna (se prop. 2025/26:61).

Det kan vidare konstateras att den prövning som ska ske enligt säkerhetsskyddslagen och den bakgrundskontroll som ska ske enligt den nya lagen har delvis olika syften och omfattning. Regeringen anser mot denna bakgrund att intresset av att skydda aktuella uppgifter inte kan anses väga tyngre än intresset av insyn. Det bör därmed inte införas någon sådan sekretessbestämmelse eller bestämmelse om tystnadsplikt för enskilda som utredningen föreslår.

13.2 Ingen ytterligare reglering om personuppgiftsbehandling behövs

Regeringens bedömning

Någon ytterligare reglering behöver inte införas för den personuppgiftsbehandling som kan komma att ske med anledning av den nya lagen.

Utredningens bedömning

Utredningen gör ingen bedömning gällande behovet av kompletterande reglering avseende personuppgiftsbehandling annat än i fråga om bakgrundskontroller.

Remissinstanserna

Remissinstanserna yttrar sig inte särskilt i frågan. *Integritetsskyddsmyndigheten* har inga synpunkter på förslagen i betänkandet utöver den som redovisas i avsnitt 13.1.

Skälen för regeringens bedömning

Behandling av personuppgifter enligt CER-direktivet

Det anges i artikel 1.9 i CER-direktivet att direktivet i synnerhet inte påverkar tillämpningen av EU:s dataskyddsförordning, det vill säga Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

Ansökningar om bakgrundskontroller ska, enligt artikel 14.2, bedömas inom en rimlig tidsram och hanteras i enlighet med nationell rätt och nationella förfaranden samt relevant och tillämplig unionsrätt, inbegripet EU:s dataskyddsförordning och dataskyddsdirektivet, det vill säga Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

Enligt artikel 10 i EU:s dataskyddsförordning får behandling av personuppgifter som rör bland annat fällande domar i brottmål och lagöverträdelser som innefattar brott endast utföras under kontroll av myndighet eller då behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs.

Dataskyddsdirektivet har genomförts i svensk rätt i huvudsak genom brottsdatalagen (2018:1177) och brottsdataförordningen (2018:1202). Lagen gäller när myndigheter, främst i rättskedjan, behandlar personuppgifter för vissa syften, däribland i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet.

I avsnitt 9.3 föreslås att den som ska genomgå bakgrundskontroll ska begära ut uppgifter om sig själv ur belastningsregistret och visa upp ett utdrag för verksamhetsutövaren. Med en sådan lösning som föreslås krävs ingen särskild reglering med anledning av vad som i CER-direktivet anges med hänvisning till dataskyddsdirektivet.

I avsnitt 9.4 föreslås att en bakgrundskontroll ska dokumenteras. Att den som gör kontrollen tar del av innehållet i registerutdraget och antecknar att ett registerutdrag har visats upp innebär, som utredningen anger, inte en behandling av uppgifter om lagöverträdelser enligt artikel 10 i EU:s dataskyddsförordning. Någon särskild reglering gällande behandling av personuppgifter som rör lagöverträdelser är därför inte nödvändig.

Den rättsliga grunden för den personuppgiftsbehandling som sker hos verksamhetsutövarna i samband med bakgrundskontrollen och i övrigt med anledning av den nya lagen är att behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som följer av lag i enlighet med artikel 6.1 c i EU:s dataskyddsförordning och 2 kap. 1 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen). Syftet med personuppgiftsbehandlingen framgår av lagen. Behandlingen är nödvändig för att uppfylla ett mål av allmänt intresse i enlighet med artikel 6.3 i EU:s dataskyddsförordning. Vidare är behandlingen proportionerlig för att uppnå syftet med densamma.

Den myndighet som tar emot anmälningar och incidentrapporter enligt förslaget i avsnitt 8.3 kan få del av uppgifter om bland annat affärs- och driftförhållanden, och sådana uppgifter kan utgöra personuppgifter. Regeringen konstaterar också att myndigheten i viss utsträckning, i enlighet med utredningens förslag till förordning, kan komma att vidarebefordra personuppgifter till andra myndigheter. Vid handläggningen av ett ärende enligt den nya lagen kommer därmed personuppgifter av olika slag att behandlas av olika myndigheter med ansvar enligt regelverket. Behandlingen kommer att utföras som en följd av de arbetsuppgifter som myndigheten som tar emot anmälningarna och rapporterna samt tillsynsmyndigheterna får genom det samlade regelverket. Den rättsliga grunden för den personuppgiftsbehandling som aktualiseras hos berörda myndigheter med särskilt ansvar enligt den nya lagen är att behandlingen är nödvändig för att utföra en uppgift av allmänt intresse som följer av föreslagen lag eller annan författning eller som ett led i myndighetsutövning enligt lagen eller annan författning på det sätt som anges i artikel 6.1 e i EU:s dataskyddsförordning. Eventuell behandling av personnummer och samordningsnummer hos de berörda myndigheterna är klart motiverad med hänsyn till ändamålet med behandlingen och vikten av en säker identifiering i enlighet med 3 kap. 10 § dataskyddslagen. Bestämmelsen har sin grund i artikel 87 i EU:s dataskyddsförordning som anger att medlemsstaterna närmare får bestämma vilka särskilda villkor ett nationellt identifikationsnummer eller något annat vedertaget sätt för identifiering får behandlas.

Sammanfattningsvis bedömer regeringen att EU:s dataskyddsförordning och dataskyddslagen ger stöd för den personuppgiftsbehandling som regelverket innebär. Vid en avvägning mellan den personliga integriteten och behovet av att personuppgifterna behandlas får behandlingen anses

vara proportionerlig. Det behöver inte införas någon ytterligare reglering för att behandlingen ska vara tillåten.

14 Ändringar i säkerhetsskyddslagen

Regeringens förslag

Sanktionsavgiften för en verksamhetsutövare som inte är en statlig myndighet, en kommun eller en region ska bestämmas till lägst 25 000 kronor och högst till det högsta av 2 procent av verksamhetsutövarens totala globala årsomsättning under närmast föregående räkenskapsår och 120 000 000 kronor.

Utredningens förslag

Förslaget från utredningen stämmer i allt väsentligt överens med regeringens. I utredningens förslag anges inte att det ska röra sig om närmast föregående räkenskapsår.

Remissinstanserna

Flera remissinstanser, däribland *Finansinspektionen, Försvarsmakten, Strålsäkerhetsmyndigheten (SSM), Säkerhetspolisen* och ett antal länsstyrelser, tillstyrker förslaget. Finansinspektionen anser att omsättningen hos vissa av myndighetens tillsynsobjekt enligt säkerhetsskyddslagen är så hög att det i sig motiverar ytterligare höjning av sanktionsavgiften. Försvarsmakten anser att det bör förtydligas hur uttrycket total global årsomsättning ska tolkas.

Advokatfirman Kahn Pedersen anser att det, på grund av sanktionsavgifters allmänna straffrättsliknande karaktär, bör tydliggöras att det är tillsynsmyndigheten som har bevisbördan dels för att en överträdelse har skett, dels i förhållande till dess allvar och övriga omständigheter som ska beaktas i fråga om sanktionsavgiftens storlek. Advokatfirman anser även att det bör regleras i lag vilket beviskrav som ska tillämpas för att en sanktionsavgift ska kunna tas ut. *Affärsverket svenska kraftnät* förutser att förslaget kan skapa förvirring i tillämpningen eftersom säkerhetsskyddslagen utgår från att en verksamhetsutövare utgörs av en juridisk person, och inte av exempelvis en koncern. *Stokab AB* anser att nuvarande nivåer är tillräckligt avskräckande men har förståelse för förslaget utifrån en jämförelse med sanktionsavgiften enligt bland annat förslaget om den nya lagen om motståndskraft hos kritiska verksamhetsutövare. Stokab AB understryker att möjligheten att besluta om högre sanktionsavgifter samtidigt ställer höga krav på tydliga regler och vägledning för reglernas tillämpning. *Tech Sverige* avstyrker förslaget och anser att det saknas indikationer på att nuvarande nivåer inte har tillräckligt avskräckande effekt. Tech Sverige pekar på svårigheterna för en verksamhetsutövare att bedöma vad som utgör fara för rikets säkerhet, och bedömer att det med

ett så komplext och svårtolkat regelverk och brist på konkret vägledning till verksamhetsutövare är olämpligt med mer ingripande sanktioner.

Några remissinstanser, bland andra *Energiföretagen Sverige*, Finansinspektionen och SSM, anser att ytterligare ändringar bör övervägas i förhållande till säkerhetsskyddslagen. Finansinspektionen anser till exempel att anmärkning bör införas som en ingripandemöjlighet även i säkerhetsskyddslagen och SSM anser att tillsynsmyndigheterna bör ges möjlighet att besluta om vilka enskilda verksamhetsutövare som bedriver säkerhetskänslig verksamhet.

Skälen för regeringens förslag

Bakgrund till säkerhetsskyddslagens utformning och sanktionsavgifter i andra sammanhang

En sanktionsavgift enligt säkerhetsskyddslagen ska bestämmas till lägst 25 000 kronor och högst 50 000 000 kronor. Sanktionsavgiften för en statlig myndighet, kommun eller region ska dock bestämmas till högst 10 000 000 kronor.

Sanktionsavgift infördes i säkerhetsskyddslagen för att säkerställa säkerhetsskyddslagstiftningens efterlevnad. Sanktionsavgift ska enligt förarbetena i första hand komma i fråga vid åsidosättande av de mest centrala skyldigheterna enligt säkerhetsskyddslagstiftningen (se prop. 2020/21:194 s. 92 f.). Vidare anfördes att säkerhetsskyddslagen omfattar olika typer av aktörer, såsom statliga myndigheter, kommuner, regioner och företag. Aktörerna skiljer sig dessutom åt i storlek och ekonomiska förutsättningar. De överträdelser som kan leda till sanktionsavgift är också av varierande karaktär och inrymmer allt från mindre allvarliga överträdelser till mycket allvarliga sådana som kan leda till stora skador för Sveriges säkerhet. För att kunna bestämma sanktionsavgifter som är effektiva, proportionella och avskräckande i alla enskilda fall borde beloppsintervallet enligt regeringen vara mycket stort. Regeringen anförde vidare att den avgiftsskyldiges finansiella ställning kan ha betydelse vid bedömning av sanktionsavgiftens storlek. Maximibeloppet bestämdes därför till 50 000 000 kronor i visst avseende. För statliga myndigheter, regioner och kommuner ansåg regeringen att det inte var motiverat med ett lika högt maximibelopp för att påverka agerandet i önskvärd riktning. Ett felaktigt handlande av en myndighet föranleds sällan av en önskan att maximera sin vinst. Sanktionsavgiftens maximibelopp för dessa verksamhetsutövare bestämdes därför till 10 000 000 kronor. Minimibeloppet bestämdes till 25 000 kronor.

Sanktionsavgiften enligt lagen om granskning av utländska direktinvesteringar ska bestämmas till lägst 25 000 kronor och högst 100 000 000 kronor (32 §).

Enligt cybersäkerhetslagen ska sanktionsavgifter bestämmas till lägst 5 000 kronor. För enskilda verksamhetsutövare som är väsentliga ska sanktionsavgiften bestämmas högst till det högsta av 2 procent av verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår eller ett belopp i kronor motsvarande 10 000 000 euro. För enskilda verksamhetsutövare som är viktiga ska avgiften bestämmas högst till det högsta av 1,4 procent av verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår eller ett belopp i kronor

motsvarande 7 000 000 euro. För offentliga verksamhetsutövare ska avgiften bestämmas till högst 10 000 000 kronor.

I avsnitt 11.5.2 föreslås att sanktionsavgiften för enskilda verksamhetsutövare enligt den nya lagen om motståndskraft hos kritiska verksamhetsutövare ska bestämmas till lägst 5 000 kronor och till högst det högsta av 2 procent av verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår och ett belopp i kronor motsvarande 10 000 000 euro. För offentliga verksamhetsutövare föreslås avgiften bestämmas till lägst 5 000 kronor och högst till 10 000 000 kronor.

Vad bör gälla enligt säkerhetsskyddslagen fortsättningsvis?

Utredningen föreslår att maximibeloppet för sanktionsavgiftens storlek i säkerhetsskyddslagen ska höjas för verksamhetsutövare som inte är en statlig myndighet, en kommun eller en region. En sanktionsavgift ska enligt förslaget bestämmas högst till det högsta av 120 000 000 kronor eller 2 procent av verksamhetsutövarens totala globala årsomsättning under föregående räkenskapsår. Den föreslagna höjningen innebär enligt utredningens mening att regeringens ambitioner om att sanktionsavgiftens storlek ska kunna vara avskräckande för alla verksamhetsutövare upprätthålls. När det gäller andra verksamhetsutövare gör utredningen bedömningen att det inte ska göras någon förändring av avgiftens storlek. Den nuvarande högsta avgiften om 10 000 000 kronor är en effektiv, proportionell och avskräckande sanktion också för allvarliga överträdelser av en statlig myndighet, kommun eller region.

Tech Sverige anser att det saknas indikationer på att nuvarande nivåer inte har tillräckligt avskräckande effekt. Regeringen konstaterar att säkerhetsskyddsregleringen gäller för de mest skyddsvärda verksamheterna i samhället. Som regeringen har gett uttryck för i andra sammanhang är det inte önskvärt att brister i en aktörs säkerhetsskydd leder till mindre ingripande åtgärder än brister i andra delar av aktörens verksamhet som inte rör säkerhetskänslig verksamhet och som därför omfattas av NIS 2- eller CER-direktiven (jfr prop. 2022/23:116 s. 126). Därför bör högre sanktionsavgifter enligt säkerhetsskyddslagen kunna komma i fråga. En höjning av sanktionsavgifterna innebär inte att nya överväganden ska göras i fråga om när en sanktionsavgift ska kunna komma i fråga. I vilka fall som en sanktionsavgift ska kunna aktualiseras enligt säkerhetsskyddslagen är tydligt genom tidigare förarbeten och det finns varken utrymme eller anledning att göra uttalanden i dessa avseenden inom ramen för denna proposition. Detsamma gäller i fråga om bevisbörda och beviskrav, som *Advokatfirman Kahn Pedersen* resonerar kring.

Regeringen ställer sig sammanfattningsvis bakom utredningens förslag om vilken ändring som bör ske gällande säkerhetsskyddslagen. Det bör anges att det rör sig om närmast föregående räkenskapsår (jfr avsnitt 11.5.2). Hur uttrycket total global årsomsättning bör tolkas, som *Försvarsmakten* nämner, behandlas i avsnitt 11.5.2. *Affärsverket svenska kraftnät* förutser att förslaget kan skapa förvirring i tillämpningen eftersom säkerhetsskyddslagen utgår från att en verksamhetsutövare utgörs av en juridisk person, och inte av exempelvis en koncern. Hur uttrycket verksamhetsutövare bör tolkas i den nya lagen som genomför CER-

direktivet utvecklas i avsnitt 5.3. Även cybersäkerhetslagen utgår från att en verksamhetsutövare utgörs av ett enskilt rättssubjekt och inte av en koncern (se prop. 2025/26:28 s. 52). Mot denna bakgrund kan regeringen inte se att det föreligger någon sådan skillnad mellan regleringarna som ger skäl för att avvika från utredningens förslag eller som ger skäl för att befara tillämpningssvårigheter.

Som *Stokab AB* understryker krävs tydliga regler och vägledning. Det finns dock inte skäl att införa ytterligare reglering i lag. Föreskrifter på lägre författningsnivå och vägledning kan innehålla sådana regler. Det finns inte utrymme för att, som *Energiföretagen Sverige*, *Finansinspektionen* och *SSM* berör, genomföra ytterligare ändringar i säkerhetsskyddslagen inom ramen för denna proposition.

15 Ikraftträdande- och övergångsbestämmelser

Regeringens förslag

Den nya lagen och övriga lagändringar ska träda i kraft den 1 januari 2027.

Äldre bestämmelser ska gälla för överträdelser av säkerhetsskyddslagen som har ägt rum före ikraftträdandet av den ändrade bestämmelsen om sanktionsavgiftens storlek.

Utredningens förslag

Förslaget från utredningen stämmer inte överens med regeringens. Utredningen föreslår att den nya lagen och övriga lagändringar ska träda i kraft den 1 augusti 2025. Utredningen föreslår inga övergångsbestämmelser.

Remissinstanserna

Remissinstanserna yttrar sig inte särskilt över förslaget.

Skälen för regeringens förslag

Av artikel 26 i CER-direktivet följer att medlemsstaterna senast den 17 oktober 2024 skulle anta och offentliggöra de bestämmelser som är nödvändiga för att följa direktivet. Bestämmelserna skulle tillämpas från den 18 oktober 2024. I direktivet anges vidare vissa andra tidsfrister för medlemsstaterna. Senast den 17 juli 2026 ska medlemsstaterna enligt artikel 6 identifiera de kritiska entiteterna för de sektorer och undersektorer som anges i bilagan till direktivet.

Den nya lagen bör träda i kraft så snart som möjligt. Lagens tillämpningsområde föreslås dock avgränsas närmare inom ramen för föreskrifter på en lägre författningsnivå och dessa föreskrifter måste ha utfärdats innan lagen kan tillämpas fullt ut. Tillsynsmyndigheterna och

berörda verksamhetsutövare måste också ges möjlighet att anpassa sin verksamhet i den utsträckning som krävs för att de ska kunna fullgöra sina uppgifter respektive skyldigheter enligt den nya lagen. Det finns inte anledning att låta vissa delar av lagen träda i kraft senare än andra. Med hänsyn till detta och vid en samlad bedömning anser regeringen att lagen i sin helhet bör träda i kraft den 1 januari 2027. Även övriga lagändringar bör träda i kraft detta datum.

Regeringen bedömer, till skillnad från utredningen, att det finns behov av en övergångsbestämmelse med anledning av den ändring som sker av säkerhetsskyddslagen (se avsnitt 14). Äldre bestämmelser bör gälla för överträdelser som har ägt rum före ikraftträdandet av den ändrade bestämmelsen.

16 Konsekvenser av förslagen

16.1 Konsekvenser för motståndskraften hos kritiska verksamhetsutövare och samhällsekonomin

Regeringens bedömning

Förslagen som genomför CER-direktivet innebär att motståndskraften hos kritiska verksamhetsutövare stärks, och de samhällsekonomiska effekterna av förslagen är godtagbara.

Konsekvenserna som en med beredskapsregleringen delvis parallell reglering för med sig måste i nuläget accepteras.

Utredningens bedömning

Bedömningen från utredningen stämmer överens med regeringens.

Remissinstanserna

Många av remissinstanserna, däribland *Drivkraft Sverige, Försvarets materielverk, Livsmedelsverket* och *Säkerhetspolisen*, välkomnar den nya lagen och uttrycker att utredningens förslag innebär att motståndskraften i samhället stärks.

Flera remissinstanser anser att utredningens förslag behöver bearbetas ytterligare för att vara effektiva och ändamålsenliga. *Länsstyrelsen i Östergötlands län* pekar på att utredningens förslag i flera delar avviker från etablerade system och uttryck inom krisberedskap, totalförsvar och informationssäkerhet och anser att förslagen därigenom riskerar att försvåra arbetet med att stärka förmågan i samhällsviktig verksamhet. *Myndigheten för civilt försvar (MCF)* anser att utredningens förslag inte nyttjar CER-direktivets fulla potential att skapa en förmågeeffekt i samhället och inte heller innebär att man uppnår syftet med direktivet som är att stärka kritiska verksamhetsutövares motståndskraft. Förslagen riskerar enligt MCF att komplicera den fortsatta utvecklingen inom krisberedskap och civilt försvar, och skapa två överlappande men

parallella system som kommer innebära otydlighet, ineffektivitet och dubbelarbete för berörda verksamhetsutövare.

Ett antal remissinstanser, däribland *Gävle kommun* och *Umeå kommun*, anser att det är svårt att bedöma hur stor påverkan lagen kommer att få innan de kritiska verksamhetsutövarna har identifierats. *Försäkringskassan* och *Svenskt Vatten* anser att det är svårt att bedöma vilka konsekvenser förslagen kommer att få till följd av att det i många delar föreslås bemyndiganden till olika myndigheter att meddela föreskrifter.

Ett fåtal remissinstanser resonerar kring de samhällsekonomiska effekterna av förslagen. *Stockholms kommun* pekar på risken för att berörda verksamhetsutövare till följd av förslagen, som innebär ett utökat antal tillsynsmyndigheter att rapportera till, behov av utvecklade incidenthanteringssystem och ökade krav på bakgrundskontroller, kommer att behöva lägga mer resurser på kontrollfunktioner och rapportering än utveckling av säkerhetsarbetet. *Sveriges advokatsamfund* anser att utredningens förslag, som bland annat innebär att tillsynen fördelas på olika myndigheter, innebär ett ineffektivt nyttjande av statens resurser och motverkar lagens syfte, samt att enskilda verksamhetsutövare kan orsakas onödiga kostnader och betydande regulatoriska utmaningar. *Vattenfall AB* ser en risk för ökad komplexitet med den nya lagen på grund av att flera lagar kommer att överlappa varandra. Detta kan enligt Vattenfall AB leda till bland annat en ineffektiv användning av resurser och minskad effekt i säkerhetsarbetet.

Skälen för regeringens bedömning

Konsekvenser för motståndskraften hos kritiska verksamhetsutövare och samhällsekonomin

Förslagen i denna proposition innebär att CER-direktivet införlivas i svensk rätt. Syftet med direktivet är att stärka motståndskraften hos kritiska verksamhetsutövare för att upprätthålla samhällsviktiga tjänster inom sektorerna energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, dricksvatten, avloppsvatten, digital infrastruktur, offentlig förvaltning, rymden samt produktion, bearbetning och distribution av livsmedel. CER-direktivet är ett bindande minimidirektiv med innebörd att medlemsstaten får anta bestämmelser i nationell rätt som syftar till att uppnå en högre grad av motståndskraft. I propositionen lämnas i princip inga förslag som går utöver direktivets krav (jfr avsnitt 5.3).

Samhällsviktiga tjänster och kritisk infrastruktur spelar en oumbärlig roll när det gäller att upprätthålla viktiga funktioner och central ekonomisk verksamhet både på den inre marknaden och i Sverige. Att stärka motståndskraften hos kritiska verksamhetsutövare är centralt för att förebygga, motstå och hantera incidenter som kan ge allvarliga störningar i samhällsviktiga tjänster. Incidenter kan hindra bedrivande av ekonomisk verksamhet, generera omfattande ekonomiska förluster, undergräva förtroende för tjänsternas tillhandahållande och medföra allvarliga konsekvenser för Sveriges och EU:s ekonomi. Incidenter kan också medföra allvarliga konsekvenser för invånarna i Sverige.

Ett antal remissinstanser, däribland *Gävle kommun* och *Svenskt Vatten*, anser att det är svårt att bedöma hur stor påverkan lagen kommer att få av

olika skäl. Den nya lagen är en del i arbetet med att säkerställa att verksamhetsutövare som tillhandahåller för samhället grundläggande tjänster vidtar fler och mer ändamålsenliga åtgärder i syfte att stärka motståndskraften i deras verksamhet. Det står därmed redan nu klart att lagen innebär att motståndskraften hos kritiska verksamhetsutövare stärks. Den nya lagens förhållande till annan befintlig reglering och förutsättningarna för att utvidga lagens tillämpningsområde, som bland andra *Länsstyrelsen i Östergötlands län* nämner, behandlas i avsnitt 5.1.

Ett antal remissinstanser yttrar sig gällande de samhällsekonomiska effekterna av förslagen. Motståndskraft hos kritiska verksamhetsutövare är viktigt för att den inre marknaden och den svenska marknaden ska fungera väl. Det kan konstateras att den föreslagna lagen är en förutsättning för att genomföra CER-direktivet i svensk rätt. Regeringen bedömer att en konsekvent nivå av motståndskraft i samhällsviktiga tjänster kan leda till kostnadsbesparingar för verksamhetsutövarna på längre sikt även om det på kort sikt kan uppstå kostnader för att möta kraven. Vidare kan höjda säkerhetsnivåer bidra till att minska negativa konsekvenser av incidenter, vilket i sin tur kan ha en positiv inverkan på tillväxt och investeringar och därmed samhällsekonomin i stort. De samhällsekonomiska effekterna är oavsett godtagbara givet bakgrunden till och syftet med regelverket.

Konsekvenser av ett delvis parallellt system i förhållande till beredskapssystemet

Förslagen i denna proposition innebär att den nya lagen som genomför CER-direktivet och det svenska beredskapssystemet delvis kommer att gälla parallellt. Som konstateras i avsnitt 5.1 tar regeringen frågan om de negativa effekter som delvis parallella system kan föra med sig, som bland andra *MCF* nämner, på mycket stort allvar. Regeringen konstaterar samtidigt att den nya lagen har ett bredare tillämpningsområde än den reglering som ligger till grund för det svenska beredskapssystemet i den bemärkelsen att en bredare krets av aktörer kommer att omfattas av den nya lagen. Det handlar därmed om en begränsad överlappning. Den nya lagen innebär också andra skyldigheter än beredskapssystemet. Som utvecklas i nämnda avsnitt bedömer regeringen, av olika skäl, att det finns ett värde i att låta terminologin som används i den nya lagen så långt som det är möjligt stämma överens med terminologin i CER-direktivet. Den föreslagna begreppsanvändningen innebär på samma gång att aktörer som omfattas av båda regelverken kommer att få förhålla sig till närliggande uttryck med eventuellt delvis olika innebörd. Även det av utredningen föreslagna systemet för tillsyn och systemet med sektorsansvariga myndigheter enligt beredskapssystemet skiljer sig delvis åt (jfr avsnitt 10.1).

Regeringen konstaterar att Sverige och andra medlemsstater genom CER-direktivet har enats på EU-nivå om vad som bör vara grundläggande krav för motståndskraft när det gäller samhällsviktiga tjänster. Direktivet skulle ha genomförts i nationell rätt i oktober 2024. Den föreslagna lagen är en förutsättning för att genomföra CER-direktivet i Sverige. Som nämns i avsnitt 5.1 finns det inget utrymme för att göra en anpassning till det svenska beredskapssystemet på det sätt som bland annat MCF efterfrågar

inom ramen för detta lagstiftningsärende. Det går inte heller i nuläget, enligt regeringens mening, att med säkerhet uttala sig om vilka konsekvenser som de parallella regelverken kan föra med sig. Som regeringen bedömer i nämnda avsnitt finns det dock skäl att efter den nya lagens ikraftträdande göra en översyn av regelverken.

Myndigheterna med ansvar enligt de olika regelverken kommer att utföra sina uppdrag utifrån delvis olika perspektiv och med olika befogenheter. Det finns enligt regeringens mening ingen risk för att berörda aktörer kommer att bedöma att det finns en otydlighet i fråga om vilken reglering som myndigheterna agerar utifrån om utredningens förslag om utpekande av tillsynsmyndigheter enligt den nya lagen genomförs. Regeringen vill också, med anledning av den framförda remisskritiken, betona myndigheters generella ansvar att samverka med varandra enligt förvaltningslagen och myndighetsförordningen. Regeringen utgår ifrån att samverkan mellan berörda myndigheter kommer att fungera väl när det gäller sådana frågor som de parallella regelverken kan ge upphov till och som behöver hanteras gemensamt.

16.2 Ekonomiska konsekvenser för den offentliga sektorn

Regeringens bedömning

Förslagen som genomför CER-direktivet innebär ökade kostnader för tillsynsmyndigheterna och Myndigheten för civilt försvar. Kostnaderna ryms inom befintliga anslagsramar.

Förslagen leder till ökade kostnader för kommuner och regioner. Kostnaderna finansierades i budgetpropositionen för 2026.

Förslagen innebär ökade kostnader för allmänna förvaltningsdomstolar. Kostnaderna ryms inom domstolarnas befintliga anslagsramar. De kostnadsökningar som förslagen medför för övriga statliga myndigheter kan också hanteras inom befintliga ekonomiska ramar.

Utredningens bedömning

Bedömningen från utredningen stämmer delvis överens med regeringens. Utredningen gör dock ingen bedömning i fråga om konsekvenser för allmänna förvaltningsdomstolar. Utredningen bedömer att det inte krävs någon finansiering för kommuner och regioner. Utredningen bedömer även att kostnaderna för de föreslagna tillsynsmyndigheterna och MCF ska finansieras genom ökade anslag.

Remissinstanserna

Ett antal myndigheter som utredningen föreslår ska pekas ut som tillsynsmyndigheter, bland andra *Finansinspektionen*, *Inspektionen för vård och omsorg (IVO), Livsmedelsverket* och *Statens energimyndighet (Energimyndigheten)*, gör en annan bedömning än utredningen i fråga om vilka kostnader som förslagen innebär för dem. *Statskontoret* anser, i likhet

med utredningen, att det på förhand är svårt att uppskatta ekonomiska konsekvenser kopplat till den löpande tillsynen utan att veta antalet kritiska verksamhetsutövare. *Polismyndigheten* har inga synpunkter gällande förslagen i betänkandet.

Vissa andra remissinstanser, däribland *Försäkringskassan* och *Rymdstyrelsen*, förutser att förslagen medför behov av ökade resurser för offentliga verksamhetsutövare. Försäkringskassan bedömer exempelvis att ökade krav på spårbarhet kommer att kräva utökad loggning och lagring av data vilket i sin tur medför högre kostnader för lagringsutrymme. Att säkra kontinuiteten avseende leveranser kan enligt Försäkringskassan även kräva att avtal tecknas med flera eller större leverantörer som har möjlighet att byta ut komponenter eller leverantörer inom sitt eget underleverantörsnät om det krävs. *Skatteverket* bedömer att förslagen innebär en viss ekonomisk konsekvens för myndigheten genom ökad administration på grund av de åtgärder som aktualiseras kopplat till bakgrundskontroller, men att det i nuläget inte är möjligt att beräkna en exakt kostnadsökning.

Domstolsverket bedömer att förslagen inte innebär något som i någon större mån påverkar Sveriges Domstolar.

Flera kommuner och regioner, däribland *Gävle kommun*, *Göteborgs kommun*, *Linköpings kommun, Malmö kommun* och *Region Gotland,* framhåller att förslagen medför betydande kostnader för kommuner och regioner och att dessa behöver tilldelas ökade resurser. *Sveriges Kommuner och Regioner (SKR)* anser det vara avgörande för kommuners och regioners förmåga att bygga upp den civila beredskapen och det civila försvaret att staten tillhandahåller adekvata resurser. *Myndigheten för civilt försvar (MCF)* anser dock att finansieringen, i enlighet med utredningens bedömning, bör ske inom verksamhetsutövarens befintliga budgetram, och ser inte att finansieringsprincipen är relevant. MCF anser, i likhet med utredningen, att det i uppdraget att tillhandahålla en samhällsviktig tjänst ingår att vidta vissa grundläggande säkerhetsåtgärder som att förhindra, reagera på och återhämta sig från incidenter liksom att ha ett gott fysisk skydd för lokaler och kritisk infrastruktur, och att denna typ av åtgärder därmed rimligen redan borde ha genomförts när det gäller offentlig verksamhet i kommunal, regional och statlig regi.

Skälen för regeringens bedömning

Konsekvenser för myndigheter med uppgifter enligt lagen

Den nya lagen innebär uppgifter för de myndigheter som kommer att pekas ut som tillsynsmyndigheter. Utredningen föreslår att Statens energimyndighet, Transportstyrelsen, Inspektionen för vård och omsorg, Läkemedelsverket, Livsmedelsverket, Post- och telestyrelsen samt länsstyrelserna i Norrbottens, Skåne, Stockholms och Västra Götalands län ska pekas ut som tillsynsmyndigheter. I avsnitt 10.1 föreslår regeringen att tillsynsmyndigheterna ska pekas ut i förordning och vilka sektorer som tillsynsmyndigheterna ska ansvara för föreslås inte heller regleras i lag. Förslagen i denna proposition kommer att innebära kostnader för de myndigheter som pekas ut som tillsynsmyndigheter. Förslagen kommer också att innebära nya uppgifter för MCF, enligt utredningens förslag till förordning, och Polismyndigheten.

Utredningen, som i betänkandet föreslår den 1 augusti 2025 som ikraftträdandedatum för regleringen, föreslår att regeringen för 2025 och 2026 ger samtliga av utredningen föreslagna tillsynsmyndigheter, förutom Finansinspektionen, ett förstärkt anslag med en miljon kronor per år med anledning av kommande uppdrag som tillsynsmyndigheter. Utredningen lämnar motsvarande förslag gällande MCF. Utredningen bedömer att de kostnader som förslagen medför för Finansinspektionen bör finansieras inom ramen för befintligt anslag. Polismyndighetens kostnader för att anpassa it-system för det utdrag ur belastningsregistret som följer av den föreslagna bakgrundskontrollen bör enligt utredningen finansieras inom befintligt anslag. Kostnaden för den löpande hanteringen av utdrag bör enligt utredningen beräknas när identifieringen av kritiska verksamhetsutövare är genomförd och när dessa har gjort den föreskrivna befattningsanalysen. De löpande kostnaderna bör enligt utredningen följas upp.

Regeringen delar utredningens uppfattning att kostnaderna för Polismyndigheten ryms inom befintligt anslag. När det gäller kostnaderna för de av utredningen föreslagna tillsynsmyndigheterna och MCF bedömer regeringen, trots ovan angiven kritik, att dessa kan hanteras inom givna budgetramar. Regeringen avser dock att följa frågan.

Konsekvenser för andra statliga myndigheter

Förslagen kan innebära skyldigheter och nya uppgifter för statliga myndigheter som pekas ut som kritiska verksamhetsutövare. Vissa remissinstanser, däribland *Försäkringskassan* och *Rymdstyrelsen*, förutser att förslagen medför behov av ökade resurser för dessa offentliga verksamhetsutövare.

De statliga myndigheter som omfattas av regleringen kommer i olika utsträckning att behöva genomföra vissa förändringar för att nå upp till de krav som föreslås gälla enligt förslagen i denna proposition och dessa åtgärder kan vara kostnadsdrivande. Som utvecklas i avsnitt 16.3 i fråga om enskilda verksamhetsutövare är det svårt att göra generella uttalanden om vilka kostnader som den nya lagen innebär för dem som kommer att omfattas av densamma. Åtgärderna kommer dock att leda till ökad motståndskraft hos offentliga verksamhetsutövare och effekterna kommer enligt regeringens bedömning sannolikt att uppväga eventuella kostnader för dessa myndigheter. Regeringens sammantagna bedömning är att kostnaderna för berörda myndigheter inte bör vara så stora att de inte kan hanteras inom givna budgetramar.

Tillsynsmyndighetens beslut får överklagas till allmän förvaltningsdomstol vilket kan medföra en ökning av antalet mål där. Det bedöms dock endast bli fråga om ett fåtal ytterligare beslut som kommer att prövas i domstol. De ekonomiska konsekvenserna för domstolarna kan därför, som *Domstolsverket* resonerar om, hanteras inom befintliga budgetramar.

Konsekvenser för kommuner och regioner

Den kommunala finansieringsprincipen innebär att kommuner och regioner ska kompenseras för statligt beslutade åtgärder som direkt tar sikte på den kommunala verksamheten. Principen gäller när riksdagen, regeringen eller en myndighet fattar bindande beslut om ändrade regler för verksamhet.

Som framgår av avsnitt 8 innebär förslagen bland annat att kommuner och regioner som identifieras som kritiska verksamhetsutövare, liksom andra kritiska verksamhetsutövare, får nya skyldigheter i form av att genomföra riskbedömningar, vidta åtgärder för motståndskraft och i vissa fall rapportera incidenter. Utredningen bedömer att finansieringsprincipen inte behöver tillämpas eftersom kraven enligt den nya regleringen inte är direkt riktade mot kommuner och regioner utan riktas till tillhandahållare av en samhällsviktig tjänst. Förslagen innebär dock nya åtaganden för kommuner och regioner och leder, som bland andra *SKR* nämner, till ökade kostnader för kommuner och regioner som kräver finansiering enligt den kommunala finansieringsprincipen. Mot denna bakgrund finansierades dessa kostnader med 75 miljoner kronor per år under perioden 2026–2028 genom förslagen i budgetpropositionen för 2026 (se prop. 2025/26:1 s. 150).

16.3 Konsekvenser för enskilda

Regeringens bedömning

Förslagen som genomför CER-direktivet kan innebära ökade kostnader och administrativa bördor för enskilda verksamhetsutövare. Förslagen kan också få konkurrensmässiga konsekvenser och innebära ökade kostnader för konsumenter och användare. Förslagen kan även innebära konsekvenser för arbetssökande, arbetstagare och andra som deltar i verksamheten och kan inverka på deras personliga integritet. Dessa konsekvenser är godtagbara.

Utredningens bedömning

Bedömningen från utredningen stämmer delvis överens med regeringens. Utredningen gör bedömningen att förslagen för närvarande inte innebär några ekonomiska konsekvenser för enskilda verksamhetsutövare. Utredningen bedömer att regleringen inte heller får effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt. Utredningen gör i övrigt ingen särskild bedömning i fråga om konsekvenserna för enskilda.

Remissinstanserna

Ett antal remissinstanser, däribland *Bolagsverket*, *Svensk Handel* och *Tech Sverige* anser att det behövs kompletterande analyser av vilka ekonomiska och andra konkurrensmässiga konsekvenser som förslagen innebär för enskilda verksamhetsutövare. Flera remissinstanser, bland andra Bolagsverket, *Energiföretagen Sverige, Lantbrukarnas Riksförbund* och *Svensk Dagligvaruhandel,* framhåller att förslagen kommer att innebära en ökad administrativ börda och ökade kostnader för enskilda verksamhetsutövare. Energiföretagen Sverige förutser att mindre företag kan få en konkurrensnackdel på grund av högre fasta kostnader per försäljningsvolym per kund. Även Svensk Dagligvaruhandel ser en risk för en snedvriden konkurrens inom dagligvaruhandeln där det finns få stora aktörer. *Malmö kommun*

anser att besparingar möjligtvis kan ske på sikt men att det inledningsvis torde vara tvärtom. Malmö kommun ifrågasätter utredningens slutsats om att regleringen inte får effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt.

Stockholm Vatten och Avfall ser positivt på utredningens förslag om att det för enskilda verksamhetsutövare kan finnas anledning att överväga om det finns behov av att införa statligt stöd. Även *Transportföretagen* anser att det är rimligt att de företag som berörs kompenseras för de merkostnader som förslagen innebär för företagen.

Regelrådet finner att utredningens konsekvensutredning är bristfällig i fråga om information om vilka företag som berörs samt regleringens påverkan på berörda företags kostnader, tidsåtgång och verksamhet.

Skälen för regeringens bedömning

Konsekvensanalyser i andra sammanhang

EU-kommissionen har uppskattat att antalet små och medelstora företag som omfattas av CER-direktivet är begränsat. Inom sektorerna transport, energi och vatten kommer de kritiska entiteterna, enligt kommissionen, sannolikt och typiskt sett att vara större företag med tusentals anställda. I andra sektorer kan det dock enligt kommissionen röra sig om mindre företag som omfattas av regleringen. Kommissionen bedömer vidare att de ökade kostnaderna som regleringen kan innebära i det enskilda fallet uppvägs av det faktum att tillhandahållandet av samhällsviktiga tjänster blir mer tillförlitligt. Kostnaderna kommer vidare, enligt kommissionen, att vara begränsade för de operatörer som redan uppfyller motsvarande krav som härrör från befintlig sektorslagstiftning på EU-nivå. Detta framgår av ett arbetsdokument från kommissionens avdelningar som utgör ett följedokument till förslaget till CER-direktivet (se COM [2020] 829 final} - {SEC [2020] 433 final} - {SWD [2020] 359 final}).

I propositionen som avser genomförandet av CER-direktivet i Finland anges att bedömningen av de ekonomiska konsekvenserna är förknippad med viss osäkerhet eftersom konsekvenserna är beroende av huruvida en aktör identifieras som en kritisk aktör inom ramen för den nationella strategin och riskbedömningen, vilket också påverkas av förändringarna i omvärlden (se RP 205/2024 rd s. 81 f.). Genomförandet av skyldigheterna enligt propositionen bedöms kunna leda till ökade kostnader för de aktörer som identifieras som kritiska i och med att de måste fullgöra sina skyldigheter. Å andra sidan innehåller den gällande lagstiftningen i Finland redan liknande skyldigheter eller så har aktörerna på frivillig basis ägnat uppmärksamhet åt sin motståndskraft till exempel inom försörjningsberedskapsverksamheten. Enligt propositionen kan ekonomiska konsekvenser uppstå i synnerhet för aktörer som inte tidigare har omfattats av skyldigheter i fråga om riskhantering eller beredskap för störningssituationer och undantagsförhållanden. Samtidigt begränsar en förbättrad motståndskraft omfattningen av incidenter eller förhindrar incidenter och deras konsekvenser, vilket förhindrar uppkomsten av kostnader för störningar. Någon särskild bedömning i fråga om de ekonomiska konsekvenserna för enskilda aktörer görs inte i propositionen.

Vid genomförandet av direktivet i Danmark har det uttalats att det inte var möjligt att närmare uppskatta de ekonomiska konsekvenserna av

lagförslaget, eftersom det råder stor osäkerhet om både effekterna av de kommande kraven och vilka som omfattas av lagen (se Forslag til Lov om kritiske enheders modstandsdygtighed [CER-loven] s. 29). De ekonomiska och administrativa konsekvenserna kommer enligt propositionen att bero på den befintliga motståndskraftsnivån hos de berörda företagen och utvecklingen av hotbilden i samhället.

Konsekvenser för dem som omfattas av den svenska lagen

Den föreslagna regleringen kommer att innehålla bestämmelser som innebär att enskilda aktörer behöver uppfylla vissa krav. Utredningen gör bedömningen att förslagen inte innebär några ekonomiska konsekvenser för enskilda verksamhetsutövare. Utredningen bedömer att regleringen inte heller får effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt. Ett antal remissinstanser, till exempel *Bolagsverket*, har synpunkter på utredningens beskrivning av vilka konsekvenser som förslagen innebär för enskilda aktörer som omfattas av regelverket. *Regelrådet* påpekar bland annat att det saknas information i utredningens konsekvensanalys om vilka företag som berörs och hur de påverkas av regleringen.

Vilka företag som träffas av den nya lagen och vilka åtgärder som de ska vidta är i allt väsentligt en följd av direktivets utformning. För att omfattas av lagen krävs dock att den enskilda aktören dessutom identifieras som en kritisk verksamhetsutövare av en myndighet. De krav som föreslås gälla för att bli identifierad som en kritisk verksamhetsutövare medför att antalet enskilda verksamhetsutövare torde vara betydligt färre än det totala antalet verksamhetsutövare i respektive sektor som lagen föreslås gälla för. Det står klart att förslagen kan innebära ökade kostnader och administrativa bördor för de företag som kommer att identifieras som kritiska verksamhetsutövare. Frågan är dock om det, som vissa remissinstanser begär, går att på förhand utveckla vilka ökade kostnader och administrativa bördor som regelverket innebär för dessa aktörer.

När det gäller skyldigheten att rapportera incidenter bedömer regeringen att kostnaderna hänförliga till denna skyldighet bör bli begränsade. Det bör generellt sett röra sig om ett begränsat antal fall som ett enskilt företag behöver rapportera om, särskilt eftersom endast sådana incidenter som medför eller kan medföra betydande störningar ska rapporteras. Skyldigheten att medverka till tillsynsåtgärder, när sådana väl vidtas, bör inte heller innebära någon större kostnad för den enskilde aktören.

Regeringen bedömer att den största kostnaden för enskilda hänför sig till riskbedömningen och de åtgärder för motståndskraft som ska vidtas enligt den nya lagen. Det kommer att vara tillsynsmyndigheten, eller ytterst en domstol, som avgör vilka åtgärder som en verksamhetsutövare är skyldig att vidta för att uppfylla kraven i den nya lagen och om verksamhetsutövarens riskbedömning överensstämmer med de krav som ställs. Det är inte möjligt att göra några uppskattningar som är relevanta för samtliga verksamhetsutövare. De åtgärder för motståndskraft som ska vidtas ska för varje verksamhetsutövare vara lämpliga och proportionella och säkerställa en nivå på motståndskraft som är lämplig i förhållande till risken. Riskbedömningen ska innehålla en redogörelse för alla, för den enskilde aktören, relevanta riskerna för en incident.

De som föreslås kunna räknas som verksamhetsutövare bedriver verksamhet inom vitt skilda sektorer och deras verksamheter kan se mycket olika ut. Vidare påverkar nivån av motståndskraft som verksamhetsutövaren i dagsläget når upp till behovet av ytterligare åtgärder. De kostnader som uppstår för en verksamhetsutövare när den nya lagen träder i kraft påverkas bland annat av om aktören sedan tidigare har hanterat risker på frivillig grund eller om denne har varit förpliktat att göra det på grund av sektorsspecifika bestämmelser. Av direktivet framgår att vissa sektorer, exempelvis energi- och transport, redan är reglerade genom sektorsspecifika unionsrättsakter men att dessa endast rör vissa aspekter medan direktivet har ett allriskperspektiv (skäl 4). I sektorn dricksvatten finns redan i dag föreskrifter om fysiskt skydd. Vissa anläggningar i de nu aktuella sektorerna är också i dag skyddsobjekt och har genom detta ett förstärkt tillträdesskydd. Detta innebär att flertalet kritiska verksamhetsutövare redan har vidtagit, i vart fall vissa, åtgärder som krävs enligt förslaget.

Hur pass stora kostnader som uppstår för en enskild aktör med anledning av skyldigheten att bland annat vidta åtgärder för motståndskraft påverkas också av verksamhetens art och omfattning. Kostnaderna kan bli högre ju större och mer omfattande ett företags verksamhet är. Å andra sidan kan även ett mindre företag drabbas av väsentliga kostnader, om dess affärsverksamhet har särdrag som innebär att verksamheten är förenad med särskilda risker. Det kommer att vara svårt att separera kostnaderna som är hänförliga till lagens införande från övriga kostnader med koppling till motståndskraft hos kritiska verksamhetsutövare. Det kommer till exempel att vara svårt att bedöma vilka kostnader kopplade till fysisk säkerhet som enbart är att hänföra till lagens införande jämfört med vad ett ändamålsenligt verksamhetsskydd rent generellt kräver. Det är många faktorer som påverkar kostnaderna för exempelvis incidenthantering, som ingår i lagens krav på åtgärder för motståndskraft, såsom störningens art och omfattning, dess konsekvenser för kontinuiteten samt hur snabbt verksamhetsutövaren återhämtar sig från incidenten. En betydande incident kan orsaka både direkta utrednings- och reparationskostnader och indirekta kostnader på grund av exempelvis avbrott i verksamheten eller ett skadat anseende.

Det går sammanfattningsvis inte att presentera en mer exakt och för samtliga företag relevant uppskattning av kostnaderna kopplade till införandet av den nya lagen, men flera av förslagen bör inte heller innebära några beaktansvärda kostnader. Förslagen kan dock innebära ökade kostnader och kommer att innebära administrativa bördor för enskilda verksamhetsutövare. Det kan konstateras att förslagen är nödvändiga för att genomföra CER-direktivet i Sverige. De kostnader och administrativa bördor som förslagen kan innebära får anses vara godtagbara givet syftet med regelverket och att regleringen krävs för att genomföra direktivet. Det finns inte anledning att ge särskild ersättning till de som omfattas av lagen som bland annat *Stockholm Vatten och Avfall* anser bör övervägas (jfr prop. 2020/21:194 s. 72 f.).

Bland andra *Malmö kommun* ifrågasätter utredningens slutsats om att regleringen inte får effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt. Vad avser förslagens inverkan på konkurrensförhållandena kan kostnaderna för att följa kraven enligt den

nya lagen komma att variera mellan företag. Detta kan i sig påverka konkurrensförhållandena. Konkurrensförhållandena kan också påverkas positivt av den ökade harmoniseringen som sker på både nationell nivå och inom EU. Det kan stärka en aktörs ställning på marknaden att ha en mer motståndskraftig verksamhet som i mindre utsträckning än andra liknande verksamheter påverkas av incidenter. Förslagen är oavsett detta nödvändiga för att genomföra CER-direktivet i nationell rätt. Konsekvenserna för konkurrensförmågan är därmed godtagbara. Detsamma gäller förslagens konsekvenser för företags arbetsförutsättningar och villkor i övrigt.

Konsekvenserna för företag bör utvärderas

Som anges ovan är det svårt att ge en exakt och för samtliga företag relevant uppskattning av kostnaderna kopplade till införandet av den nya lagen. En utvärdering av konsekvenserna för företagen bör därför ske tre år efter den nya lagens ikraftträdande. I samband med detta bör en översyn av författningarna kopplade till genomförandet av CER-direktivet ske.

Ekonomiska konsekvenser för konsumenter och andra användare

I fråga om de ekonomiska konsekvenserna för konsumenter och andra användare bedömer regeringen, i likhet med utredningen, att de eventuella negativa konsekvenser som förslagen kan innebära för dem är godtagbara. I de fall åtgärder inte har vidtagits för att åstadkomma en tillräcklig nivå av motståndskraft kan det inte uteslutas att kostnader för sådana åtgärder kan avspegla sig i priset för konsumenten och andra användare. Detta ska dock vägas mot de kostnader som kan uppkomma för konsumenter och andra användare på grund av brister i motståndskraften hos den kritiska verksamhetsutövaren.

Konsekvenser av förslaget om bakgrundskontroller för enskilda individer

Konsekvenser för arbetssökande, arbetstagare och andra som deltar i verksamheten, och deras personliga integritet, samt skyddet för personuppgifter beskrivs när det gäller förslaget om bakgrundskontroller i avsnitt 9 och 13.

16.4 Konsekvenser för den kommunala självstyrelsen

Regeringens bedömning

Förslagen som genomför CER-direktivet har ingen påverkan på den kommunala självstyrelsen.

Utredningens bedömning

Bedömningen från utredningen stämmer inte överens med regeringens. Förslagen har enligt utredningen en begränsad påverkan på den

kommunala självstyrelsen men går inte utöver vad som är nödvändigt för att skydda sådan verksamhet som förslagen tar sikte på.

Remissinstanserna

Remissinstanserna yttrar sig inte särskilt över bedömningen.

Skälen för regeringens bedömning

Den kommunala självstyrelsen är grundlagsfäst i Sverige (1 kap. 1 § andra stycket regeringsformen). I 14 kap. 1 § regeringsformen anges att beslutanderätten i kommunerna utövas av valda församlingar. Enligt 14 kap. 2 § regeringsformen sköter kommunerna lokala och regionala angelägenheter av allmänt intresse på den kommunala självstyrelsens grund. Den kommunala självstyrelsen utgör en av grundstenarna för den svenska demokratin (se till exempel prop. 1973:90 s. 188 och bet. 1973:KU26 s. 39).

Principen om den kommunala självstyrelsen framgår av 1 kap. 2 § kommunallagen. Där anges att kommuner och regioner, på demokratins och den kommunala självstyrelsens grund, sköter de angelägenheter som anges i lagen eller i annan författning. Kommuner och regioner får själva ha hand om angelägenheter av allmänt intresse som har anknytning till kommunens eller regionens område eller deras medlemmar och som inte ska tas om hand enbart av staten, en annan kommun, region eller någon annan (2 kap. 1 och 2 §§).

Den kommunala självstyrelsen är inte absolut. Enligt 8 kap. 2 § första stycket 3 regeringsformen beslutar riksdagen genom lag bland annat om kommunernas och regionernas befogenheter och åligganden. Graden av självstyrelse avgörs ytterst av formerna för samverkan mellan staten och den kommunala sektorn (se bland annat prop. 1990/91:117 s. 23 och bet. 2016/17:KU10 s. 86). I 14 kap. 3 § regeringsformen anges att en inskränkning i den kommunala självstyrelsen inte bör gå utöver vad som är nödvändigt med hänsyn till de ändamål som har föranlett den. Vid en sådan proportionalitetsbedömning ska en avvägning göras mellan de kommunala självstyrelseintressena och de nationella intressen som den föreslagna lagstiftningen ska tillgodose.

Ökad motståndskraft kopplat till samhällsviktiga tjänster som erbjuds av kommuner och regioner är en grundläggande förutsättning för att offentlig service ska fungera på ett tillfredsställande sätt. Säkerhetsläget i Sverige och runtom i världen innebär att hela den offentliga sektorn behöver anpassa sig för att kunna möta de utmaningar som finns med att säkerställa en säker offentlig sektor. Sverige och andra medlemsstater har genom CER-direktivet enats på EU-nivå om vad som bör vara grundläggande krav på området. Förslagen innebär nya skyldigheter för stora delar av samhället och inte endast i förhållande till kommunerna och regionerna. Regeringen anser, till skillnad mot utredningen, att förslagen inte kan sägas innebära särskilda konsekvenser för den kommunala självstyrelsen.

16.5 Övriga konsekvenser

Regeringens bedömning

Förslagen som genomför CER-direktivet kan få positiva effekter för det brottsförebyggande arbetet. Förslagen kommer inte att medföra några andra konsekvenser.

Förslaget om ändring i säkerhetsskyddslagen innebär i förlängningen att Sveriges säkerhet stärks. De ekonomiska konsekvenser som förslaget kan innebära för enskilda verksamhetsutövare är godtagbara givet syftet med förslaget. Förslaget får inga andra konsekvenser.

Utredningens bedömning

Bedömningen från utredningen av konsekvenserna av förslagen som genomför CER-direktivet stämmer överens med regeringens. Utredningen gör ingen särskild bedömning i fråga om konsekvenserna av förslaget om ändring i säkerhetsskyddslagen.

Remissinstanserna

Remissinstanserna yttrar sig inte särskilt över bedömningen.

Skälen för regeringens bedömning

Förslagen om krav på riskbedömning och åtgärder för motståndskraft och incidentrapportering i den nya lagen förebygger både avsiktliga angrepp och så kallade handhavandefel. Förslagen bör, i likhet med vad utredningen anger, leda till att brott som riktas mot samhällsviktiga tjänster i viss mån kan förebyggas, upptäckas och förhindras. Förslagen bedöms inte ha betydelse för sysselsättning och offentlig service i olika delar av landet. Förslagen bedöms inte heller ha betydelse för jämställdheten mellan kvinnor och män eller för möjligheterna att nå de integrationspolitiska målen eller få några andra konsekvenser.

Skyddet för Sveriges säkerhet kan stärkas genom förslag som innebär mer verkningsfulla sanktionsmöjligheter vid överträdelser av säkerhetsskyddslagen. De ekonomiska konsekvenser som förslaget i avsnitt 14 kan innebära för vissa verksamhetsutövare i enskilda fall är godtagbara givet syftet med regleringen. Förslaget får inga andra särskilda konsekvenser.

17 Författningskommentar

17.1 Förslaget till lag om motståndskraft hos kritiska verksamhetsutövare

En ny lag om motståndskraft hos kritiska verksamhetsutövare införs. Lagen genomför delvis Europaparlamentets och rådets direktiv (EU)

2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (här benämnt CER-direktivet). Allmänna överväganden om behovet av en ny lag finns i avsnitt 5.1. I följande avsnitt kommenteras förslagen till den nya lagen.

1 kap. Inledande bestämmelser

Lagens tillämpningsområde och syfte

1 § Denna lag gäller för verksamhetsutövare som har identifierats som kritiska med stöd av lagen (kritiska verksamhetsutövare). Syftet med lagen är att stärka kritiska verksamhetsutövares motståndskraft och förmåga att tillhandahålla samhällsviktiga tjänster.

Bestämmelserna i lagen genomför delvis Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG, i den ursprungliga lydelsen (här benämnt CER-direktivet).

I paragrafen anges bland annat lagens tillämpningsområde och syfte. Övervägandena finns i avsnitt 5.1. Paragrafen utformas delvis enligt *Lagrådets* förslag.

Förutsättningarna för att identifiera en verksamhetsutövare som kritisk regleras i 2 kap. 1 och 2 §§ och behandlas i författningskommentaren till dessa paragrafer. Vad som avses med uttrycken motståndskraft och samhällsviktig tjänst framgår av 2 § 4 och 6. I paragrafen anges också att lagen delvis genomför CER-direktivet. Hänvisningar i lagen till CER-direktivet avser direktivet i dess ursprungliga lydelse, en så kallad statisk hänvisning.

Uttryck i lagen

2 § I denna lag betyder

1. *enskild verksamhetsutövare*: en kritisk verksamhetsutövare som inte är en offentlig verksamhetsutövare,
2. *incident*: en händelse som kan medföra en betydande störning eller som medför en störning i den kritiska verksamhetsutövarens tillhandahållande av en samhällsviktig tjänst,
3. *kritisk infrastruktur*: en tillgång, en anläggning, utrustning, ett nätverk eller ett system, eller en del av en tillgång, en anläggning, utrustning, ett nätverk eller ett system, som krävs för tillhandahållandet av en samhällsviktig tjänst,
4. *motståndskraft*: förmågan att förebygga, skydda mot, reagera på, stå emot, begränsa konsekvenserna av, absorbera, anpassa sig till och återhämta sig från en incident,
5. *offentlig verksamhetsutövare*: en kritisk verksamhetsutövare som är
   a) en statlig myndighet, eller
   b) en region, en kommun eller ett kommunalförbund,
6. *samhällsviktig tjänst*: en tjänst som är avgörande för upprätthållandet av centrala samhällsfunktioner, ekonomisk verksamhet, folkhälsa, allmän säkerhet eller för skyddet av miljön och som omfattas av bilagan till CER-direktivet.

I paragrafen anges vad som avses med vissa uttryck som används i lagen. Övervägandena finns i avsnitt 5.1–5.3, 6.2, 6.3, 8.2 och 8.3. Paragrafen utformas delvis enligt *Lagrådets* förslag.

I *punkt 1* anges vad som avses med uttrycket enskild verksamhetsutövare, som kan avse både en fysisk och juridisk person, när det används i lagen. Av punkt 5 framgår vad som avses med offentlig verksamhetsutövare och av 1 § första stycket framgår vad som avses med kritisk verksamhetsutövare. Kategoriseringen som enskild verksamhetsutövare får betydelse för vilken sanktionsavgift som kan komma i fråga med stöd av 5 kap. om verksamhetsutövaren inte uppfyller sina skyldigheter enligt lagen och beslut om sanktionsavgift fattas. En kritisk verksamhetsutövare omfattas som utgångspunkt i sin helhet av lagen oavsett om denne bedriver endast sådan verksamhet som lagen gäller till viss del (jfr 5 §). Det är dock den samhällsviktiga tjänsten som är i fokus vid bedömningen av vilka åtgärder en kritisk verksamhetsutövare ska vidta enligt 3 kap. Övervägandena finns i avsnitt 5.2 och 5.3.

Av *punkt 2* framgår vad som avses med uttrycket incident. Definitionen stämmer i allt väsentligt överens med definitionen i artikel 2.3 i CER-direktivet. Uttrycket förekommer bland annat i 2 kap. 2 § och 3 kap. 2 §. Med incident avses enligt definitionen en händelse som kan medföra en betydande störning eller som medför en störning i den kritiska verksamhetsutövarens tillhandahållande av en samhällsviktig tjänst. Enligt definitionen ska det röra sig om en händelse som på angivet sätt kan påverka eller påverkar en samhällsviktig tjänst som verksamhetsutövaren själv tillhandahåller. Inverkan på en samhällsviktig tjänst som tillhandahålls av någon annan aktör faller därmed utanför definitionen. Regeringen eller den myndighet som regeringen bestämmer får med stöd av 9 § meddela ytterligare föreskrifter om vad som avses med uttrycket. I sådana föreskrifter kan bland annat närmare regleras vad som är skillnaden mellan betydande störning och störning samt den närmare innebörden av uttrycket kan medföra. Övervägandena finns i avsnitt 8.3.

I *punkt 3* anges definitionen av uttrycket kritisk infrastruktur. Definitionen stämmer överens med artikel 2.4 i CER-direktivet. Uttrycket förekommer i 2 kap. 2 § och 3 kap. 3 §. Uttrycket omfattar exempelvis byggnader, nätverks- eller informationssystem och maskiner men även en del av en byggnad, ett sådant system eller en maskin. Det saknar betydelse hur stor del av infrastrukturen som det är fråga om. Även en mindre del av till exempel en maskin kan anses utgöra kritisk infrastruktur. Avgörande är att tillgången, anläggningen, utrustningen, nätverket eller systemet eller delen som det rör sig om krävs för tillhandahållandet av en samhällsviktig tjänst. Detta innebär att det måste finnas en koppling mellan den kritiska infrastrukturen som sådan och tillhandahållandet av tjänsten. Hur stark denna koppling måste vara får avgöras i det enskilda fallet med hänsyn till den kritiska infrastrukturens art och dess betydelse för den samhällsviktiga tjänsten. Övervägandena finns i avsnitt 6.3.

Av *punkt 4* framgår vad som avses med uttrycket motståndskraft. Definitionen motsvarar definitionen i artikel 2.2 i CER-direktivet. Uttrycket förekommer bland annat i 1 § första stycket och 3 kap. 3 § och tar sikte på förmågan att begränsa konsekvenserna av en inträffad incident och att förhindra en potentiell incident. Uttrycket incident definieras i punkt 2. Övervägandena finns i avsnitt 8.2.

Av *punkt 5* framgår vad som avses med uttrycket offentlig verksamhetsutövare när det används i lagen. Av punkt 1 framgår vad som avses med enskild verksamhetsutövare och av 1 § första stycket framgår vad som

avses med kritisk verksamhetsutövare. Vilken betydelse kategoriseringen får och vilken del av verksamhetsutövaren som omfattas av lagen utvecklas i författningskommentaren till punkt 1. I 7 § görs ett undantag från lagens tillämpningsområde för bland annat vissa statliga myndigheter. Övervägandena finns i avsnitt 5.2 och 5.3.

I *punkt 6* definieras uttrycket samhällsviktig tjänst. Definitionen stämmer i stort överens med definitionen i artikel 2.5 i CER-direktivet men med tillägget att den samhällsviktiga tjänsten ska omfattas av bilagan till direktivet. Uttrycket förekommer bland annat i 2 kap. 2 § och 3 kap. 9 §. Med centrala samhällsfunktioner avses grundläggande system och strukturer som gör det möjligt för ett samhälle att fungera, samtidigt som de skyddar till exempel de demokratiska institutionerna. Uttrycket ekonomisk verksamhet omfattar all verksamhet som går ut på att erbjuda varor och tjänster på en marknad. Uttrycket folkhälsa omfattar exempelvis skyddet och främjandet av människors fysiska och psykiska hälsa. Allmän säkerhet avser skydd av institutioner och väsentliga offentliga tjänster och säkrande av invånares överlevnad. Den del av definitionen som avser miljön tar bland annat sikte på verksamhet för att förebygga och avhjälpa miljöskador.

Att den samhällsviktiga tjänsten ska omfattas av bilagan till CER-direktivet innebär att den ska ingå i någon av de sektorer och undersektorer som anges i den första och andra kolumnen i bilagan till CER-direktivet. EU-kommissionen har antagit Kommissionens delegerade förordning (EU) 2023/2450 av den 25 juli 2023 om komplettering av Europaparlamentets och rådets direktiv (EU) 2022/2557 genom upprättande av en förteckning över samhällsviktiga tjänster. Denna förordning ska beaktas vid bedömningen av om tjänsten omfattas av bilagan. Övervägandena finns i avsnitt 6.2.

Undantag från lagens tillämpningsområde

3 § Om det i lag eller annan författning finns bestämmelser som innehåller krav på åtgärder för motståndskraft ska de bestämmelserna gälla om verkan av kraven minst motsvarar verkan av skyldigheterna enligt denna lag med beaktande av bestämmelsernas omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till kraven i bestämmelserna.

Paragrafen utgör ett sådant undantag från lagens tillämpningsområde som medges enligt artikel 1.2 och 1.3 i CER-direktivet. Övervägandena finns i avsnitt 5.4.2.

Skyldigheten att vidta åtgärder för motståndskraft enligt lagen regleras i 3 kap. 3–8 §§. Med lag eller annan författning avses bland annat EU-förordningar och föreskrifter som har meddelats av en myndighet. Vid jämförelsen av verkan ska hänsyn tas till bestämmelsernas omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till kraven i bestämmelserna. Motsvarande bestämmelser kan finnas till exempel kopplat till hamnskydd. Cybersäkerhetslagen (2025:1506) har exempelvis företräde framför den nya lagen i den mån regleringarna överlappar varandra.

4 § För en verksamhetsutövare som har identifierats som kritisk inom någon eller några av sektorerna bankverksamhet, finansmarknadsinfrastruktur eller digital

infrastruktur i bilagan till CER-direktivet gäller inte skyldigheterna enligt denna lag för den delen av verksamheten.

Paragrafen utgör ett sådant undantag från lagens tillämpningsområde som medges enligt artikel 8 i CER-direktivet. Övervägandena finns i avsnitt 5.4.1. Paragrafen utformas efter synpunkter från *Lagrådet*.

Varje medlemsstat ska enligt artikel 6.3 i CER-direktivet upprätta en förteckning över kritiska entiteter, i lagen benämnda kritiska verksamhetsutövare. Medlemsstaterna ska enligt samma artikel informera kritiska entiteter i de sektorer som anges i punkterna 3, 4 och 8 i tabellen i bilagan till direktivet om att de inte har några skyldigheter enligt kapitlen III och IV i direktivet såvida inte nationella åtgärder föreskriver något annat. De sektorer som anges i punkterna är bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur. Medlemsstaterna ska vidare enligt artikel 8 i CER-direktivet säkerställa att artikel 11 och kapitlen III, IV och VI i direktivet inte är tillämpliga på kritiska entiteter inom nyss nämnda sektorer. Dessa sektorer omfattas av krav i andra EU-rättsakter, bland annat Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011.

Paragrafen innebär att skyldigheterna enligt lagen inte gäller för en verksamhetsutövare som enbart har identifierats som kritisk inom någon eller några av sektorerna bankverksamhet, finansmarknadsinfrastruktur eller digital infrastruktur i bilagan till CER-direktivet. Berörd myndighet ska dock, om förutsättningarna enligt 2 kap. 2 § är uppfyllda, ändå identifiera verksamhetsutövaren som kritisk med stöd av 2 kap. 1 §. Detta krävs som en följd av artikel 6.3 i CER-direktivet. Det är alltså möjligt att i lagens mening vara en kritisk verksamhetsutövare utan att omfattas av de skyldigheter som följer av lagen. Identifieringen får inga konsekvenser för verksamhetsutövaren. Om verksamhetsutövaren är identifierad som kritisk även inom en annan sektor än sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur gäller lagen i sin helhet i förhållande till den förstnämnda delen av verksamheten (jfr dock 5 §).

5 § Denna lag gäller inte för en statlig myndighet som till övervägande del bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen (2018:585) eller som till övervägande del bedriver brottsbekämpande verksamhet.

För en enskild verksamhetsutövare som bedriver enbart säkerhetskänslig verksamhet enligt säkerhetsskyddslagen eller som erbjuder tjänster enbart till sådana statliga myndigheter som avses i första stycket gäller inte skyldigheterna enligt denna lag.

För andra kritiska verksamhetsutövare som till någon del bedriver sådan verksamhet eller erbjuder sådana tjänster som avses i första eller andra stycket gäller inte skyldigheterna enligt denna lag för den delen av verksamheten.

Paragrafen utgör ett sådant undantag från lagens tillämpningsområde som medges enligt artikel 1.6 och 1.7 i CER-direktivet. Övervägandena finns i avsnitt 5.4.3.

Av *första stycket* följer att lagen inte gäller för en statlig myndighet som till övervägande del bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen eller som till övervägande del bedriver brotts-

bekämpande verksamhet. Detta innebär att berörd myndighet inte ska identifiera en statlig myndighet som omfattas av undantaget som kritisk verksamhetsutövare enligt 2 kap. 1 §. Med brottsbekämpande verksamhet avses sådan verksamhet som en brottsbekämpande myndighet, till exempel Polismyndigheten men inte domstolarna, bedriver för att förebygga, förhindra eller upptäcka brottslig verksamhet eller för att utreda eller lagföra brott. Med övervägande del avses att myndighetens huvudsakliga verksamhet rör säkerhetskänslig verksamhet eller utgör brottsbekämpning.

Andra stycket innebär att skyldigheterna enligt lagen inte gäller för en enskild verksamhetsutövare som bedriver enbart säkerhetskänslig verksamhet eller som erbjuder tjänster enbart till en sådan statlig myndighet som avses i första stycket. Vilka som räknas som enskilda verksamhetsutövare framgår av 2 § 1. Berörd myndighet ska dock, om förutsättningarna enligt 2 kap. 2 § är uppfyllda, ändå identifiera verksamhetsutövaren som kritisk med stöd av 2 kap. 1 §. Detta krävs som en följd av artikel 6.3 i CER-direktivet (se vidare författningskommentaren till 4 §). Identifieringen får dock inga konsekvenser för verksamhetsutövaren.

Enligt *tredje stycket* gäller skyldigheterna enligt lagen endast i begränsad utsträckning för vissa kritiska verksamhetsutövare. Skyldigheterna gäller inte fullt ut för verksamhetsutövare som till mindre del än till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpande verksamhet. Skyldigheterna gäller inte heller fullt ut för den som till någon del erbjuder tjänster till en sådan statlig myndighet som avses i första stycket. Skyldigheten att vidta åtgärder för motståndskraft enligt till exempel 3 kap. 3 § och genomföra incidentrapportering enligt 3 kap. 9 § gäller inte i förhållande till den säkerhetskänsliga verksamheten, den brottsbekämpande verksamheten eller den del av verksamheten som erbjuder sådana tjänster som anges i bestämmelsen men däremot i förhållande till den övriga delen av verksamheten.

6 § Skyldigheterna att lämna uppgifter enligt denna lag gäller inte uppgifter som är säkerhetsskyddsklassificerade enligt 1 kap. 2 § säkerhetsskyddslagen (2018:585).

Paragrafen utgör ett sådant undantag från lagens tillämpningsområde som medges enligt artikel 1.8 i CER-direktivet. Övervägandena finns i avsnitt 5.4.4.

Paragrafen innebär att en verksamhetsutövare inte är skyldig att till exempel inom ramen för sin rapporteringsskyldighet enligt 3 kap. 9 § lämna ut säkerhetsskyddsklassificerade uppgifter. Med säkerhetsskyddsklassificerade uppgifter avses detsamma som i 1 kap. 2 § säkerhetsskyddslagen och därmed uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) eller som skulle ha omfattats av sekretess enligt den lagen, om den hade varit tillämplig.

7 § Denna lag gäller inte för regeringen, Regeringskansliet, utlandsmyndigheter, kommittéväsendet, myndigheter under riksdagen, domstolar och inte heller för nämnder som utövar rättskipning.

Lagen gäller inte heller för förbundsfullmäktige eller förbundsdirektion i ett kommunalförbund eller för kommunfullmäktige eller regionfullmäktige.

Paragrafen utgör ett sådant undantag från lagens tillämpningsområde som medges enligt artikel 2.10 i CER-direktivet. Övervägandena finns i avsnitt 5.3.

Uttrycket utlandsmyndigheter inbegriper ambassader, karriärkonsulat, representationer och delegationer vid internationella organisationer som EU, FN, OECD och Nato. Med domstolar avses samtliga domstolar, inkluderat särskilda domstolar och specialdomstolar. Mark- och miljödomstolarna hör till de så kallade särskilda domstolarna. Arbetsdomstolen och Försvarsunderrättelsedomstolen är specialdomstolar. Med nämnder som utövar rättskipning avses nämnder som utför rättskipande uppgifter såsom Rättshjälpsnämnden, Notarienämnden och Överklagandenämnden för nämndemannauppdrag.

Uppdrag enligt CER-direktivet

8 § Den myndighet som regeringen bestämmer ska göra en nationell riskbedömning och vara gemensam kontaktpunkt enligt artiklarna 5 och 9 i CER-direktivet.

I paragrafen anges att det är regeringen som utser den myndighet som ska inneha angivna funktioner enligt CER-direktivet. Övervägandena finns i avsnitt 6.1 och 13.1. Paragrafen utformas efter synpunkter från *Lagrådet*.

Bemyndigande

9 § Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om vad som utgör en incident enligt 2 § 2.

Paragrafen innehåller ett bemyndigande. Regeringen eller den myndighet som regeringen bestämmer får, med stöd av paragrafen, meddela ytterligare föreskrifter om vad som räknas som en incident enligt lagen, inklusive vad som utgör en betydande störning. Uttrycket incident förekommer, förutom i 2 § 2, även i 2 § 4, 2 kap. 2 § och 3 kap. 2, 3 och 9 §§. Övervägandena finns i avsnitt 8.3.

2 kap. Identifiering av kritiska verksamhetsutövare

1 § Den eller de myndigheter som regeringen bestämmer ska i enskilda fall besluta om identifiering av kritiska verksamhetsutövare.

Paragrafen genomför delvis artikel 6.1 och 6.5 i CER-direktivet. Övervägandena finns i avsnitt 6.4.

Paragrafen innebär att den eller de myndigheter som regeringen bestämmer ska identifiera kritiska verksamhetsutövare genom beslut i enskilda fall. Vilka krav som ställs för att en verksamhetsutövare ska identifieras som kritisk framgår av 2 §.

2 § För att identifieras som kritisk verksamhetsutövare enligt 1 § krävs att

1. verksamhetsutövaren tillhandahåller en eller flera samhällsviktiga tjänster,

2. verksamhetsutövaren

a) omfattas av någon av kategorierna i bilagan till CER-direktivet, eller

b) är en statlig myndighet som regeringen i övrigt bestämmer ska kunna omfattas av lagen,

3. verksamhetsutövaren bedriver verksamhet i och har kritisk infrastruktur belägen i Sverige, och

4. en incident skulle få en betydande störande effekt för

a) verksamhetsutövarens tillhandahållande av en eller flera samhällsviktiga tjänster, eller

b) tillhandahållandet av andra samhällsviktiga tjänster som är beroende av den eller de samhällsviktiga tjänster som verksamhetsutövaren tillhandahåller.

Paragrafen genomför artikel 6.2 i CER-direktivet. Paragrafen anger de kriterier som ska vara uppfyllda för att en verksamhetsutövare ska identifieras som kritisk enligt 1 §. Övervägandena finns i avsnitt 5.3, 6.2 och 6.3. Paragrafen utformas efter synpunkter från *Lagrådet*.

I *punkt 1* anges att verksamhetsutövaren ska tillhandahålla en eller flera samhällsviktiga tjänster. Vad som avses med uttrycket samhällsviktig tjänst framgår av 1 kap. 2 § 6. Tillhandahålla innebär att något görs tillgängligt för användning eller konsumtion, inklusive led som exempelvis etablering, drift eller kontroll.

Enligt *punkt 2 a* ska verksamhetsutövaren ingå i någon av de kategorier som anges i den tredje kolumnen i bilagan till CER-direktivet. I denna kolumn nämns bland annat kategorin offentliga förvaltningsentiteter. Övervägandena om vilka statliga myndigheter som ingår i kategorin offentliga förvaltningsentiteter finns i avsnitt 5.3.

Punkt 2 b innebär ett undantag från kravet i punkt 2 a. Undantaget innebär att regeringen i förordning kan bestämma att statliga myndigheter ska kunna identifieras som kritiska verksamhetsutövare även om de inte ingår i kategorin offentliga förvaltningsentiteter eller någon annan kategori i den tredje kolumnen i bilagan till CER-direktivet.

I *punkt 3* anges dels ett krav på att verksamhetsutövaren ska bedriva verksamhet i Sverige, dels ett krav på att verksamhetsutövaren ska ha kritisk infrastruktur i Sverige. Vem som kan anses bedriva verksamhet i Sverige får avgöras utifrån omständigheterna i det enskilda fallet. Verksamhetsutövarens etableringsställe saknar dock betydelse vid bedömningen av om kravet är uppfyllt. Det ska finnas en koppling mellan den verksamhet som bedrivs här och tillhandahållandet av den samhällsviktiga tjänsten. Den verksamhet som bedrivs i Sverige behöver dock inte vara avgörande för tillhandahållandet av den samhällsviktiga tjänsten och all verksamhetsutövarens verksamhet behöver inte bedrivas här. Förekomsten av kritisk infrastruktur i Sverige kan i sig tala för att kravet på att bedriva verksamhet i landet är uppfyllt. Ledning för bedömningen av om verksamheten bedrivs i Sverige bör också tas från punkterna 30–32 i Kommissionens riktlinjer och rapporteringsmall som utarbetats i enlighet med artiklarna 5.5, 6.6 och 7.3 i direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft, C/2025/4990. Att den kritiska infrastrukturen ska vara belägen i Sverige innebär att den ska vara belägen inom Sveriges gränser. Vad som avses med uttrycket kritisk infrastruktur framgår av 1 kap. 2 § 3.

Punkt 4 a och b anger som ett sista krav för identifiering som kritisk verksamhetsutövare att en incident skulle få en betydande störande effekt

antingen för verksamhetsutövarens eget tillhandahållande av en eller flera samhällsviktiga tjänster eller för andra verksamhetsutövares tillhandahållande av samhällsviktiga tjänster som är beroende av den förstnämnda verksamhetsutövarens samhällsviktiga tjänst eller tjänster. Innebörden av uttrycken incident och samhällsviktig tjänst framgår av 1 kap. 2 § 2 och 6. Regeringen eller den myndighet som regeringen bestämmer får med stöd av 4 § meddela föreskrifter om vad som utgör en betydande störande effekt.

3 § En myndighet som avses i 1 § ska så snart det kan ske besluta att en verksamhetsutövare som inte längre uppfyller kraven enligt 2 § inte ska omfattas av lagen.

Ett beslut enligt första stycket gäller omedelbart.

Paragrafen genomför delvis artikel 6.5 i CER-direktivet. Övervägandena finns i avsnitt 6.4.

Paragrafen reglerar situationen att en verksamhetsutövare inte längre bedöms vara kritisk, till exempel med anledning av att verksamhetsutövarens verksamhet har utvecklats på visst sätt eller att det i övrigt har tillkommit en omständighet som innebär att förutsättningarna enligt 2 § inte längre är uppfyllda. Berörd myndighet har, efter att den fått kännedom om en sådan tillkommande omständighet till exempel via verksamhetsutövaren, en skyldighet att så snart det kan ske fatta beslut om att verksamhetsutövaren inte längre är att bedöma som kritisk. Att beslut ska fattas så snart det kan ske innebär att beslut ska fattas utan onödigt dröjsmål. Under förutsättning att verksamhetsutövaren inte är identifierad som kritisk av en annan myndighet upphör skyldigheterna enligt lagen att gälla för verksamhetsutövaren omedelbart i samband med beslutet.

4 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om vad som utgör en betydande störande effekt enligt 2 § 4.

Paragrafen innehåller ett bemyndigande. Regeringen eller den myndighet som regeringen bestämmer får, med stöd av paragrafen, meddela föreskrifter om vad som utgör en betydande störande effekt. Övervägandena finns i avsnitt 6.3.

3 kap. Skyldigheter för kritiska verksamhetsutövare

Anmälningsskyldighet

1 § En kritisk verksamhetsutövare som tillhandahåller en samhällsviktig tjänst till eller i minst sex medlemsstater inom Europeiska unionen ska så snart det kan ske anmäla detta till den eller de myndigheter som regeringen bestämmer.

Paragrafen genomför delvis artikel 17.2 i CER-direktivet och innebär en skyldighet för vissa kritiska verksamhetsutövare att göra en anmälan. Övervägandena finns i avsnitt 7.1.

Enligt artikel 17 i CER-direktivet ska kritiska entiteter av särskild europeisk betydelse (härefter kritiska verksamhetsutövare av särskild europeisk betydelse) identifieras. Av artikel 17.2 i direktivet framgår att medlemsstaterna ska säkerställa att en kritisk entitet informerar sin

behöriga myndighet om den tillhandahåller samhällsviktiga tjänster till eller i minst sex medlemsstater. Den anmälningsskyldighet som regleras i paragrafen är en del av genomförandet av artikeln.

Vad som avses med uttrycket tillhandahåller en samhällsviktig tjänst behandlas i författningskommentaren till 1 kap. 2 § 6 och 2 kap. 2 § 1. En anmälan ska göras även om verksamhetsutövaren tillhandahåller olika samhällsviktiga tjänster i de olika medlemsstaterna och oavsett om verksamhetsutövaren har identifierats som kritisk i de andra medlemsstaterna.

Att en anmälan ska göras så snart det kan ske innebär att en anmälan ska göras i omedelbar anslutning till att verksamhetsutövaren identifieras som kritisk enligt 2 kap. 1 §, om det rör sig om en verksamhetsutövare som redan vid den tidpunkten tillhandahåller en samhällsviktig tjänst till eller i minst sex medlemsstater. Om en verksamhetsutövare utvecklar sin verksamhet på ett sätt som gör att denne omfattas av anmälningsskyldigheten ska en anmälan göras i samband med att verksamhetsutövaren börjar att tillhandahålla en samhällsviktig tjänst i eller till minst sex medlemsstater.

En verksamhetsutövare som inte uppfyller sin skyldighet att göra en anmälan ska bli föremål för ingripande enligt 5 kap. Det kommer i det enskilda fallet att vara tillsynsmyndigheten eller ytterst en domstol som avgör om en anmälan har gjorts i rätt tid.

Regeringen, eller den myndighet som regeringen bestämmer, har möjlighet att meddela verkställighetsföreskrifter med stöd av 8 kap. 7 § regeringsformen som kan bland annat reglera anmälans innehåll.

Riskbedömning

2 § En kritisk verksamhetsutövare ska göra en riskbedömning.

Riskbedömningen ska dokumenteras och innehålla en redogörelse för alla relevanta risker för en incident.

Riskbedömningen ska uppdateras vid behov och minst vart fjärde år.

Paragrafen genomför delvis artikel 12 i CER-direktivet och behandlar verksamhetsutövarens skyldighet att göra en riskbedömning som ska uppdateras. Övervägandena finns i avsnitt 8.1. Paragrafen utformas delvis enligt *Lagrådets* förslag.

Enligt paragrafen ska riskbedömningen dokumenteras och paragrafen reglerar även riskbedömningens innehåll. Innebörden av att riskbedömningen ska innehålla en redogörelse för alla relevanta risker för en incident är att riskbedömningen ska utgå från ett allriskperspektiv. Detta allriskperspektiv innebär att såväl omvärldsfaktorer som den kritiska verksamhetsutövarens individuella och sektorsspecifika förutsättningar ska beaktas vid bedömningen. Med incident avses, enligt 1 kap. 2 § 2, en händelse som kan medföra en betydande störning eller som medför en störning i den kritiska verksamhetsutövarens tillhandahållande av en samhällsviktig tjänst. Kravet på att det ska röra sig om relevanta risker innebär att riskbedömningen inte behöver innehålla en redogörelse för risker som inte kan få en sådan effekt som nämns i 1 kap. 2 § 2. Regeringen eller den myndighet som regeringen bestämmer får enligt 12 § meddela ytterligare föreskrifter om riskbedömningen.

Tidpunkten för när en kritisk verksamhetsutövare senast ska ha genomfört sin riskbedömning regleras i 10 §. En uppdatering av riskbedömningen ska ske minst vart fjärde år. Bedömningen av behovet av en uppdatering dessförinnan ska göras med hänsyn till den kritiska verksamhetsutövarens specifika omständigheter och utvecklingen av riskerna och ska därvid bland annat utgå från dels den aktuella verksamheten och hur denna utvecklas, dels hur riskerna som sådana utvecklas. En kritisk verksamhetsutövare som inte uppfyller sina skyldigheter i dessa avseenden ska bli föremål för ingripande enligt 5 kap. Det är tillsynsmyndigheten eller ytterst en domstol som bedömer om det har funnits behov av att uppdatera riskbedömningen innan fyra år har gått.

Åtgärder för motståndskraft

3 § En kritisk verksamhetsutövare ska vidta lämpliga och proportionella tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa sin motståndskraft (åtgärder för motståndskraft). Åtgärderna för motståndskraft ska vidtas på grundval av verksamhetsutövarens riskbedömning och annan relevant information samt inkludera åtgärder som är nödvändiga för att

1. förhindra att incidenter inträffar,
2. säkerställa ett tillfredsställande fysiskt skydd av lokaler och kritisk infrastruktur,
3. reagera på, stå emot och begränsa konsekvenserna av incidenter,
4. återhämta sig från incidenter,
5. säkerställa en ändamålsenlig hantering av personalsäkerhet, inbegripet åtgärder enligt 4–7 §§, och
6. öka kunskapen och medvetenheten om åtgärderna för motståndskraft hos berörd personal.

Verksamhetsutövaren ska upprätta och följa en plan för motståndskraft som beskriver de åtgärder som har vidtagits eller ska vidtas enligt första stycket.

Paragrafen genomför delvis artikel 13.1 och 13.2 i CER-direktivet. Paragrafen anger vilka åtgärder som en kritisk verksamhetsutövare är skyldig att vidta för att säkerställa sin motståndskraft. Uttrycket motståndskraft definieras i 1 kap. 2 § 4. När skyldigheten att vidta åtgärder för motståndskraft inträder regleras i 10 §. Övervägandena finns i avsnitt 8.2 och 9.1–9.4.

Av *första stycket* följer krav på att verksamhetsutövaren ska vidta lämpliga och proportionella tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa sin motståndskraft. Sådana åtgärder benämns åtgärder för motståndskraft. Det kan till exempel röra sig om åtgärder till skydd mot oönskad förändring av, obehörig insyn i eller obehörig åtkomst till system eller annan infrastruktur. Det kan vidare röra sig om åtgärder till skydd mot obehöriga personer samt till skydd för lokaler och utrustning av betydelse för säkerheten. Det kan också bland annat handla om att verksamhetsutövaren fördelar ansvar, roller och mandat i organisationen samt utarbetar rutiner och genomför uppföljning och utvärdering.

Kravet på lämplighet innebär att åtgärderna ska vara relevanta och effektiva i förhållande till de identifierade riskerna. Vid bedömningen av om åtgärderna är proportionella ska hänsyn exempelvis tas till verksamhetsutövarens grad av riskexponering och storlek samt till

sannolikheten för att incidenter inträffar och till eventuella incidenters allvarlighetsgrad, inbegripet deras samhälleliga och ekonomiska konsekvenser. En åtgärd kan exempelvis vara proportionell men mindre lämplig än någon annan åtgärd i förhållande till en viss risk.

Åtgärderna för motståndskraft ska bland annat utgå från den riskbedömning som den kritiska verksamhetsutövaren är skyldig att genomföra enligt 2 §. Verksamhetsutövaren ska vidta de åtgärder som, med beaktande av kravet på lämplighet och proportionalitet, är nödvändiga för att uppnå de syften som anges i punkt 1–6. Uttrycket nödvändiga för ska inte tolkas som att en verksamhetsutövare har en skyldighet att se till att det till exempel aldrig inträffar en incident i verksamheten. En verksamhetsutövare som inte uppfyller sin skyldighet enligt paragrafen ska bli föremål för ingripande enligt 5 kap.

Huruvida en verksamhetsutövare har vidtagit tillräckliga åtgärder för motståndskraft får bedömas i varje enskilt fall och blir en fråga för tillsynsmyndigheten och ytterst en domstol.

Av *punkt 1* framgår att verksamhetsutövaren ska vidta de åtgärder för motståndskraft som är nödvändiga för att förhindra att incidenter inträffar. Vad som avses med uttrycket incident framgår av 1 kap. 2 § 2. Skyldigheten handlar om att vidta åtgärder för att minska risken för att det inträffar en händelse som kan medföra en betydande störning, eller som medför en störning, i verksamhetsutövarens tillhandahållande av en samhällsviktig tjänst. Verksamhetsutövaren ska, i enlighet med artikel 13.1 a i CER-direktivet, inom ramen för skyldigheten bland annat vidta åtgärder för katastrofriskreducering och klimatanpassning.

Av *punkt 2* följer ett krav på att den kritiska verksamhetsutövaren ska vidta åtgärder som är nödvändiga för att säkerställa ett tillfredsställande fysiskt skydd av lokaler och kritisk infrastruktur. Vad som avses med uttrycket kritisk infrastruktur framgår av 1 kap. 2 § 3. Kravet kan innebära att verksamhetsutövaren ska sätta upp stängsel och andra slags fysiska barriärer, ha metoder och rutiner för övervakning av vissa områden samt använda sig av detektionsutrustning och olika slags åtkomstkontroller, till exempel i form av användarautentisering och behörighetsstyrning.

Skyldigheten enligt *punkt 3* att vidta åtgärder som är nödvändiga för att reagera på, stå emot och begränsa konsekvenserna av incidenter innebär bland annat att verksamhetsutövaren ska ha en förmåga att genomföra risk- och krishanteringsförfaranden på ett ändamålsenligt sätt samt ha goda rutiner för att hantera incidenter.

Punkt 4 innebär ett krav på att vidta åtgärder som är nödvändiga för att den kritiska verksamhetsutövaren ska kunna återhämta sig från incidenter. Detta innebär exempelvis att verksamhetsutövaren ska vidta åtgärder för kontinuitetshantering, det vill säga att planera för och ha förmåga att upprätthålla verksamheten på en acceptabel nivå oavsett vilken störning verksamheten utsätts för eller om en kris inträffar. Verksamhetsutövaren kan inom ramen för denna skyldighet bland annat behöva identifiera alternativa försörjningskedjor som krävs för att kunna återuppta tillhandahållandet av en samhällsviktig tjänst.

Punkt 5 innebär en skyldighet att vidta nödvändiga åtgärder för att säkerställa en ändamålsenlig hantering av personalsäkerhet, inbegripet att vidta åtgärder i enlighet med de skyldigheter som regleras i 4–7 §§. Skyldigheten enligt bestämmelsen tar bland annat sikte på att fastställa

åtkomstkontroll till lokaler, kritisk infrastruktur och känslig information. Verksamhetsutövaren ska också införa ändamålsenliga krav på utbildning och kvalifikationer för deltagande i verksamheten.

Enligt *punkt 6* ska kritiska verksamhetsutövare vidta nödvändiga åtgärder för att öka kunskapen och medvetenheten om åtgärderna för motståndskraft hos berörd personal. Denna skyldighet kan handla om att se till att personalen genomgår utbildning och tar del av informationsmaterial men också om att genomföra eller delta i övningar som ökar kunskapen och medvetenheten om relevanta hot och risker samt åtgärder för att möta dessa. Det kan handla om att verksamhetsutövaren själv anordnar utbildningar och övningar och tar fram informationsmaterial men det kan också handla om att personalen tar del av sådant som anordnas eller tillhandahålls av en extern aktör, till exempel en myndighet.

Enligt *andra stycket* ska verksamhetsutövaren upprätta och följa en plan för motståndskraft som beskriver de åtgärder som har vidtagits eller ska vidtas enligt första stycket.

Regeringen eller den myndighet som regeringen bestämmer får enligt 12 § meddela ytterligare föreskrifter om åtgärderna som ska vidtas enligt paragrafen.

4 § En kritisk verksamhetsutövare ska göra en analys av vilka befattningar som ska omfattas av krav på bakgrundskontroll enligt 5 § (befattningsanalys).

Befattningsanalysen ska dokumenteras och innehålla uppgifter om sådana befattningar där deltagandet i verksamheten innebär möjlighet att orsaka mer än ringa störning i den kritiska verksamhetsutövarens tillhandahållande av en eller flera samhällsviktiga tjänster.

Befattningsanalysen ska uppdateras vid behov och minst en gång om året.

Paragrafen genomför delvis artiklarna 13.1, 14.1 och 14.2 i CER-direktivet och behandlar skyldigheten för kritiska verksamhetsutövare att göra en befattningsanalys som ska dokumenteras och uppdateras. Övervägandena finns i avsnitt 9.2.

Av paragrafen framgår att befattningsanalysen ska dokumenteras och innehålla uppgifter om de befattningar där deltagandet i verksamheten innebär möjlighet att orsaka mer än ringa störning i den kritiska verksamhetsutövarens tillhandahållande av en eller flera samhällsviktiga tjänster. Befattningsanalysen ska innehålla en beskrivning av sådana befattningar som innebär möjlighet att orsaka angiven slags störning. Med befattning avses i detta sammanhang en funktion eller en tjänst som innehas av en anställd eller någon annan person som deltar i verksamheten på annan grund, till exempel inom ramen för ett tillfälligt uppdrag. Med ringa störning avses en mycket begränsad störning. Bedömningen av om deltagandet kan orsaka mer än ringa störning ska göras utifrån den enskilda verksamheten och vilket deltagande som det är fråga om med beaktande av tillträdes- och åtkomsträttigheter till lokaler, anläggningar och annan kritisk infrastruktur. Av 12 § följer att regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om bland annat befattningsanalysen. Sådana föreskrifter kan bland annat avse hur man ska bedöma risken för störning.

Befattningsanalysen ska uppdateras minst en gång om året men också tidigare vid behov. Det kan exempelvis finnas behov av en tidigare

uppdatering om tillhandahållandet av den samhällsviktiga tjänsten förändras, vid organisatoriska förändringar eller om it-system byts ut med förändrade processer eller behörigheter som följd. En verksamhetsutövare som inte uppfyller sin skyldighet att dokumentera och uppdatera en befattningsanalys ska bli föremål för ingripande enligt 5 kap.

5 § En kritisk verksamhetsutövare ska säkerställa att en person som deltar i eller ska delta i verksamheten, i den mån det följer av verksamhetsutövarens befattningsanalys, har genomgått en bakgrundskontroll.

En bakgrundskontroll innebär att den person som kontrollen avser ska

1. styrka sin identitet, och
2. genomgå en registerkontroll enligt 6 §.

En förnyad bakgrundskontroll ska göras när det finns skäl för det, och senast två år efter den senaste kontrollen.

Paragrafen genomför delvis artikel 14.1–14.3 i CER-direktivet. Paragrafen innebär en skyldighet för den kritiska verksamhetsutövaren att säkerställa att viss personal och vissa andra som på annat sätt deltar i verksamheten har genomgått bakgrundskontroller. Paragrafen reglerar även bakgrundskontrollens innehåll och när förnyade bakgrundskontroller ska ske. En verksamhetsutövare som inte uppfyller sin skyldighet att genomföra en bakgrundskontroll respektive en förnyad bakgrundskontroll ska bli föremål för ingripande enligt 5 kap. Övervägandena finns i avsnitt 9.1 och 9.3.

I *första stycket* anges en skyldighet för verksamhetsutövaren att säkerställa att en person som deltar i eller ska delta i verksamheten som bedrivs av verksamhetsutövaren, i den mån det följer av verksamhetsutövarens befattningsanalys som regleras i 4 §, har genomgått en bakgrundskontroll. Syftet med en bakgrundskontroll är att utvärdera om den person som kontrollen avser kan utgöra en potentiell säkerhetsrisk för den berörda verksamhetsutövaren. Det finns olika säkerhetsrisker som kan behöva utvärderas. Den kritiska verksamhetsutövaren kan exempelvis behöva bedöma om det finns en risk för att personen kan missbruka sina åtkomsträttigheter för skadliga ändamål eller om det finns en risk för att personen kan hamna i en intressekonflikt eller bli utsatt för olika påtryckningar på ett sätt som kan skada verksamheten.

En bedömning av om det föreligger potentiella säkerhetsrisker kopplat till en enskild person förutsätter en helhetsbedömning av den information som verksamhetsutövaren har tillgänglig. Det handlar om uppgifter som verksamhetsutövaren naturligt får del av inom ramen för en rekryteringsprocess respektive under pågående anställning eller annat deltagande i verksamheten. Bakgrundskontroller ska enbart avse personer som deltar i eller som erbjuds att delta i verksamhet med krav på bakgrundskontroll enligt verksamhetsutövarens befattningsanalys.

I *andra stycket* anges vad en bakgrundskontroll ska omfatta för åtgärder.

Punkt 1 innebär att den person som är föremål för bakgrundskontrollen ska styrka sin identitet. Av 12 § följer att regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om bland annat bakgrundskontroller. Sådana föreskrifter kan reglera bland annat hur kontrollerna ska ske och vilka identitetshandlingar som ska godtas.

Punkt 2 innebär att den person som är föremål för bakgrundskontrollen ska genomgå en registerkontroll enligt 6 §. Eftersom bakgrundskontroller ska avse enbart personer som deltar i eller som erbjuds att delta i verksamheten bör registerkontrollen utgöra det sista ledet i ett rekryteringsförfarande. Vid ett rekryteringsförfarande ges den enskilde en valmöjlighet; att visa upp ett utdrag ur belastningsregistret eller att återkalla sin ansökan. Om den enskilde väljer att inte visa upp ett utdrag ur belastningsregistret kan verksamhetsutövaren inte anställa personen i fråga eftersom en bakgrundskontroll enligt lagen inte har kunnat genomföras. Om en anställd, trots begäran enligt 6 §, inte visar upp ett utdrag ur belastningsregistret förhindras verksamhetsutövaren också att uppfylla sin skyldighet att genomföra en bakgrundskontroll. Under förutsättning att verksamhetsutövarens bedömning att inkludera befattningen i sin befattningsanalys är korrekt, uppfyller inte verksamhetsutövaren kraven i lagen om arbetstagaren är kvar i sin befattning. Verksamhetsutövaren behöver då vidta åtgärder, vilket kan inbegripa arbetsrättsliga åtgärder. Vid en identifierad risk, till exempel med anledning av förekomst i belastningsregistret, behöver den kritiska verksamhetsutövaren bedöma om det behöver vidtas några ytterligare åtgärder för motståndskraft enligt 3 §.

I *tredje stycket* anges att en ny bakgrundskontroll ska göras när det finns skäl för det, och annars senast två år efter den senaste bakgrundskontrollen. Bestämmelsen ger en möjlighet att genomföra en förnyad bakgrundskontroll tidigare än två år efter det att den senaste bakgrundskontrollen genomfördes om verksamhetsutövaren efter en bedömning i det enskilda fallet anser att det föreligger skäl för det. Det kan exempelvis röra sig om att det finns indikationer på att personen inte på ett korrekt sätt förhåller sig till regler och överenskommelser i fråga om till exempel åtkomstbegränsningar eller tillträde till fysiska lokaler eller it-system, eller att personen har varit frånvarande från arbetet under en längre tid under omständigheter som ger anledning att ifrågasätta skälen för frånvaron.

6 § En person som avses i 5 § ska på begäran av den kritiska verksamhetsutövaren visa upp ett utdrag ur det register som förs enligt lagen (1998:620) om belastningsregister.

Utdraget får inte vara äldre än sex månader.

Paragrafen genomför delvis artikel 14.3 i CER-direktivet och anger registerkontrollens innehåll och omfattning. Överväganden finns i avsnitt 9.3. Paragrafen utformas delvis enligt *Lagrådets* förslag.

Av *första stycket* följer att den person som registerkontrollen avser ska visa upp ett utdrag ur belastningsregistret på begäran av den kritiska verksamhetsutövaren. Vad som kan bli konsekvenserna av att personen inte uppvisar ett utdrag behandlas i författningskommentaren till 5 §.

Enligt *andra stycket* får utdraget inte vara äldre än sex månader när det visas upp.

7 § Vid en bakgrundskontroll ska den kritiska verksamhetsutövaren anteckna om den person som kontrollen avser har styrkt sin identitet och visat upp ett sådant utdrag som avses i 6 §. Någon annan dokumentation av kontrollen får inte göras.

Anteckningar enligt första stycket ska bevaras i två år från den dag då bakgrundskontrollen avslutades.

Paragrafen innehåller krav på dokumentation vid bakgrundskontroller och reglerar bevarande av sådan dokumentation. Överväganden finns i avsnitt 9.4.

Första stycket innebär en skyldighet för den kritiska verksamhetsutövaren att föra anteckning om att den person som kontrollen avser har styrkt sin identitet och om att ett utdrag ur belastningsregistret har visats upp. Anteckningar ska inte göras avseende innehållet i det som visas upp, utan ska avse endast att uppvisande har skett.

Enligt *andra stycket* ska anteckningarna bevaras i två år från den dag då bakgrundskontrollen avslutades.

8 § En kritisk verksamhetsutövare ska utse en kontaktpunkt för tillsynsmyndigheten.

Paragrafen genomför artikel 13.3 i CER-direktivet. Övervägandena finns i avsnitt 8.2.

Paragrafen innebär att en kritisk verksamhetsutövare ska utse en kontaktpunkt för tillsynsmyndigheten. En kritisk verksamhetsutövare kan välja mellan att peka ut en specifik individ eller en funktion för att fullgöra uppgiften. Av 12 § följer att regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om bland annat kontaktpunkten.

Incidentrapportering

9 § En kritisk verksamhetsutövare ska till den myndighet som regeringen bestämmer anmäla sådana incidenter som medför eller kan medföra en betydande störning i den kritiska verksamhetsutövarens tillhandahållande av en samhällsviktig tjänst.

En incidentanmälan enligt första stycket ska lämnas så snart det kan ske, dock senast 24 timmar efter det att verksamhetsutövaren har fått kännedom om incidenten. Senast en månad efter incidentanmälan ska verksamhetsutövaren lämna en rapport om incidenten till samma myndighet.

Paragrafen genomför delvis artikel 15.1 i CER-direktivet och reglerar kritiska verksamhetsutövares skyldighet att rapportera vissa incidenter. En verksamhetsutövare som inte uppfyller sin skyldighet att genomföra incidentrapporteringen ska bli föremål för ingripande enligt 5 kap. Övervägandena finns i avsnitt 8.3.

Med incident avses, enligt 1 kap. 2 § 2, både en händelse som kan medföra en betydande störning och en händelse som medför en störning i den kritiska verksamhetsutövarens tillhandahållande av en samhällsviktig tjänst. Uttrycket incident omfattar alltså även händelser som medför en störning. Rapporteringsskyldigheten gäller dock endast sådana incidenter som medför eller kan medföra en betydande störning och därmed omfattas inte alla incidenter av rapporteringsskyldigheten. Alla incidenter som, vid en inledande bedömning av bland annat incidentens art, orsak och omfattning samt av verksamhetsutövarens förutsättningar att exempelvis reagera på och begränsa konsekvenserna av incidenten, bedöms medföra

eller kunna medföra en betydande störning omfattas av rapporteringsskyldigheten. Även en händelse som typiskt sett hade kunnat orsaka en betydande störning om den inte hade avvärjts omfattas av rapporteringsskyldigheten. I 12 § anges att regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om incidentrapporteringen.

Rapporteringen ska genomföras i två steg. En incidentanmälan ska först lämnas så snart det kan ske och senast inom 24 timmar efter det att verksamhetsutövaren har fått kännedom om incidenten. Tidsangivelsen om 24 timmar är alltså att betrakta som en bortre tidsgräns. Uttrycket så snart det kan ske innebär att rapportering ska göras i omedelbar anslutning till att verksamhetsutövaren har fått kännedom om incidenten. Senast en månad efter incidentanmälan ska verksamhetsutövaren även lämna en rapport om incidenten till samma myndighet.

Skyldigheten att rapportera incidenter innebär inget krav på att lämna uppgifter som är säkerhetsskyddsklassificerade. Detta följer av 1 kap. 6 §.

När skyldigheterna inträder

10 § En kritisk verksamhetsutövares skyldigheter enligt 2 § börjar gälla nio månader efter det att denne har fått del av ett sådant beslut som avses i 2 kap. 1 §. Skyldigheterna enligt 3–9 §§ börjar gälla tio månader efter det att verksamhetsutövaren har fått del av beslutet.

Paragrafen genomför delvis artiklarna 6.3 och 12 i CER-direktivet. Övervägandena finns i avsnitt 6.4 och 8.1. Paragrafen utformas efter synpunkter från *Lagrådet*.

Paragrafen reglerar när skyldigheterna enligt 2–9 §§ uppstår. Innebörden av skyldigheterna behandlas i författningskommentaren till paragraferna som omfattas av uppräkningen. Skyldigheterna börjar gälla angiven tid efter att verksamhetsutövaren har fått del av ett beslut om att denne har identifierats som kritisk verksamhetsutövare. Uttrycket har fått del av ska tolkas i ljuset av hur det används i till exempel 44 § förvaltningslagen (2017:900). Det finns därmed inget krav på att ett beslut enligt 2 kap. 1 § ska delges verksamhetsutövaren men tillsynsmyndigheten ska se till att verksamhetsutövaren har fått reda på innehållet i beslutet.

Bakgrundskontroller inför deltagande i samverkan enligt CER-direktivet

11 § Regeringen eller den myndighet som regeringen bestämmer får genomföra bakgrundskontroller enligt 5 § av personer som föreslås delta i ett rådgivande uppdrag eller företräda Sverige i gruppen för kritiska entiteters motståndskraft enligt artiklarna 18 och 19 i CER-direktivet.

Paragrafen genomför delvis artikel 18.5 samt artikel 19.2 i CER-direktivet. Övervägandena finns i avsnitt 9.5. Paragrafen utformas efter synpunkter från *Lagrådet*.

Bemyndigande

12 § Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om riskbedömning enligt 2 §, åtgärder för motståndskraft enligt 3–8 §§ och incidentrapportering enligt 9 §.

Paragrafen innehåller bemyndiganden som ger regeringen eller den myndighet som regeringen bestämmer möjlighet att meddela vissa föreskrifter. Övervägandena finns i avsnitt 8.1–8.3 och 9.1.

Regeringen eller den myndighet som regeringen bestämmer får, med stöd av paragrafen, meddela ytterligare föreskrifter om den riskbedömning som en kritisk verksamhetsutövare är skyldig att göra enligt 2 §, om vilka åtgärder som ska vidtas för att verksamhetsutövaren ska anses uppfylla lagens krav på att vidta åtgärder för motståndskraft enligt 3–8 §§ och om den incidentrapportering som ska genomföras enligt 9 §.

4 kap. Tillsyn

Tillsynsmyndigheten och tillsynsmyndighetens uppdrag

1 § Den eller de myndigheter som regeringen bestämmer ska vara tillsynsmyndighet.

Paragrafen genomför delvis artikel 9.1 i CER-direktivet. I paragrafen finns en upplysning om att regeringen bestämmer vilken eller vilka myndigheter som ska vara tillsynsmyndighet. Övervägandena finns i avsnitt 10.1.

2 § En tillsynsmyndighet ska

1. utöva tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs,
2. utöva tillsyn över att sådana rättsakter följs som har antagits med stöd av artikel 13.6 i CER-direktivet, och
3. inom ramen för sin tillsyn medverka till att rådgivande uppdrag genomförs i enlighet med artikel 18 i CER-direktivet.

Paragrafen genomför delvis artiklarna 9.1 och 18 i CER-direktivet. I paragrafen regleras vad som är en tillsynsmyndighets uppgift. Övervägandena finns i avsnitt 7.2 och 10.1. Paragrafen utformas efter synpunkter från *Lagrådet*.

Av *punkt 1* framgår att tillsynsmyndigheten ska utöva tillsyn över att lagen och föreskrifter som har meddelats i anslutning till lagen följs.

Av *punkt 2* framgår att tillsynsansvaret även omfattar sådana genomförandeakter som EU-kommissionen antar med stöd av artikel 13.6 i CER-direktivet.

Punkt 3 innebär att tillsynsmyndigheten inom ramen för sin tillsyn ska medverka till att rådgivande uppdrag genomförs i enlighet med artikel 18 i CER-direktivet för att bedöma de åtgärder som en kritisk verksamhetsutövare av särskild europeisk betydelse har vidtagit för att uppfylla vissa skyldigheter (se 3 kap. 2–9 §§). Medlemsstaterna ska enligt artikel 18.7 i direktivet säkerställa att kritiska verksamhetsutövare av särskild europeisk betydelse ger åtkomst till uppgifter, system och anläggningar som rör tillhandahållandet av deras samhällsviktiga tjänster och som är nödvändiga för genomförandet av det rådgivande uppdraget. Tillsyns-

myndigheten kan inom ramen för denna del av sitt uppdrag, och med stöd av 3–6 §§, bland annat inhämta sådana uppgifter och få åtkomst till sådana system och anläggningar som avses i artikel 18.7 i CER-direktivet.

Tillsynsmyndighetens befogenheter

3 § Den som står under tillsyn ska på begäran tillhandahålla en tillsynsmyndighet de uppgifter eller handlingar som behövs för tillsynen.

Paragrafen genomför delvis artikel 21.1 samt artikel 21.2 i CER-direktivet. Paragrafen innebär en skyldighet för verksamhetsutövaren att, på begäran av en tillsynsmyndighet, tillhandahålla tillsynsmyndigheten de uppgifter eller handlingar som myndigheten behöver för att utföra sina uppgifter enligt lagen. Övervägandena finns i avsnitt 10.2.

Tillsynsmyndigheten avgör vilka uppgifter eller handlingar som behövs i det enskilda fallet med beaktande av bland annat det krav på proportionalitet som följer av 5 § tredje stycket förvaltningslagen. Om verksamhetsutövaren inte medverkar, kan tillsynsmyndigheten förelägga verksamhetsutövaren enligt 5 § och i sista hand begära handräckning av Kronofogdemyndigheten enligt 6 §.

4 § En tillsynsmyndighet har i den omfattning det behövs för tillsynen rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamhet som omfattas av tillsynen.

Paragrafen, som genomför delvis artikel 21.1 och 21.4 i CER-direktivet, reglerar en tillsynsmyndighets rätt att få tillträde till områden, lokaler och andra utrymmen i den utsträckning det behövs för att den ska kunna utöva tillsyn. Rätten omfattar inte bostäder. Övervägandena finns i avsnitt 10.2.

Tillträdesrätten motsvaras av en skyldighet för verksamhetsutövaren att ge begärt tillträde. Att det intrång som tillträdet innebär måste stå i proportion till behovet av åtgärden följer av 5 § tredje stycket förvaltningslagen. Tillträdesrätten ger inte myndigheten rätt att bereda sig tillträde med tvång. Om verksamhetsutövaren inte medverkar, kan tillsynsmyndigheten enligt 5 § förelägga verksamhetsutövaren att ge tillträde och i sista hand begära handräckning av Kronofogdemyndigheten enligt 6 §.

5 § En tillsynsmyndighet får besluta att förelägga den som står under tillsyn att tillhandahålla uppgifter eller handlingar eller ge tillträde enligt 3 och 4 §§.

Ett föreläggande får förenas med vite. Ett vitesföreläggande får även riktas mot staten.

Paragrafen, som genomför delvis artikel 21.1–21.3 i CER-direktivet, reglerar tillsynsmyndighetens möjlighet att fatta beslut om att förelägga den som står under tillsyn att tillhandahålla uppgifter eller handlingar enligt 3 § och ge tillträde enligt 4 §. Övervägandena finns i avsnitt 10.2.

Som utgångspunkt ska tillsynsmyndigheten i första hand försöka förmå verksamhetsutövaren att agera på frivillig väg. Det följer av 5 § tredje stycket förvaltningslagen att beslut om förelägganden får fattas endast om det är proportionerligt. Myndigheten ska göra en proportionalitetsbedömning i varje enskilt fall. Ett föreläggande får förenas med vite. Lagen (1985:206) om viten är då tillämplig.

6 § En tillsynsmyndighet får begära handräckning av Kronofogdemyndigheten för de tillsynsåtgärder som avses i 3 och 4 §§. Vid handräckning gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande.

Paragrafen, som genomför delvis artikel 21.1 och 21.2 i CER-direktivet, reglerar tillsynsmyndighetens möjlighet att begära handräckning av Kronofogdemyndigheten. Övervägandena finns i avsnitt 10.2.

Tillsynsmyndigheten får begära handräckning av Kronofogdemyndigheten för att få tillgång till uppgifter eller handlingar enligt 3 § eller för att få tillträde till sådana lokaler och andra utrymmen som anges i 4 §. Vid sådan handräckning gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande.

5 kap. Ingripanden

När och hur tillsynsmyndigheten ska ingripa

1 § En tillsynsmyndighet ska ingripa om en kritisk verksamhetsutövare har åsidosatt sina skyldigheter enligt 3 kap. 1–9 §§ eller enligt föreskrifter som har meddelats i anslutning till de paragraferna eller enligt sådana rättsakter som har antagits med stöd av artikel 13.6 i CER-direktivet.

Ett ingripande sker genom ett beslut om föreläggande enligt 2 §, ett beslut om sanktionsavgift enligt 3 § eller, om det inte finns skäl att ingripa mot en överträdelse på något annat sätt, genom att besluta om anmärkning.

Tillsynsmyndigheten får avstå från ett ingripande om överträdelsen är ringa eller ursäktlig, eller om det annars med hänsyn till omständigheterna vore oskäligt att ingripa.

Paragrafen genomför delvis artiklarna 21.3, 21.4 och 22 i CER-direktivet. Paragrafen reglerar när och hur tillsynsmyndigheten ska ingripa vid vissa överträdelser. Övervägandena finns i avsnitt 11.1–11.3. Paragrafen utformas efter synpunkter från *Lagrådet*.

Vad de skyldigheter som räknas upp i *första stycket* innebär behandlas i författningskommentaren till angivna paragrafer. Det är obligatoriskt för tillsynsmyndigheten att ingripa om verksamhetsutövaren har åsidosatt någon av skyldigheterna, om det inte finns skäl att avstå från ingripande enligt paragrafens tredje stycke.

I *andra stycket* anges på vilka sätt ingripande kan ske. Om en tillsynsmyndighet inte finner skäl att ingripa på något annat sätt, ska den besluta om en anmärkning. En tillsynsmyndighet kan ingripa på flera sätt mot samma överträdelse. Tillsynsmyndigheten kan välja att besluta om sanktionsavgift, även om den dessförinnan har ingripit genom att besluta om ett föreläggande. Anmärkning ska dock meddelas endast om ingen annan ingripandeåtgärd vidtas. En sanktionsavgift får enligt 6 § inte beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

Tillsynsmyndigheten får enligt *tredje stycket* avstå från ett ingripande om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna vore oskäligt att ingripa. Ringa överträdelser tar sikte på överträdelser som är mindre allvarliga, till exempel då det rör sig om

en överträdelse som inte har fått några uppenbara negativa konsekvenser. Att en överträdelse är ursäktlig innebär att den är föranledd av ett beteende som av särskilda omständigheter är att betrakta som mindre klandervärt än annars. Så kan till exempel vara fallet om verksamhetsutövaren har gjort det som rimligen kan krävas för att förhindra en överträdelse. Bestämmelsen ger också utrymme för att beakta om det på annat sätt skulle vara oskäligt med ett ingripande. En tillsynsmyndighet bör till exempel kunna avstå från ett ingripande om verksamhetsutövaren drabbas av flera sanktionsavgifter vid samma prövningstillfälle för olika slags överträdelser och den samlade reaktionen skulle bli oproportionerlig. Tillsynsmyndigheten kan också till exempel avstå från att ingripa om det skulle riskera att bryta mot dubbelbestraffningsförbudet.

Förelägganden

2 § En tillsynsmyndighet får besluta de förelägganden som behövs för att en kritisk verksamhetsutövare ska uppfylla skyldigheterna som avses i 1 § första stycket.

Ett föreläggande får förenas med vite. Ett vitesföreläggande får även riktas mot staten.

Paragrafen genomför delvis artikel 21.3 i CER-direktivet. Övervägandena finns i avsnitt 11.4.

Paragrafen innebär en rätt för tillsynsmyndigheten att besluta de förelägganden som behövs för att få en verksamhetsutövare att fullgöra angivna skyldigheter. Sådana förelägganden får förenas med vite. Lagen om viten är då tillämplig.

Sanktionsavgift

3 § En tillsynsmyndighet får besluta att ta ut en sanktionsavgift av en kritisk verksamhetsutövare till följd av en överträdelse av de skyldigheter som avses i 1 § första stycket.

Paragrafen genomför delvis artikel 22 i CER-direktivet. Övervägandena finns i avsnitt 11.5.1.

Det är inte obligatoriskt att ta ut en sanktionsavgift när en överträdelse har konstaterats, utan tillsynsmyndigheten avgör om en avgift ska tas ut i det enskilda fallet. En avgift kan tas ut även om överträdelsen varken har varit uppsåtlig eller berott på oaktsamhet. Av 7 § framgår att en sanktionsavgift får beslutas endast om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

4 § Sanktionsavgiften ska bestämmas till lägst 5 000 kronor och till högst

1. det högsta av 2 procent av en enskild verksamhetsutövares totala globala årsomsättning under närmast föregående räkenskapsår, och ett belopp i kronor motsvarande 10 000 000 euro, eller
2. 10 000 000 kronor för en offentlig verksamhetsutövare.

Paragrafen genomför delvis artikel 22 i CER-direktivet. Paragrafen fastställer minimi- och maximibelopp för sanktionsavgifter. Övervägandena finns i avsnitt 11.5.2.

Av paragrafen framgår att det lägsta belopp som en sanktionsavgift kan

bestämmas till är 5 000 kronor. Maximinivån beror på vilken typ av verksamhetsutövare det är fråga om. Vad som avses med uttrycken enskild verksamhetsutövare och offentlig verksamhetsutövare framgår av 1 kap. 2 § 1 och 5. Hur avgiftens storlek närmare ska bestämmas regleras genom 5 §. Belopp i den övre delen av beloppsintervallen bör komma i fråga endast för mycket allvarliga överträdelser.

5 § När sanktionsavgiftens storlek bestäms ska särskild hänsyn tas till

1. den skada eller risk för skada som har uppstått till följd av överträdelsen,
2. om den kritiska verksamhetsutövaren tidigare har gjort sig skyldig till en överträdelse, och
3. den ekonomiska fördel som överträdelsen har inneburit för verksamhetsutövaren.

Paragrafen genomför delvis artikel 22 i CER-direktivet. Paragrafen reglerar vilka omständigheter som särskilt ska beaktas vid bestämmande av sanktionsavgiftens storlek. Övervägandena finns i avsnitt 11.5.3.

I bedömningen av skada eller risk för skada som har uppstått till följd av överträdelsen bör tillsynsmyndigheten beakta bland annat ekonomiska förluster för andra än verksamhetsutövaren och antal användare som berörs. Vid bedömningen av om verksamhetsutövaren tidigare har gjort sig skyldig till en överträdelse bör tiden mellan den tidigare och den aktuella överträdelsen vägas in. Det bör även beaktas om överträdelserna är likartade. Ekonomisk fördel inbegriper både fastställbara vinster och sådana kostnader som har undvikits till följd av överträdelsen.

Uppräkningen i paragrafen är inte uttömmande, utan det kan finnas andra relevanta omständigheter som bör beaktas. Utöver de i paragrafen angivna omständigheterna kan hänsyn till exempel behöva tas till hur länge överträdelsen har pågått och om den har skett uppsåtligen.

6 § En sanktionsavgift får inte beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

Paragrafen genomför delvis artikel 22 i CER-direktivet. Paragrafen syftar till att förhindra att en överträdelse blir föremål för både sanktionsavgift och utdömande av vite enligt ett tidigare föreläggande. Övervägandena finns i avsnitt 11.5.4.

Paragrafen innebär att tillsynsmyndigheten är förhindrad att besluta om en sanktionsavgift, om överträdelsen omfattas av ett vitesföreläggande för samma överträdelse och en domstolsprocess har inletts om utdömande av vitet.

En sanktionsavgift får inte heller tas ut av verksamhetsutövaren om en sådan avgift har tagits ut enligt ett annat regelverk för samma överträdelse. Detta följer inte av paragrafen utan av dubbelbestraffningsförbudet.

7 § En sanktionsavgift får beslutas endast om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

Paragrafen genomför delvis artikel 22 i CER-direktivet. Paragrafen reglerar bland annat den bortre tidsgränsen för när en sanktionsavgift får beslutas. Övervägandena finns i avsnitt 11.5.4.

Sanktionsavgift får inte tas ut om kommunikation enligt förvaltningslagen med den som avgiften ska tas ut av inte har skett inom två år från överträdelsen. Det är tillsynsmyndighetens ansvar att kontrollera att kommunikation har skett. Av paragrafen följer vidare att ett beslut om sanktionsavgift ska delges den avgiftsskyldige, vilket innebär att tillsynsmyndigheten ska använda sig av de metoder för delgivning som regleras i delgivningslagen (2010:1932) för att säkerställa att den som beslutet gäller får del av det.

8 § En sanktionsavgift ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas i rätt tid, ska tillsynsmyndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m.

Sanktionsavgiften tillfaller staten.

Paragrafen innehåller bestämmelser om betalning och indrivning av sanktionsavgifter. Övervägandena finns i avsnitt 11.5.4.

9 § En sanktionsavgift faller bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

Paragrafen innebär att skyldigheten att betala en sanktionsavgift kan falla bort. Övervägandena finns i avsnitt 11.5.4.

6 kap. Överklagande

1 § Beslut enligt denna lag får överklagas till allmän förvaltningsdomstol. När ett sådant beslut överklagas är den beslutande myndigheten motpart i domstolen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen, som genomför delvis artikel 21.4 i CER-direktivet, reglerar överklagande av beslut enligt lagen. Övervägandena finns i avsnitt 12. Paragrafen utformas i allt väsentligt enligt *Lagrådets* förslag.

Beslut som överklagas ska prövas av den förvaltningsrätt inom vars domkrets ärendet först prövats i enlighet med 14 § andra stycket lagen (1971:289) om allmänna förvaltningsdomstolar. Förvaltningsrättens avgörande kan överklagas till behörig kammarrätt. Prövningstillstånd krävs vid överklagande till kammarrätten.

Paragrafen reglerar endast förutsättningarna att överklaga beslut enligt lagen. Vid handräckning gäller, som följer av 4 kap. 6 §, bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande. Utsökningsbalkens bestämmelser om överklagande gäller därmed också i det sammanhanget.

17.2 Förslaget till lag om ändring i lagen (1998:620) om belastningsregister

9 § En enskild har rätt att på begäran skriftligen få ta del av samtliga uppgifter ur registret om sig själv. Om sådana uppgifter finns har den enskilde även rätt att få sådan skriftlig information som anges i 4 kap. 3 § första stycket 1–8 brottsdatalagen (2018:1177). Uppgifterna ska på begäran lämnas ut utan avgift en gång per kalenderår.

En enskild som behöver ett registerutdrag om sig själv har rätt att få ett begränsat utdrag ur registret

1. för att kunna ta till vara sin rätt i ett främmande land eller få tillstånd att resa in, bosätta sig eller arbeta där,
2. enligt bestämmelser i skollagen (2010:800),
3. enligt bestämmelser i lagen (2018:1219) om försäkringsdistribution,
4. enligt bestämmelser i lagen (2007:171) om registerkontroll av personal vid vissa boenden som tar emot barn,
5. enligt bestämmelser i lagen (2010:479) om registerkontroll av personal som utför vissa insatser åt barn med funktionshinder,
6. enligt bestämmelser i lagen (2013:852) om registerkontroll av personer som ska arbeta med barn,
7. enligt bestämmelser i lagen (2026:43) om registerkontroll vid arbete i hemmet åt äldre personer eller vuxna personer med funktionsnedsättning,
8. enligt bestämmelser i lagen (2026:44) om registerkontroll vid anställning till ledande befattningar i kommuner*, eller*
9. enligt bestämmelser i lagen (2026:000) om motståndskraft hos kritiska verksamhetsutövare.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om vilka uppgifter ett sådant utdrag som avses i andra stycket 1–3 ska innehålla.

Regeringen får meddela föreskrifter om vilka uppgifter ett sådant utdrag som avses i andra stycket 4–*9* ska innehålla.

En begäran om uppgifter ur registret ska vara skriftlig. Polismyndigheten ska säkerställa att begäran görs av en behörig person.

I paragrafen anges i vilka fall en enskild har rätt att ta del av uppgifter ur belastningsregistret om sig själv. Ändringen i paragrafens andra stycke genomför delvis artikel 14.2 och 14.3 i Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (här benämnt CER-direktivet). Övervägandena finns i avsnitt 9.3.

En ny punkt införs i paragrafen och bestämmelsen innebär en rätt för en enskild att med stöd av lagen om motståndskraft hos kritiska verksamhetsutövare få ett begränsat utdrag ur belastningsregistret om sig själv.

Paragrafen ändras också på så sätt att regeringen bemyndigas att få meddela föreskrifter om vilka uppgifter ett sådant utdrag ska innehålla.

12 a § Uppgifter ur registret får efter en begäran som sker med stöd av rådets rambeslut 2009/315/RIF av den 26 februari 2009 om organisationen av medlemsstaternas utbyte av uppgifter ur kriminalregistret och uppgifternas innehåll lämnas ut till en myndighet i en annan medlemsstat i Europeiska unionen för något annat ändamål än att användas i ett brottmålsförfarande om motsvarande rätt att få del av uppgifterna finns för en svensk myndighet.

En uppgift som har förts in i registret med stöd av 4 a § får dock inte lämnas ut om Polismyndigheten har underrättats av en behörig myndighet i den stat som har överfört uppgiften om att uppgiften har gallrats i den staten.

Uppgifter ur registret får lämnas ut till en annan medlemsstat i Europeiska unionen om begäran görs med stöd av Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG, i den ursprungliga lydelsen. Detta gäller även om motsvarande rätt att få del av uppgifterna saknas för en svensk myndighet.

Ändringen i paragrafen genomför delvis artikel 14.2 och 14.3 i CER-direktivet. I paragrafen anges när uppgifter ur belastningsregistret får lämnas ut till en utländsk myndighet för något annat ändamål än att användas i ett brottmålsförfarande. För att utlämnande ska få ske krävs att motsvarande rätt att få del av uppgifterna finns för en svensk myndighet. Övervägandena finns i avsnitt 9.6.

Tredje stycket, som är nytt, innebär att uppgifter från belastningsregistret får lämnas ut till en utländsk myndighet som har gjort en framställan med stöd av CER-direktivet. Ett sådant utlämnande får ske även om motsvarande rätt att få del av uppgifterna saknas för en svensk myndighet. Hänvisningen till direktivet är statisk och avser därmed EU-rättsakten i dess lydelse vid en viss tidpunkt.

17.3 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

15 kap.

3 d § *Sekretessen enligt 1 a § hindrar inte att Myndigheten för civilt försvar i egenskap av en sådan gemensam kontaktpunkt som avses i 1 kap. 8 § lagen (2026:000) om motståndskraft hos kritiska verksamhetsutövare lämnar en uppgift till en tillsynsmyndighet enligt samma lag, om uppgiften behövs för att tillsynsmyndigheten ska kunna fullgöra sitt uppdrag.*

Sekretessen hindrar inte heller att en sådan tillsynsmyndighet som avses i första stycket lämnar en uppgift till Myndigheten för civilt försvar, om uppgiften behövs för att Myndigheten för civilt försvar ska kunna fullgöra sitt uppdrag som sådan gemensam kontaktpunkt som avses i första stycket.

En uppgift enligt första eller andra stycket får lämnas endast om intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.

Paragrafen, som är ny, innehåller sekretessbrytande bestämmelser för dels Myndigheten för civilt försvar (MCF), dels tillsynsmyndigheterna enligt lagen om motståndskraft hos kritiska verksamhetsutövare när det gäller sekretess i det internationella samarbetet. Övervägandena finns i avsnitt 13.1.

Första stycket gör det möjligt för MCF att lämna vidare en uppgift som omfattas av sekretess i det internationella samarbetet och som myndigheten har fått del av i egenskap av ansvarig för i paragrafen angiven funktion, om uppgiften behövs för att den mottagande tillsynsmyndigheten ska kunna fullgöra sitt uppdrag enligt lagen om motståndskraft hos kritiska verksamhetsutövare.

Enligt *andra stycket* är det även möjligt för en tillsynsmyndighet att vidarebefordra en uppgift som omfattas av sekretess i det internationella samarbetet till MCF, om uppgiften behövs för att myndigheten ska kunna fullgöra sina uppgifter i egenskap av angiven funktion.

Enligt *tredje stycket* bryts sekretessen endast om intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda. Det ska alltså göras en intresseavvägning.

18 kap.

8 b § Sekretess gäller för uppgift i en incidentrapport enligt cybersäkerhetslagen (2025:1506) *och lagen (2026:000) om motståndskraft hos kritiska verksamhetsutövare samt* för uppgift om vilka åtgärder som en verksamhetsutövare har vidtagit till följd av incidenten, om det inte står klart att uppgiften kan röjas utan att den rapporterande verksamhetsutövarens framtida verksamhet skadas eller syftet med vidtagen åtgärd motverkas.

För uppgift i en allmän handling gäller sekretessen i högst fyrtio år.

Paragrafen innehåller bestämmelser om sekretess för uppgifter i incidentrapporter enligt cybersäkerhetslagen och uppgifter om vilka åtgärder som en verksamhetsutövare har vidtagit med anledning av sådana incidenter som har rapporterats. Paragrafen ändras så att den avser även incidentanmälningar och incidentrapporter enligt lagen om motståndskraft hos kritiska verksamhetsutövare och motsvarande uppgifter kopplat till sådana. Övervägandena finns i avsnitt 13.1.

17.4 Förslaget till lag om ändring i säkerhetsskyddslagen (2018:585)

7 kap.

4 § En sanktionsavgift ska bestämmas till lägst 25 000 kronor och högst *till det högsta av 2 procent av verksamhetsutövarens totala globala årsomsättning under närmast föregående räkenskapsår och 120 000 000 kronor*. Sanktionsavgiften för en statlig myndighet, kommun eller region ska dock bestämmas till högst 10 000 000 kronor.

Paragrafen fastställer minimi- och maximibelopp för en sanktionsavgift enligt lagen. Övervägandena finns i avsnitt 14.

Ändringen innebär att det högsta beloppet som en sanktionsavgift kan bestämmas till höjs för en verksamhetsutövare som inte är en statlig myndighet, kommun eller region.

Ikraftträdande- och övergångsbestämmelser

1. Denna lag träder i kraft den 1 januari 2027.

2. Äldre bestämmelser gäller fortfarande för överträdelser som har ägt rum före ikraftträdandet.

Övervägandena finns i avsnitt 15.

Enligt *punkt 1* träder lagen i kraft den 1 januari 2027.

Enligt *punkt 2* ska äldre bestämmelser fortfarande tillämpas i fråga om överträdelser som har skett före ikraftträdandet av den ändrade bestämmelsen.

17.5 Förslaget till lag om ändring i cybersäkerhetslagen (2025:1506)

Genom ändringarna av lagen genomförs delvis Europaparlamentets och rådets direktiv (EU) av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

1 kap.

8 a § *Lagen gäller också för en verksamhetsutövare som har identifierats som en kritisk verksamhetsutövare enligt 2 kap. 1 § lagen (2026:000) om motståndskraft hos kritiska verksamhetsutövare.*

Paragrafen, som är ny, genomför artikel 2.3 i NIS 2-direktivet. Övervägandena finns i avsnitt 6.5.

Paragrafen innebär att den som är identifierad som en kritisk verksamhetsutövare enligt 2 kap. 1 § lagen om motståndskraft hos kritiska verksamhetsutövare omfattas av cybersäkerhetslagen. Det ställs inte upp några andra krav utöver att verksamhetsutövaren ska vara identifierad som kritisk verksamhetsutövare. Av 2 kap. 2 § cybersäkerhetslagen framgår att en verksamhetsutövare som omfattas av den lagen är skyldig att så snart det kan ske anmäla sig till den myndighet som regeringen bestämmer.

9 § Som väsentlig verksamhetsutövare räknas

1. en verksamhetsutövare som är en statlig myndighet,
2. en verksamhetsutövare som är större än ett medelstort företag och som

a) är en kommun eller en region,

b) i övrigt omfattas av bilaga 1 till NIS 2-direktivet i den ursprungliga lydelsen men inte av 7 § 2 eller 3, eller

c) är en enskild utbildningsanordnare med tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina,

3. en verksamhetsutövare som avses i 6 § och som storleksmässigt motsvarar eller är större än ett medelstort företag,
4. en verksamhetsutövare som avses i 7 § 2 eller 3,
5. en verksamhetsutövare som är en kvalificerad tillhandahållare av betrodda tjänster,
6. en verksamhetsutövare som räknas som väsentlig enligt föreskrifter som har meddelats med stöd av 15 § andra stycket, *och*
7. *en verksamhetsutövare som avses i 8 a §.*

Verksamhetsutövare som inte är väsentliga är viktiga verksamhetsutövare.

Ändringen i paragrafen genomför artikel 3.1 f i NIS 2-direktivet. Övervägandena finns i avsnitt 6.5.

Ändringen innebär att den som har identifierats som kritisk verksamhetsutövare enligt 2 kap. 1 § lagen om motståndskraft hos kritiska

verksamhetsutövare är en väsentlig verksamhetsutövare enligt cybersäkerhetslagen. Kategoriseringen är av betydelse för vilka tillsynsåtgärder som kan vidtas med stöd av 3 kap. cybersäkerhetslagen och vilka ingripanden som kan komma i fråga med stöd av 4 kap. samma lag.

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2557

av den 14 december 2022

om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA DIREKTIV

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ([1]),

med beaktande av Regionkommitténs yttrande ([2]),

i enlighet med det ordinarie lagstiftningsförfarandet ([3]), och

av följande skäl:

(1) Som tillhandahållare av samhällsviktiga tjänster spelar kritiska entiteter en oumbärlig roll när det gäller att upprätthålla viktiga samhällsfunktioner eller central ekonomisk verksamhet på den inre marknaden, i en unionsekonomi som i allt högre grad kännetecknas av ömsesidigt beroende. Det är därför mycket viktigt att det inrättas en unionsram som syftar dels till att stärka kritiska entiteters motståndskraft på den inre marknaden genom att fastställa harmoniserade minimiregler, dels till att bistå entiteterna genom enhetligt och särskilt stöd och tillsynsåtgärder.

(2) I rådets direktiv 2008/114/EG ([4]) föreskrivs ett förfarande för att klassificera infrastruktur i energi- och transportsektorerna som europeisk kritisk infrastruktur, vars driftstörning eller förstörelse skulle få betydande gränsöverskridande konsekvenser i minst två medlemsstater. Det direktivet är uteslutande inriktat på skyddet av sådan infrastruktur. Vid den utvärdering av direktiv 2008/114/EG som gjordes 2019 konstaterades dock att skyddsåtgärder som enbart gäller enskilda tillgångar inte är tillräckliga för att förhindra alla störningar från att uppstå, på grund av den alltmer sammankopplade och gränsöverskridande karaktären hos den verksamhet som bedrivs med kritisk infrastruktur. Därför är det nödvändigt att ändra ansatsen i riktning mot att säkerställa att risker

([1]) EUT C 286, 16.7.2021, s. 170.
([2]) EUT C 440, 29.10.2021, s. 99.
([3]) Europaparlamentets ståndpunkt av den 22 november 2022 (ännu inte offentliggjord i EUT) och rådets beslut av den 8 december 2022.
([4]) Rådets direktiv 2008/114/EG av den 8 december 2008 om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna (EUT L 345, 23.12.2008, s. 75).

redovisas bättre, att bättre definiera och skapa enhetlighet i rollen och uppgifterna för kritiska entiteter i egenskap av tillhandahållare av tjänster som är nödvändiga för att den inre marknaden ska kunna fungera, och att unionsregler antas för att stärka kritiska entiteters motståndskraft. Kritiska entiteter bör kunna öka sin förmåga att förebygga, skydda mot, reagera på, stå emot, begränsa, absorbera, anpassa sig till och återhämta sig från incidenter som kan störa tillhandahållandet av samhällsviktiga tjänster.

(3) Samtidigt som ett antal åtgärder på unionsnivå, såsom det europeiska programmet för skydd av kritisk infrastruktur, och nationell nivå syftar till att stödja skyddet av kritisk infrastruktur i unionen bör mer göras för att de entiteter som driver sådan infrastruktur ska vara bättre rustade att hantera de risker för deras verksamhet som kan leda till störningar i tillhandahållandet av samhällsviktiga tjänster. Mer bör också göras för att bättre rusta sådana entiteter eftersom det finns en dynamisk hotbild, som inbegriper framväxande hybrid- och terroristhot, och ett ökande ömsesidigt beroende mellan infrastruktur och sektorer. Dessutom finns det en ökad fysisk risk på grund av naturkatastrofer och klimatförändringen, som leder till att extrema väderhändelser blir allt vanligare och mer omfattande och medför långsiktiga förändringar i genomsnittliga klimatförhållanden som kan minska kapaciteten, effektiviteten och livslängden för vissa typer av infrastruktur om det inte vidtas klimatanpassningsåtgärder. Den inre marknaden kännetecknas dessutom av fragmentering när det gäller identifiering av kritiska entiteter, eftersom relevanta sektorer och kategorier av entiteter inte erkänns på ett enhetligt sätt som kritiska i alla medlemsstater. Detta direktiv bör därför åstadkomma en solid harmoniseringsnivå när det gäller de sektorer och kategorier av entiteter som omfattas av dess tillämpningsområde.

(4) Vissa sektorer inom ekonomin, exempelvis energi- och transportsektorerna, är redan reglerade genom sektorsspecifika unionsrättsakter, men dessa rättsakter innehåller bestämmelser som endast rör vissa aspekter av motståndskraften hos entiteter som är verksamma inom de sektorerna. För att på ett heltäckande sätt hantera motståndskraften hos de entiteter som är kritiska för att den inre marknaden ska fungera väl inrättas genom detta direktiv en övergripande ram för att hantera kritiska entiteters motståndskraft med hänsyn till alla faror, oberoende av om det är naturliga faror eller faror orsakade av människan, olyckshändelser eller avsiktligt framkallade faror.

(5) Det ökande ömsesidiga beroendet mellan infrastruktur och sektorer är ett resultat av ett alltmer gränsöverskridande och ömsesidigt beroende nätverk av tillhandahållande av tjänster som använder viktig infrastruktur i hela unionen inom sektorerna för energi, transporter, bankverksamhet, dricksvatten, avloppsvatten, produktion, bearbetning och distribution av livsmedel, hälso- och sjukvård, rymden, finansmarknadsinfrastruktur och digital infrastruktur samt vissa aspekter av sektorn för offentlig förvaltning. Rymdsektorn omfattas av tillämpningsområdet för detta direktiv när det gäller tillhandahållandet av vissa tjänster som är beroende av markbaserad infrastruktur som ägs, förvaltas och drivs av medlemsstater eller privata parter; infrastruktur som ägs, förvaltas eller drivs av unionen eller för unionens räkning inom ramen för dess rymdprogram omfattas därför inte av tillämpningsområdet för detta direktiv.

När det gäller energisektorn och särskilt metoderna för produktion och överföring av el (avseende elförsörjning) kan det i produktionen av el, när så anses lämpligt, ingå kärnkraftsanläggningars delar för överföring av el, men inte de specifikt kärnkraftsrelaterade delar som omfattas av fördrag och unionsrätt, inbegripet relevanta unionsrättsakter avseende kärnkraft. Processen för identifiering av kritiska entiteter inom livsmedelssektorn bör på lämpligt sätt återspegla den inre marknadens karaktär inom den sektorn och de omfattande unionsreglerna i fråga om allmänna principer och krav för livsmedelslagstiftning och livsmedelssäkerhet. För att säkerställa en proportionerlig ansats och för att på lämpligt sätt återspegla dessa entiteters roll och betydelse på nationell nivå, bör kritiska entiteter därför endast identifieras bland livsmedelsföretag, oavsett om de är vinstdrivande eller inte och oavsett om de är offentliga eller privata, som uteslutande bedriver logistikverksamhet och grossisthandel samt storskalig industriell produktion och bearbetning med en betydande marknadsandel på nationell nivå. Detta ömsesidiga beroende innebär att alla störningar av samhällsviktiga tjänster, även sådana som till en början är begränsade till en entitet eller en sektor, kan få dominoeffekter i vidare bemärkelse, vilket kan leda till långtgående och långvariga negativa konsekvenser för tillhandahållandet av tjänster på hela den inre marknaden. Större kriser såsom covid-19-pandemin har visat hur sårbara våra alltmer av varandra beroende samhällen är för risker med låg sannolikhet och stora konsekvenser.

(6) De entiteter som deltar i tillhandahållandet av samhällsviktiga tjänster omfattas i allt högre grad av olika krav som införs enligt nationell rätt. Vissa medlemsstater ställer mindre hårda säkerhetskrav på dessa entiteter, vilket inte bara leder till olika grad av motståndskraft utan också riskerar att ge negativa effekter för upprätthållandet av viktiga samhällsfunktioner eller central ekonomisk verksamhet i unionen och skapar hinder för den inre marknadens funktion. Investerare och företag kan förlita sig på och ha förtroende för kritiska entiteter som är motståndskraftiga, och tillförlitlighet och förtroende är hörnstenar i en välfungerande inre marknad. Likartade typer av entiteter betraktas som kritiska i vissa medlemsstater men inte i andra, och de som identifieras som kritiska omfattas av olika krav i olika medlemsstater. Detta leder till en ytterligare och onödig administrativ börda för företag som bedriver gränsöverskridande verksamhet, särskilt för företag med verksamhet i medlemsstater som ställer hårdare krav. En unionsram skulle därför också leda till likvärdiga förutsättningar för kritiska entiteter i hela unionen.

(7) Det är nödvändigt att införa harmoniserade minimiregler för att säkerställa tillhandahållandet av samhällsviktiga tjänster på den inre marknaden, stärka kritiska entiteters motståndskraft samt förbättra det gränsöverskridande samarbetet mellan behöriga myndigheter. Det är viktigt att dessa regler är framtidssäkrade när det gäller utformning och genomförande, samtidigt som utrymme ges för den flexibilitet som krävs. Det är också mycket viktigt att förbättra kritiska entiteters förmåga att tillhandahålla samhällsviktiga tjänster med avseende på en rad olika risker.

(8) För att uppnå en hög grad av motståndskraft bör medlemsstaterna identifiera kritiska entiteter som kommer att omfattas av särskilda krav och tillsyn och som kommer att ges särskilt stöd och vägledning med avseende på alla relevanta risker.

(9) Med tanke på hur viktig cybersäkerhet är för kritiska entiteters motståndskraft och för att skapa enhetlighet bör man, när så är möjligt, säkerställa samstämmighet mellan detta direktiv och Europaparlamentets och rådets direktiv (EU) 2022/2555 ([5]). Med tanke på den högre frekvensen av och de särskilda egenskaperna hos cyberrisker införs det genom direktiv (EU) 2022/2555 heltäckande krav på en stor uppsättning entiteter för att säkerställa deras cybersäkerhet. Eftersom cybersäkerhet hanteras i tillräcklig grad genom (EU) 2022/2555 bör de frågor som omfattas av det direktivet uteslutas från tillämpningsområdet för det här direktivet, utan att det påverkar tillämpningen av den särskilda ordningen för entiteter inom sektorn för digital infrastruktur.

(10) Om det enligt bestämmelser i sektorsspecifika unionsrättsakter krävs att kritiska entiteter ska vidta åtgärder för att stärka sin motståndskraft, och om dessa krav av medlemsstaterna erkänns vara minst likvärdiga med motsvarande skyldigheter enligt det här direktivet, bör de relevanta bestämmelserna i det här direktivet inte vara tillämpliga, för att undvika dubbelarbete och onödig börda. I sådant fall bör de relevanta bestämmelserna i de unionsrättsakterna tillämpas. Om de relevanta bestämmelserna i det här direktivet inte är tillämpliga bör inte heller bestämmelserna om tillsyn och kontroll av efterlevnad i det här direktivet vara tillämpliga.

(11) Detta direktiv påverkar inte medlemsstaternas och deras myndigheters befogenheter i fråga om administrativ självständighet eller deras ansvar att skydda den nationella säkerheten och försvaret eller deras befogenhet att skydda andra väsentliga statliga funktioner, särskilt ifråga om allmän säkerhet, territoriell integritet och upprätthållande av lag och ordning. Undantaget för offentliga förvaltningsentiteter från tillämpningsområdet för detta direktiv bör tillämpas på entiteter vars verksamhet till övervägande del bedrivs på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet utredning, upptäckt och lagföring av brott. Offentliga förvaltningsentiteter vars verksamhet endast marginellt hänför sig till dessa områden bör dock omfattas av detta direktivs tillämpningsområde. Vid tillämpningen av detta direktiv anses entiteter med tillsynsbefogenheter inte bedriva verksamhet på brottsbekämpningsområdet, och de är därför inte undantagna från detta direktivs tillämpningsområde på den grunden. Offentliga förvaltningsentiteter som inrättats gemensamt med ett tredjeland i enlighet med ett internationellt avtal är undantagna från detta direktivs tillämpningsområde. Detta direktiv är inte tillämpligt på medlemsstaternas diplomatiska och konsulära beskickningar i tredjeländer.

([5]) Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972, och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (se sidan 80 i detta nummer av EUT).

Vissa kritiska entiteter bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet utredning, upptäckt och lagföring av brott, eller tillhandahåller tjänster uteslutande till offentliga förvaltningsentiteter som till övervägande del bedriver verksamhet på de områdena. Med tanke på medlemsstaternas ansvar att skydda den nationella säkerheten och försvaret bör medlemsstaterna kunna besluta att skyldigheterna för kritiska entiteter enligt detta direktiv helt eller delvis inte ska gälla dessa kritiska entiteter om de tjänster de tillhandahåller eller den verksamhet de bedriver till övervägande del har anknytning till områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet utredning, upptäckt och lagföring av brott. Kritiska entiteter vars tjänster eller verksamhet endast marginellt hänför sig till dessa områden bör fortfarande omfattas av detta direktivs tillämpningsområde. Ingen medlemsstat bör vara skyldig att lämna information vars avslöjande skulle strida mot dess väsentliga intressen i fråga om nationell säkerhet. Unionsregler eller nationella regler till skydd för säkerhetsskyddsklassificerade uppgifter och sekretessavtal är relevanta i detta sammanhang.

(12) För att inte äventyra nationell säkerhet eller kritiska entiteters säkerhetsintressen och kommersiella intressen bör tillgången till samt utbytet och hanteringen av känslig information ske med försiktighet och med särskild hänsyn till de transmissionskanaler och den lagringskapacitet som används.

(13) I syfte att säkerställa ett heltäckande förhållningssätt för kritiska entiteters motståndskraft bör varje medlemsstat inrätta en strategi för att stärka kritiska entiteters motståndskraft (*strategin*). Strategin bör fastställa de strategiska mål och policyåtgärder som ska genomföras. Strategin bör, i syfte att uppnå samstämmighet och effektivitet, utformas så att den smidigt integrerar befintlig politik och, när så är möjligt, bygger på relevanta befintliga nationella och sektorsspecifika strategier, planer eller liknande dokument. För att uppnå ett heltäckande förhållningssätt bör medlemsstaterna säkerställa att deras strategier innehåller en policyram för utökat samarbete mellan de behöriga myndigheterna enligt detta direktiv och de behöriga myndigheterna enligt direktiv (EU) 2022/2555 i samband med utbyte av information om cybersäkerhetsrisker, cyberhot och cyberincidenter och icke-cyberrelaterade risker, hot och incidenter och i samband med fullgörandet av tillsynsuppgifter. Vid inrättandet av sina strategier bör medlemsstaterna ta vederbörlig hänsyn till hybridkaraktären hos hoten mot kritiska entiteter.

(14) Medlemsstaterna bör underrätta kommissionen om sina strategier och om betydande uppdateringar av dem, särskilt för att kommissionen ska kunna bedöma huruvida detta direktiv tillämpas korrekt när det gäller policyval avseende kritiska entiteters motståndskraft på nationell nivå. Informationen om strategierna kan vid behov lämnas som sekretessbelagd information. Kommissionen bör utarbeta en sammanfattande rapport om de strategier som medlemsstaterna har informerat om, vilken ska ligga till grund för informationsutbyte för att identifiera bästa praxis och frågor av gemensamt intresse inom ramen för gruppen för kritiska entiteters motståndskraft. På grund av den känsliga karaktären hos den aggregerade information som ska ingå i den sammanfattande rapporten, oavsett om den är sekretessbelagd eller inte, bör kommissionen på lämpligt sätt beakta säkerheten för de kritiska entiteterna, medlemsstaterna och unionen. Den sammanfattande rapporten och strategierna bör skyddas mot olagliga eller avsiktligt skadliga handlingar och bör endast vara tillgängliga för behöriga personer i syfte att uppfylla målen i detta direktiv. Informationen om strategierna och om betydande uppdateringar av dem bör även hjälpa kommissionen att förstå hur förhållningssätten till kritiska entiteters motståndskraft utvecklas och bidra till övervakningen av effekterna och mervärdet av detta direktiv, vilket kommissionen regelbundet ska se över.

(15) Medlemsstaternas åtgärder för att identifiera och bidra till att säkerställa kritiska entiteters motståndskraft bör följa en riskbaserad ansats med inriktning på de entiteter som är mest relevanta för att viktiga samhällsfunktioner och central ekonomisk verksamhet ska kunna upprätthållas. För att säkerställa en sådan riktad ansats bör varje medlemsstat inom en harmoniserad ram göra en bedömning av relevanta risker för naturolyckor och risker orsakade av människan, inbegripet risker av sektorsövergripande eller gränsöverskridande slag, som kan påverka tillhandahållandet av samhällsviktiga tjänster, däribland olyckor, naturkatastrofer, hot mot folkhälsan såsom pandemier och hybridhot eller andra antagonistiska hot, inklusive terroristbrott, brottslig infiltration och sabotage (*medlemsstaternas riskbedömning*). När medlemsstaternas riskbedömningar görs bör medlemsstaterna ta hänsyn till andra allmänna eller sektorsspecifika riskbedömningar som har gjorts enligt andra unionsrättsakter och bör ta hänsyn till i hur stor grad sektorer är beroende av varandra, inbegripet av sektorer i andra medlemsstater och tredjeländer. Resultatet av medlemsstaternas riskbedömningar bör användas för att identifiera kritiska entiteter och bistå dessa entiteter med att uppfylla sina krav på motståndskraft. Detta direktiv är endast tillämpligt på medlemsstater och kritiska entiteter som är verksamma inom unionen. Den expertis och kunskap som genereras av

de behöriga myndigheterna, särskilt genom riskbedömningar, och av kommissionen, särskilt genom olika former av stöd och samarbete, kan dock användas, när så är lämpligt och i enlighet med tillämpliga rättsliga instrument, till förmån för tredjeländer, särskilt de i unionens direkta grannskap, genom att bidra till det befintliga samarbetet om motståndskraft.

(16) För att säkerställa att alla relevanta entiteter omfattas av kraven på motståndskraft i detta direktiv och för att minska skillnaderna i det avseendet är det viktigt att införa harmoniserade regler som möjliggör en enhetlig identifiering av kritiska entiteter i hela unionen och samtidigt ger medlemsstaterna möjlighet att på lämpligt sätt återge dessa entiteters roll och betydelse på nationell nivå. Varje medlemsstat bör vid tillämpning av de kriterier som fastställs i detta direktiv identifiera entiteter som tillhandahåller en eller flera samhällsviktiga tjänster och som bedriver verksamhet och har kritisk infrastruktur på dess territorium. En entitet bör anses bedriva verksamhet på territoriet i en medlemsstat där den utför verksamhet som är nödvändig för den eller de samhällsviktiga tjänsterna i fråga och där den entitetens kritiska infrastruktur, som används för att tillhandahålla tjänsten eller tjänsterna, är belägen. Om ingen entitet uppfyller dessa kriterier i en medlemsstat bör den medlemsstaten inte vara skyldig att identifiera en kritisk entitet i motsvarande sektor eller undersektor. För att skapa ändamålsenlighet, effektivitet, enhetlighet och rättssäkerhet bör det också fastställas lämpliga regler för att underrätta entiteter om att de har identifierats som kritiska entiteter.

(17) Medlemsstaterna bör, på ett sätt som uppfyller målen för detta direktiv, till kommissionen överlämna en förteckning över samhällsviktiga tjänster, antalet kritiska entiteter som har identifierats för varje sektor och undersektor som anges i bilagan och för den eller de samhällsviktiga tjänster som varje entitet tillhandahåller och, om sådana tillämpas, tröskelvärden. Det bör vara möjligt att presentera tröskelvärden som sådana eller i aggregerad form, vilket innebär att genomsnittliga uppgifter kan anges per geografiskt område, per år, per sektor, per undersektor eller på annat sätt, och att uppgifter om intervallet för tillhandahållna indikatorer kan ingå.

(18) Det bör upprättas kriterier för att fastställa hur betydande en störande effekt som uppstår till följd av en incident är. Dessa kriterier bör utgå från de kriterier som fastställs i Europaparlamentets och rådets direktiv (EU) 2016/1148 ([6]) för att ta vara på medlemsstaternas ansträngningar för att identifiera leverantörer av samhällsviktiga tjänster enligt definitionen i det direktivet, och de erfarenheter som har gjorts i det avseendet. Större kriser såsom covid-19-pandemin har visat hur viktigt det är att säkerställa säkerheten i leveranskedjan och hur störningar av den kan få negativa ekonomiska och samhälleliga konsekvenser inom ett stort antal sektorer och över gränserna. Medlemsstaterna bör därför i möjligaste mån även beakta effekterna på leveranskedjan när de fastställer i hur stor grad andra sektorer och undersektorer är beroende av den samhällsviktiga tjänst som tillhandahålls av en kritisk entitet.

(19) I enlighet med tillämplig unionsrätt och nationell rätt, inbegripet Europaparlamentets och rådets förordning (EU) 2019/452 ([7]), som inrättar en ram för granskning av utländska direktinvesteringar i unionen, bör det potentiella hot som utländskt ägande av kritisk infrastruktur inom unionen utgör erkännas, eftersom tjänster, ekonomin och unionsmedborgarnas fria rörlighet och säkerhet är beroende av en välfungerande kritisk infrastruktur.

(20) Enligt direktiv (EU) 2022/2555 ska entiteter som tillhör sektorn för digital infrastruktur, vilka kan identifieras som kritiska entiteter enligt det här direktivet, vidta lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem samt för att underrätta om betydande incidenter och cyberhot. Eftersom hot mot säkerheten i nätverks- och informationssystem kan ha olika ursprung tillämpas i direktiv (EU) 2022/2555 en allriskansats som omfattar motståndskraften hos nätverks- och informationssystem och dessa systems fysiska komponenter och miljö.

([6]) Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EUT L 194, 19.7.2016, s. 1).

([7]) Europaparlamentets och rådets förordning (EU) 2019/452 av den 19 mars 2019 om upprättande av en ram för granskning av utländska direktinvesteringar i unionen (EUT L 79I, 21.3.2019, s. 1).

Eftersom de krav som fastställs i direktiv (EU) 2022/2555 i det avseendet minst är likvärdiga med motsvarande skyldigheter enligt det här direktivet, bör de skyldigheter som fastställs i artikel 11 och kapitlen III, IV och VI i detta direktiv inte vara tillämpliga på entiteter som tillhör sektorn för digital infrastruktur, för att undvika dubbelarbete och en onödig administrativ börda. Med tanke på hur viktiga de tjänster som tillhandahålls av entiteter inom sektorn för digital infrastruktur är för kritiska entiteter som tillhör alla andra sektorer, bör medlemsstaterna dock, med utgångspunkt i de kriterier och enligt det förfarande som föreskrivs i det här direktivet, identifiera entiteter som tillhör sektorn för digital infrastruktur som kritiska entiteter. Följaktligen bör strategierna, medlemsstaternas riskbedömningar och de stödåtgärder som anges i kapitel II i det här direktivet vara tillämpliga. Medlemsstaterna bör ha rätt att anta eller behålla bestämmelser i nationell rätt för att uppnå en högre grad av motståndskraft för dessa kritiska entiteter, förutsatt att dessa bestämmelser är förenliga med tillämplig unionsrätt.

(21) I unionsrätten om finansiella tjänster införs heltäckande krav på att finansiella entiteter ska hantera alla risker de ställs inför, inklusive operativa risker, och säkerställa driftskontinuitet. Denna rätt inbegriper Europaparlamentets och rådets förordningar (EU) nr 648/2012 ([8]), (EU) nr 575/2013 ([9]) och (EU) nr 600/2014 ([10]) samt Europaparlamentets och rådets direktiv 2013/36/EU ([11]) och 2014/65/EU ([12]). Denna rättsliga ram kompletteras av Europaparlamentets och rådets förordning (EU) 2022/2554 ([13]), där det fastställs krav som är tillämpliga på finansiella entiteter i fråga om riskhantering inom informations- och kommunikationsteknik (IKT), däribland beträffande skyddet av fysisk IKT-infrastruktur. Eftersom de entiteternas motståndskraft därför omfattas på ett heltäckande sätt bör artikel 11 och kapitlen III, IV och VI i det här direktivet inte vara tillämpliga på dessa entiteter, för att undvika dubbelarbete och en onödig administrativ börda.

Med tanke på hur viktiga de tjänster som tillhandahålls av entiteter i finanssektorn är för kritiska entiteter som tillhör alla andra sektorer, bör medlemsstaterna dock, med utgångspunkt i de kriterier och enligt det förfarande som föreskrivs i det här direktivet, identifiera entiteter i finanssektorn som kritiska entiteter. Följaktligen bör strategierna, medlemsstaternas riskbedömningar och de stödåtgärder som anges i kapitel II i det här direktivet vara tillämpliga. Medlemsstaterna bör ha rätt att anta eller behålla bestämmelser i nationell rätt för att uppnå en högre grad av motståndskraft för dessa kritiska entiteter, förutsatt att dessa bestämmelser är förenliga med tillämplig unionsrätt.

(22) Medlemsstaterna bör utse eller inrätta myndigheter som är behöriga att övervaka tillämpningen av och vid behov kontrollera efterlevnaden av reglerna i detta direktiv och säkerställa att dessa myndigheter har tillräckliga befogenheter och resurser. Med tanke på skillnaderna i nationella styrningsstrukturer och för att skydda redan befintliga sektoriella arrangemang eller unionens tillsyns- och regleringsorgan samt för att undvika dubbelarbete bör medlemsstaterna kunna utse eller inrätta mer än en behörig myndighet. Om en medlemsstat utser eller inrättar mer än en behörig myndighet bör den tydligt avgränsa de berörda myndigheternas respektive uppgifter och säkerställa att de samarbetar smidigt och effektivt. Alla behöriga myndigheter bör också samarbeta mer generellt med andra relevanta myndigheter, på både unionsnivå och nationell nivå.

([8]) Europaparlamentets och rådets förordning (EU) nr 648/2012 av den 4 juli 2012 om OTC-derivat, centrala motparter och transaktionsregister (EUT L 201, 27.7.2012, s. 1).

([9]) Europaparlamentets och rådets förordning (EU) nr 575/2013 av den 26 juni 2013 om tillsynskrav för kreditinstitut och om ändring av förordning (EU) nr 648/2012 (EUT L 176, 27.6.2013, s. 1).

([10]) Europaparlamentets och rådets förordning (EU) nr 600/2014 av den 15 maj 2014 om marknader för finansiella instrument och om ändring av förordning (EU) nr 648/2012 (EUT L 173, 12.6.2014, s. 84).

([11]) Europaparlamentets och rådets direktiv 2013/36/EU av den 26 juni 2013 om behörighet att utöva verksamhet i kreditinstitut och om tillsyn av kreditinstitut och värdepappersföretag, om ändring av direktiv 2002/87/EG och om upphävande av direktiv 2006/48/EG och 2006/49/EG (EUT L 176, 27.6.2013, s. 338).

([12]) Europaparlamentets och rådets direktiv 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU (EUT L 173, 12.6.2014, s. 349).

([13]) Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (se sidan 1 i detta nummer av EUT).

(23) För att underlätta gränsöverskridande samarbete och kommunikation och för att göra det möjligt att genomföra detta direktiv på ett effektivt sätt bör varje medlemsstat, utan att det påverkar tillämpningen av kraven i sektorsspecifika unionsrättsakter, utse en gemensam kontaktpunkt med ansvar för samordningen av frågor angående kritiska entiteters motståndskraft och gränsöverskridande samarbete på unionsnivå (*gemensam kontaktpunkt*), i förekommande fall inom en behörig myndighet. Varje gemensam kontaktpunkt bör även vid behov samarbeta och samordna kommunikationen med sin medlemsstats behöriga myndigheter, andra medlemsstaters gemensamma kontaktpunkter och gruppen för kritiska entiteters motståndskraft.

(24) De behöriga myndigheterna enligt detta direktiv och de behöriga myndigheterna enligt direktiv (EU) 2022/2555 bör samarbeta och utbyta information i fråga om cybersäkerhetsrisker, cyberhot och cyberincidenter och icke-cyberrelaterade risker, hot och incidenter som påverkar kritiska entiteter samt i fråga om relevanta åtgärder som vidtas de behöriga myndigheterna enligt det här direktivet och de behöriga myndigheterna enligt direktiv (EU) 2022/2555. Det är viktigt att medlemsstaterna säkerställer att kraven i det här direktivet och i direktiv (EU) 2022/2555 genomförs på ett kompletterande sätt och att kritiska entiteter inte utsätts för en administrativ börda som går utöver vad som är nödvändigt för att uppnå målen i det här direktivet och i det direktivet.

(25) Medlemsstaterna bör ge kritiska entiteter, inbegripet dem som kan betecknas som små eller medelstora företag, stöd för att stärka sin motståndskraft, i enlighet med medlemsstaternas skyldigheter enligt detta direktiv, utan att detta påverkar de kritiska entiteternas eget rättsliga ansvar för att säkerställa efterlevnaden, och därvid förhindra en oskälig administrativ börda. Framför allt skulle medlemsstaterna kunna utarbeta vägledningsmaterial och metoder, stödja anordnandet av övningar för att testa kritiska entiteters motståndskraft och tillhandahålla rådgivning och utbildning för kritiska entiteters personal. Om det är nödvändigt och motiverat av mål av allmänt intresse kan medlemsstaterna tillhandahålla ekonomiska resurser och bör underlätta frivilligt utbyte av information och utbyte av god praxis mellan kritiska entiteter, utan att detta påverkar tillämpningen av de konkurrensregler som fastställs i fördraget om Europeiska unionens funktionssätt (EUF-fördraget).

(26) I syfte att stärka motståndskraften hos kritiska entiteter som identifierats av medlemsstaterna och för att minska den administrativa bördan för dessa kritiska entiteter, bör de behöriga myndigheterna samråda med varandra när så är lämpligt i syfte att säkerställa att detta direktiv tillämpas på ett konsekvent sätt. Dessa samråd bör inledas på begäran av en berörd behörig myndighet och vara inriktade på att säkerställa en enhetlig ansats när det gäller sammankopplade kritiska entiteter som använder kritisk infrastruktur som är fysiskt sammankopplad mellan två eller flera medlemsstater, som tillhör samma koncerner eller företagsstrukturer, eller som har identifierats i en medlemsstat och tillhandahåller samhällsviktiga tjänster till eller i andra medlemsstater.

(27) Om det enligt bestämmelser i unionsrätten eller nationell rätt krävs att kritiska entiteter ska bedöma risker som är relevanta för tillämpningen av detta direktiv och vidta åtgärder för att säkerställa sin motståndskraft, bör dessa krav beaktas på lämpligt sätt vid tillsynen av de kritiska entiteternas efterlevnad av detta direktiv.

(28) Kritiska entiteter bör ha en heltäckande bild av de relevanta risker som de är utsatta för och en skyldighet att analysera de riskerna. För det ändamålet bör de göra riskbedömningar när det är nödvändigt med hänsyn till deras specifika omständigheter och utvecklingen av riskerna, och under alla omständigheter vart fjärde år, för att bedöma alla relevanta risker som kan störa tillhandahållandet av deras samhällsviktiga tjänster (*riskbedömning av kritiska entiteter*). Om kritiska entiteter, i enlighet med skyldigheter som föreskrivs i andra rättsakter, har gjort andra riskbedömningar eller utarbetat dokument som är relevanta för riskbedömningen av kritiska entiteter bör de kunna använda dessa bedömningar och dokument för att uppfylla kraven i detta direktiv avseende riskbedömning av kritiska entiteter. En behörig myndighet bör kunna slå fast att en befintlig riskbedömning som gjorts av en kritisk entitet och som omfattar relevanta risker och den relevanta beroendegraden helt eller delvis uppfyller de skyldigheter som fastställs i detta direktiv.

(29) Kritiska entiteter bör vidta de tekniska, säkerhetsmässiga och organisatoriska åtgärder som är lämpliga och proportionella i förhållande till de risker de ställs inför, i syfte att förebygga, skydda mot, reagera på, stå emot, begränsa, absorbera, anpassa sig till och återhämta sig efter en incident. De kritiska entiteterna bör vidta dessa åtgärder i enlighet med detta direktiv, men den detaljerade utformningen och omfattningen av åtgärderna bör avspegla de olika risker som varje kritisk entitet har identifierat inom ramen för sin riskbedömning av kritiska entiteter och särdragen hos den entiteten på ett ändamålsenligt och proportionerligt sätt. I syfte att främja en enhetlig unionsomfattande ansats bör kommissionen efter samråd med gruppen för kritiska entiteters motståndskraft anta icke-bindande riktlinjer för att närmare fastställa de tekniska, säkerhetsmässiga och organisatoriska åtgärderna. Medlemsstaterna bör säkerställa att varje kritisk entitet utser en sambandsansvarig eller motsvarande som kontaktpunkt med de behöriga myndigheterna.

(30) För effektivitetens och ansvarsutkrävandets skull bör de kritiska entiteterna beskriva de åtgärder som de vidtar tillräckligt detaljerat för att dessa syften avseende effektivitet och ansvarsutkrävande ska uppnås, med hänsyn till de identifierade riskerna, i en plan för motståndskraft eller i ett eller flera dokument som är likvärdiga med en plan för motståndskraft, och tillämpa den planen i praktiken. Om en kritisk entitet redan har vidtagit tekniska, säkerhetsmässiga och organisatoriska åtgärder och utarbetat dokument, i enlighet med andra rättsakter, som är relevanta för motståndskraftsstärkande åtgärder enligt detta direktiv, bör den, i syfte att undvika dubbelarbete, kunna använda dessa åtgärder och dokument för att uppfylla kraven avseende motståndskraft enligt detta direktiv. För att undvika dubbelarbete bör en behörig myndighet kunna slå fast att befintliga åtgärder för motståndskraft som vidtagits av en kritisk entitet och som adresserar dess skyldighet att vidta tekniska, säkerhetsmässiga och organisatoriska åtgärder enligt detta direktiv helt eller delvis uppfyller kraven i detta direktiv.

(31) I Europaparlamentets och rådets förordningar (EG) nr 725/2004 ([14]) och (EG) nr 300/2008 ([15]) samt Europaparlamentets och rådets direktiv 2005/65/EG ([16]) fastställs krav som är tillämpliga på entiteter inom luftfarts- och sjöfartssektorerna för att förebygga incidenter till följd av olagliga handlingar och för att stå emot och begränsa konsekvenserna av sådana incidenter. De åtgärder som krävs enligt det här direktivet är bredare i fråga om de risker som behandlas och de åtgärder som ska vidtas, men kritiska entiteter inom dessa sektorer bör i sin plan för motståndskraft eller motsvarande dokument återge de åtgärder som har vidtagits enligt dessa andra unionsrättsakter. Kritiska entiteter ska också ta hänsyn till Europaparlamentets och rådets direktiv 2008/96/EG ([17]), där det införs en nätövergripande vägsäkerhetsbedömning för att kartlägga riskerna för olyckor och en riktad vägsäkerhetsinspektion för att, på grundval av inspektioner på plats av befintliga vägar eller vägsträckor, identifiera farliga förhållanden, brister och problem som ökar risken för olyckor och personskador. Säkerställande av de kritiska entiteternas skydd och motståndskraft är av yttersta vikt för järnvägssektorn, och när de kritiska entiteterna genomför åtgärder för motståndskraft i enlighet med det här direktivet uppmuntras de att hänvisa till icke-bindande riktlinjer och dokument över god praxis som har utarbetats inom ramen för sektorsbaserade arbetsflöden, exempelvis EU:s plattform för tågresenärers säkerhet som inrättats genom kommissionens beslut 2018/C 232/03 ([18]).

(32) Risken för att anställda vid kritiska entiteter eller deras uppdragstagare till exempel missbrukar sina åtkomsträttigheter inom den kritiska entitetens organisation för skadliga ändamål är ett växande problem. Medlemsstaterna bör därför ange på vilka villkor kritiska entiteter, i vederbörligen motiverade fall och med beaktande av medlemsstaternas riskbedömningar, får ansöka om bakgrundskontroll av personer som ingår i specifika personalkategorier. Det bör säkerställas att de berörda myndigheterna bedömer sådana ansökningar inom en rimlig tidsram och behandlar dem i enlighet med nationell rätt och nationella förfaranden samt relevant och tillämplig unionsrätt, inbegripet om skydd av personuppgifter. För att bekräfta identiteten på en person som är föremål för en bakgrundskontroll är det lämpligt att medlemsstaterna kräver ett identitetsbevis, såsom pass, nationellt identitetskort eller digitala identifieringsformer, i enlighet med tillämplig rätt.

([14]) Europaparlamentets och rådets förordning (EG) nr 725/2004 av den 31 mars 2004 om förbättrat sjöfartsskydd på fartyg och i hamnanläggningar (EUT L 129, 29.4.2004, s. 6).
([15]) Europaparlamentets och rådets förordning (EG) nr 300/2008 av den 11 mars 2008 om gemensamma skyddsregler för den civila luftfarten och om upphävande av förordning (EG) nr 2320/2002 (EUT L 97, 9.4.2008, s. 72).
([16]) Europaparlamentets och rådets direktiv 2005/65/EG av den 26 oktober 2005 om ökat hamnskydd (EUT L 310, 25.11.2005, s. 28).
([17]) Europaparlamentets och rådets direktiv 2008/96/EG av den 19 november 2008 om förvaltning av vägars säkerhet (EUT L 319, 29.11.2008, s. 59).
([18]) Kommissionens beslut av den 29 juni 2018 om inrättandet av EU:s plattform för tågresenärers säkerhet (EUT C 232, 3.7.2018, s. 10).

Bakgrundskontroller bör omfatta en kontroll av den berörda personen i kriminalregister. Medlemsstaterna bör använda det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister i enlighet med de förfaranden som fastställs i rådets rambeslut 2009/315/RIF ([19]) och, i förekommande och tillämpliga fall, Europaparlamentets och rådets förordning (EU) 2019/816 ([20]) för att inhämta information ur kriminalregister som innehas av andra medlemsstater. Medlemsstaterna kan också, i förekommande och tillämpliga fall, utnyttja andra generationen av Schengens informationssystem (SIS II), som inrättats genom Europaparlamentets och rådets förordning (EU) 2018/1862 ([21]), underrättelser och annan tillgänglig objektiv information som kan vara nödvändig för att avgöra om den berörda personen är lämplig för att arbeta i den befattning för vilken den kritiska entiteten har begärt en bakgrundskontroll.

(33) En mekanism för anmälan av vissa incidenter bör inrättas för att göra det möjligt för de behöriga myndigheterna att reagera snabbt och ändamålsenligt på incidenter och få en heltäckande bild av verkningarna, arten och de möjliga konsekvenserna av samt orsaken till incidenter som de kritiska entiteterna hanterar. De kritiska entiteterna bör utan onödigt dröjsmål lämna in en anmälan till de behöriga myndigheterna om incidenter som medför en betydande störning eller kan medföra en betydande störning av tillhandahållandet av samhällsviktiga tjänster. Om detta inte är operativt omöjligt bör de kritiska entiteterna lämna in en första anmälan senast 24 timmar efter det att de har fått kännedom om en incident. Den första anmälan bör endast innehålla den information som är absolut nödvändig för att göra den behöriga myndigheten medveten om incidenten och för att den kritiska entiteten vid behov ska kunna söka hjälp. En sådan anmälan bör om möjligt innehålla information om den förmodade orsaken till incidenten. Medlemsstaterna bör säkerställa att kravet på att lämna in denna första anmälan inte avleder den kritiska entitetens resurser från verksamhet som rör incidenthantering, vilken bör prioriteras. Den första anmälan bör i förekommande fall åtföljas av en detaljerad rapport senast en månad efter incidenten. Den detaljerade rapporten bör komplettera den första anmälan och ge en mer komplett bild av incidenten.

(34) Standardisering bör förbli en i första hand marknadsdriven process. Det kan dock fortfarande finnas situationer där det är lämpligt att kräva överensstämmelse med specificerade standarder. Medlemsstaterna bör, när så är användbart, uppmuntra användning av europeiska och internationella standarder och tekniska specifikationer som är relevanta för åtgärder för säkerhet och motståndskraft som är tillämpliga på kritiska entiteter.

(35) Kritiska entiteter bedriver i allmänhet sin verksamhet inom ramen för ett allt mer sammankopplat nätverk av tillhandahållande av tjänster och infrastruktur och tillhandahåller ofta samhällsviktiga tjänster i mer än en medlemsstat, men vissa av dessa kritiska entiteter har särskild betydelse för unionen och den inre marknaden eftersom de tillhandahåller samhällsviktiga tjänster till eller i minst sex medlemsstater, och kan därför omfattas av särskilt stöd på unionsnivå. Därför bör det fastställas regler om rådgivande uppdrag med avseende på sådana kritiska entiteter av särskild europeisk betydelse. Dessa regler påverkar inte de regler om tillsyn och kontroll av efterlevnad som fastställs i detta direktiv.

(36) På motiverad begäran från kommissionen eller en eller flera medlemsstater till eller i vilka den samhällsviktiga tjänsten tillhandahålls, och om det krävs ytterligare upplysningar för att man ska kunna ge råd till en kritisk entitet avseende uppfyllandet av dess skyldigheter enligt detta direktiv eller för att man ska kunna bedöma huruvida en kritisk entitet av särskild europeisk betydelse uppfyller dessa skyldigheter, bör den medlemsstat som har identifierat en kritisk entitet av särskild europeisk betydelse som en kritisk entitet förse kommissionen med viss information i enlighet med detta direktiv. Kommissionen bör, i samförstånd med den medlemsstat som har identifierat den kritiska entiteten av särskild europeisk betydelse som en kritisk entitet, kunna anordna ett rådgivande uppdrag för att bedöma de åtgärder som den entiteten har infört. För att säkerställa att sådana rådgivande uppdrag utförs korrekt bör kompletterande regler fastställas, särskilt om hur de rådgivande uppdragen ska anordnas och genomföras, de uppföljande åtgärder som ska vidtas och vilka skyldigheter de berörda kritiska entiteterna av särskild europeisk betydelse har. Utan att det påverkar skyldigheten för den medlemsstat där det rådgivande

([19]) Rådets rambeslut 2009/315/RIF av den 26 februari 2009 om organisationen av medlemsstaternas utbyte av uppgifter ur kriminalregistret och uppgifternas innehåll (EUT L 93, 7.4.2009, s. 23).

([20]) Europaparlamentets och rådets förordning (EU) 2019/816 av den 17 april 2019 om inrättande av ett centraliserat system för identifiering av medlemsstater som innehar uppgifter om fällande domar mot tredjelandsmedborgare och statslösa personer (Ecris-TCN) för att komplettera det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister och om ändring av förordning (EU) 2018/1726 (EUT L 135, 22.5.2019, s. 1).

([21]) Europaparlamentets och rådets förordning (EU) 2018/1862 av den 28 november 2018 om inrättande, drift och användning av Schengens informationssystem (SIS) på området polissamarbete och straffrättsligt samarbete, om ändring och upphävande av rådets beslut 2007/533/RIF och om upphävande av Europaparlamentets och rådets förordning (EG) nr 1986/2006 och kommissionens beslut 2010/261/EU (EUT L 312, 7.12.2018, s. 56).

uppdraget genomförs och för den berörda kritiska entiteten att följa reglerna i detta direktiv, bör det rådgivande uppdraget genomföras i enlighet med de närmare föreskrifterna i den medlemsstatens rätt, till exempel om de exakta villkor som ska vara uppfyllda för att få åtkomst till relevanta lokaler eller handlingar och om rättslig prövning. Särskild expertis som behövs för sådana rådgivande uppdrag skulle i förekommande fall kunna begäras via Centrumet för samordning av katastrofberedskap, som inrättats genom Europaparlamentets och rådets beslut nr 1313/2013/EU ([22]).

(37) För att ge kommissionen stöd och underlätta samarbete mellan medlemsstaterna och utbyte av information, inbegripet bästa praxis, i frågor som rör detta direktiv bör det inrättas en grupp för kritiska entiteters motståndskraft, som kommissionens expertgrupp. Medlemsstaterna bör sträva efter att säkerställa att de utsedda företrädarna från deras behöriga myndigheter i gruppen för kritiska entiteters motståndskraft samarbetar ändamålsenligt och effektivt, inbegripet genom att när så är lämpligt utse företrädare med säkerhetsgodkännande. Gruppen för kritiska entiteters motståndskraft bör inleda sitt arbete så snart som möjligt, för att erbjuda ytterligare möjligheter till lämpligt samarbete under införlivandeperioden för detta direktiv. Gruppen för kritiska entiteters motståndskraft bör samverka med andra relevanta sektorsspecifika expertgrupper.

(38) Gruppen för kritiska entiteters motståndskraft bör samarbeta med den samarbetsgrupp som inrättats enligt direktiv (EU) 2022/2555 för att stödja en övergripande ram för cybermotståndskraft och icke-cyberrelaterad motståndskraft för kritiska entiteter. Gruppen för kritiska entiteters motståndskraft och den samarbetsgrupp som inrättats enligt direktiv (EU) 2022/2555 bör föra en regelbunden dialog för att främja samarbete mellan de behöriga myndigheterna enligt det här direktivet och de behöriga myndigheterna enligt direktiv (EU) 2022/2555 och för att underlätta utbyte av information, särskilt i frågor som är relevanta för båda grupperna.

(39) För att uppnå målen för detta direktiv och utan att det påverkar medlemsstaternas och de kritiska entiteternas rättsliga ansvar att säkerställa efterlevnad av sina respektive skyldigheter enligt detta direktiv bör kommissionen, när den anser att det är lämpligt, ge stöd till behöriga myndigheter och kritiska entiteter för att underlätta deras efterlevnad av respektive skyldigheter. När kommissionen ger stöd till medlemsstater och kritiska entiteter i genomförandet av skyldigheter enligt detta direktiv bör den utgå från befintliga strukturer och verktyg, exempelvis inom ramen för unionens civilskyddsmekanism som inrättats genom beslut nr 1313/2013/EU, och det europeiska referensnätverket för skydd av kritisk infrastruktur. Dessutom bör den informera medlemsstaterna om tillgängliga resurser på unionsnivå, såsom Fonden för inre säkerhet, som inrättats genom Europaparlamentets och rådets förordning (EU) 2021/1149 ([23]), Horisont Europa, som inrättats genom Europaparlamentets och rådets förordning (EU) 2021/695 ([24]), eller andra instrument som är relevanta för kritiska entiteters motståndskraft.

(40) Medlemsstaterna bör säkerställa att deras behöriga myndigheter har vissa särskilda befogenheter att tillämpa och kontrollera efterlevnaden av detta direktiv på ett korrekt sätt med avseende på kritiska entiteter, när dessa entiteter omfattas av deras jurisdiktion i enlighet med vad som fastställs i detta direktiv. Dessa befogenheter bör särskilt omfatta befogenhet att utföra inspektioner och revisioner, befogenhet att utöva tillsyn, befogenhet att kräva att kritiska entiteter ska lämna information och bevis som rör de åtgärder de har vidtagit för att uppfylla sina skyldigheter och, vid behov, befogenhet att utfärda föreläggande om att avhjälpa konstaterade överträdelser. När medlemsstaterna utfärdar sådana föreläggande bör de inte kräva åtgärder som går utöver vad som är nödvändigt och proportionerligt för att säkerställa att den berörda kritiska entiteten uppfyller skyldigheterna, med beaktande av, i synnerhet, överträdelsens allvarlighetsgrad och den berörda kritiska entitetens ekonomiska kapacitet. Mer generellt bör dessa befogenheter åtföljas av lämpliga och effektiva skyddsåtgärder som ska fastställas i nationell rätt i enlighet

([22]) Europaparlamentets och rådets beslut nr 1313/2013/EU av den 17 december 2013 om en civilskyddsmekanism för unionen (EUT L 347, 20.12.2013, s. 924).

([23]) Europaparlamentets och rådets förordning (EU) 2021/1149 av den 7 juli 2021 om inrättande av Fonden för inre säkerhet (EUT L 251, 15.7.2021, s. 94).

([24]) Europaparlamentets och rådets förordning (EU) 2021/695 av den 28 april 2021 om inrättande av Horisont Europa – ramprogrammet för forskning och innovation, om fastställande av dess regler för deltagande och spridning och om upphävande av förordningarna (EU) nr 1290/2013 och (EU) nr 1291/2013 (EUT L 170, 12.5.2021, s. 1).

med Europeiska unionens stadga om de grundläggande rättigheterna. När de behöriga myndigheterna enligt detta direktiv bedömer om en kritisk entitet uppfyller sina skyldigheter enligt detta direktiv bör de kunna begära att de behöriga myndigheterna enligt direktiv (EU) 2022/2555 utövar sina tillsyns- och efterlevnadskontrollbefogenheter med avseende på en entitet enligt det direktivet som har identifierats som en kritisk entitet enligt det här direktivet. De behöriga myndigheterna enligt det här direktivet och de behöriga myndigheterna enligt direktiv (EU) 2022/2555 bör samarbeta och utbyta information för detta ändamål.

(41) I syfte att tillämpa detta direktiv på ett ändamålsenligt och enhetligt sätt bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen med avseende på att komplettera detta direktiv genom att upprätta en förteckning över samhällsviktiga tjänster. Denna förteckning bör användas av de behöriga myndigheterna för att genomföra medlemsstaternas riskbedömningar och identifiera kritiska entiteter enligt detta direktiv. Mot bakgrund av den minimiharmoniseringsansats som föreskrivs i detta direktiv är denna förteckning icke uttömmande och medlemsstaterna kan komplettera den med ytterligare samhällsviktiga tjänster på nationell nivå för att ta hänsyn till nationella särdrag vid tillhandahållandet av samhällsviktiga tjänster. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning ([25]). För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter erhåller Europaparlamentet och rådet alla handlingar samtidigt som medlemsstaternas experter, och deras experter ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.

(42) För att säkerställa enhetliga villkor för genomförandet av detta direktiv, bör kommissionen tilldelas genomförandebefogenheter. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ([26]).

(43) Eftersom målen för detta direktiv, nämligen att säkerställa att tjänster som är nödvändiga för att upprätthålla viktiga samhällsfunktioner eller central ekonomisk verksamhet tillhandahålls på ett obehindrat sätt på den inre marknaden och att stärka motståndskraften hos kritiska entiteter som tillhandahåller sådana tjänster, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens effekter, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går detta direktiv inte utöver vad som är nödvändigt för att uppnå dessa mål.

(44) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([27]) och avgav ett yttrande den 11 augusti 2021.

(45) Direktiv 2008/114/EG bör därför upphävas.

([25]) EUT L 123, 12.5.2016, s. 1.
([26]) Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).
([27]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Innehåll och tillämpningsområde

1. I detta direktiv

a) fastställs skyldigheter för medlemsstaterna att vidta särskilda åtgärder som syftar till att säkerställa att tjänster som är nödvändiga för att upprätthålla viktiga samhällsfunktioner eller central ekonomisk verksamhet inom tillämpningsområdet för artikel 114 i EUF-fördraget tillhandahålls på ett obehindrat sätt på den inre marknaden, särskilt skyldigheter för att identifiera kritiska entiteter samt för att stödja kritiska entiteter i uppfyllandet av de skyldigheter som åläggs dem,

b) fastställs skyldigheter för kritiska entiteter som syftar till att stärka deras motståndskraft och förmåga att tillhandahålla tjänster som avses i led a på den inre marknaden,

c) fastställs regler

i) om tillsyn av kritiska entiteter,

ii) om efterlevnadskontroll,

iii) för identifiering av kritiska entiteter av särskild europeisk betydelse samt om rådgivande uppdrag för att bedöma de åtgärder som sådana entiteter har infört för att uppfylla sina skyldigheter enligt kapitel III,

d) inrättas gemensamma förfaranden för samarbete och rapportering om tillämpningen av detta direktiv,

e) fastställs åtgärder i syfte att uppnå en hög grad av motståndskraft för kritiska entiteter, för att säkerställa tillhandahållande av samhällsviktiga tjänster i unionen och förbättra den inre marknadens funktionssätt.

2. Detta direktiv ska inte vara tillämpligt på frågor som omfattas av direktiv (EU) 2022/2555, utan att detta påverkar tillämpningen av artikel 8 i det här direktivet. Med beaktande av förhållandet mellan kritiska entiteters fysiska säkerhet och cybersäkerhet ska medlemsstaterna säkerställa att det här direktivet och direktiv (EU) 2022/2555 genomförs på ett samordnat sätt.

3. Om det enligt bestämmelser i sektorsspecifika unionsrättsakter krävs att kritiska entiteter ska vidta åtgärder för att stärka sin motståndskraft och om de kraven erkänns av medlemsstaterna som åtminstone likvärdiga med de motsvarande skyldigheter som fastställs i detta direktiv, ska de berörda bestämmelserna i detta direktiv, inbegripet de bestämmelser om tillsyn och efterlevnadskontroll som fastställs i kapitel VI, inte vara tillämpliga.

4. Utan att det påverkar tillämpningen av artikel 346 i EUF-fördraget ska information som är konfidentiell enligt unionsregler eller nationella regler, såsom regler om affärshemligheter, utbytas med kommissionen och andra relevanta myndigheter i enlighet med detta direktiv endast när sådant utbyte är nödvändigt för att tillämpa detta direktiv. Den information som utbyts ska begränsas till vad som är relevant och proportionerligt för ändamålet med utbytet. Vid informationsutbytet ska informationens konfidentialitet och kritiska entiteters säkerhetsintressen och kommersiella intressen bevaras samtidigt som medlemsstaternas säkerhet respekteras.

5. Detta direktiv påverkar inte medlemsstaternas ansvar att skydda den nationella säkerheten och försvaret eller deras befogenhet att skydda andra väsentliga statliga funktioner, inbegripet att säkerställa statens territoriella integritet och upprätthålla lag och ordning.

6. Detta direktiv är inte tillämpligt på offentliga förvaltningsentiteter som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet utredning, upptäckt och lagföring av brott.

7. Medlemsstaterna får besluta att artikel 11 och kapitlen III, IV och VI, helt eller delvis, inte är tillämpliga på särskilda kritiska entiteter som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet utredning, upptäckt och lagföring av brott, eller som uteslutande tillhandahåller tjänster till de offentliga förvaltningsentiteter som avses i punkt 6 i den här artikeln.

8. De skyldigheter som fastställs i detta direktiv får inte medföra tillhandahållande av information vars utlämnande skulle strida mot väsentliga intressen i fråga om medlemsstaternas nationella säkerhet, allmänna säkerhet eller försvar.

9. Detta direktiv påverkar inte tillämpningen av unionsrätt om skydd av personuppgifter, i synnerhet Europaparlamentets och rådets förordning (EU) 2016/679 ([28]) och Europaparlamentets och rådets direktiv 2002/58/EG ([29]).

Artikel 2

Definitioner

I detta direktiv gäller följande definitioner:

1. *kritisk entitet*: en offentlig eller privat entitet som har identifierats av en medlemsstat i enlighet med artikel 6 som tillhörande en av de kategorier som anges i den tredje kolumnen i tabellen i bilagan.

2. *motståndskraft*: en kritisk entitets förmåga att förebygga, skydda mot, reagera på, stå emot, begränsa, absorbera, anpassa sig till och återhämta sig från en incident.

3. *incident*: varje händelse som kan medföra en betydande störning, eller som medför en störning, av tillhandahållandet av en samhällsviktig tjänst, inbegripet när den påverkar de nationella system som skyddar rättsstatens principer.

4. *kritisk infrastruktur*: en tillgång, en anläggning, utrustning, ett nätverk eller ett system, eller en del av en tillgång, en anläggning, utrustning, ett nätverk eller ett system, som krävs för tillhandahållandet av en samhällsviktig tjänst.

5. *samhällsviktig tjänst*: en tjänst som är avgörande för att upprätthålla viktiga samhällsfunktioner, ekonomisk verksamhet, folkhälsa och allmän säkerhet, eller miljön.

6. *risk*: risk för förlust eller störning orsakad av en incident, som ska uttryckas som en kombination av omfattningen av förlusten eller störningen och sannolikheten för att incidenten inträffar.

7. *riskbedömning*: den övergripande processen för att fastställa arten och omfattningen av en risk genom att identifiera och analysera potentiella relevanta hot, sårbarheter och faror som skulle kunna leda till en incident och genom att utvärdera den potentiella förlusten eller störningen i samband med tillhandahållandet av en samhällsviktig tjänst till följd av den incidenten.

8. *standard*: en standard enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EU) nr 1025/2012 ([30]).

([28]) Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

([29]) Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

([30]) Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG (EUT L 316, 14.11.2012, s. 12).

9. *teknisk specifikation*: en teknisk specifikation enligt definitionen i artikel 2.4 i förordning (EU) nr 1025/2012.

10. *offentlig förvaltningsentitet*: en entitet som erkänts som sådan i en medlemsstat enligt nationell rätt, med undantag för rättsväsendet, parlament och centralbanker, och som uppfyller följande kriterier:

a) Den har inrättats för att tillgodose behov i det allmännas intresse och har inte industriell eller kommersiell karaktär.

b) Den har ställning som juridisk person eller har lagstadgad rätt att agera för en annan entitet som har ställning som juridisk person.

c) Den finansieras till största delen av statliga myndigheter eller av andra offentligrättsliga organ på central nivå, står under administrativ tillsyn av dessa myndigheter eller organ, eller har ett förvaltnings-, lednings- eller tillsynsorgan där mer än hälften av ledamöterna utses av statliga myndigheter eller av andra offentligrättsliga organ på central nivå.

d) Den har befogenhet att rikta administrativa eller reglerande beslut till fysiska eller juridiska personer som påverkar deras rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital.

Artikel 3

Minimiharmonisering

Detta direktiv hindrar inte medlemsstaterna från att anta eller behålla bestämmelser i nationell rätt som syftar till att uppnå en högre grad av motståndskraft för kritiska entiteter, förutsatt att sådana bestämmelser står i överensstämmelse med medlemsstaternas förpliktelser enligt unionsrätten.

KAPITEL II

NATIONELLA RAMAR FÖR KRITISKA ENTITETERS MOTSTÅNDSKRAFT

Artikel 4

Strategi för kritiska entiteters motståndskraft

1. Efter ett samråd som, i den mån det är praktiskt möjligt, ska vara öppet för berörda parter ska varje medlemsstat senast den 17 januari 2026 anta en strategi för att stärka kritiska entiteters motståndskraft (*strategin*). Strategin ska innehålla strategiska mål och policyåtgärder, som bygger på relevanta befintliga nationella och sektorsspecifika strategier, planer eller liknande dokument, för att uppnå och upprätthålla en hög grad av motståndskraft hos kritiska entiteter, och ska åtminstone omfatta de sektorer som anges i bilagan.

2. Varje strategi ska innehålla åtminstone följande delar:

a) Strategiska mål och prioriteringar för att stärka kritiska entiteters övergripande motståndskraft, med beaktande av gränsöverskridande och sektorsöverskridande beroenden och ömsesidiga beroenden.

b) En styrningsram för att uppnå de strategiska målen och prioriteringarna, inklusive en beskrivning av rollerna och ansvarsområdena för de olika myndigheter, kritiska entiteter och andra parter som deltar i genomförandet av strategin.

c) En beskrivning av de åtgärder som är nödvändiga för att stärka kritiska entiteters övergripande motståndskraft, inklusive en beskrivning av den riskbedömning som avses i artikel 5.

d) En beskrivning av den process genom vilken kritiska entiteter identifieras.

e) En beskrivning av processen till stöd för kritiska entiteter i enlighet med detta kapitel, inbegripet åtgärder för att förbättra samarbetet mellan, å ena sidan den offentliga sektorn och, å andra sidan, den privata sektorn och offentliga och privata entiteter.

f) En förteckning över de viktigaste myndigheter och berörda parter som inte är kritiska entiteter men som deltar i genomförandet av strategin.

g) En policyram för samordning mellan de behöriga myndigheterna enligt detta direktiv och de behöriga myndigheterna enligt direktiv (EU) 2022/2555 för att dela information om cybersäkerhetsrisker, cyberhot och cyberincidenter och icke-cyberrelaterade risker, hot och incidenter och utföra tillsynsuppgifter.

h) En beskrivning av de åtgärder som redan har införts för att underlätta genomförandet av skyldigheter enligt kapitel III i detta direktiv för små och medelstora företag i den mening som avses i bilagan till kommissionens rekommendation 2003/361/EG ([31]) som medlemsstaten i fråga har identifierat som kritiska entiteter.

Efter ett samråd som, i den mån det är praktiskt möjligt, är öppet för berörda parter ska medlemsstaterna uppdatera sina strategier minst vart fjärde år.

3. Medlemsstaterna ska meddela kommissionen sina strategier och betydande uppdateringar av dem inom tre månader efter det att de har antagits.

Artikel 5

Riskbedömning av medlemsstaterna

1. Kommissionen ges befogenhet att anta en delegerad akt i enlighet med artikel 23 senast den 17 november 2023 för att komplettera detta direktiv genom att upprätta en icke uttömmande förteckning över samhällsviktiga tjänster inom de sektorer och undersektorer som anges i bilagan. De behöriga myndigheterna ska använda den förteckningen över samhällsviktiga tjänster för att göra en riskbedömning (*medlemsstaternas riskbedömning*) senast den 17 januari 2026 och därefter när så är nödvändigt och minst vart fjärde år. De behöriga myndigheterna ska använda medlemsstaternas riskbedömningar i syfte att identifiera kritiska entiteter i enlighet med artikel 6 och bistå de kritiska entiteterna med att vidta åtgärder enligt artikel 13.

Medlemsstaternas riskbedömningar ska innehålla en redogörelse för relevanta risker för naturolyckor och risker orsakade av människan, inbegripet risker av sektorsövergripande eller gränsöverskridande slag, olyckor, naturkatastrofer, hot mot folkhälsan och hybridhot eller andra antagonistiska hot, inklusive terroristbrott enligt Europaparlamentets och rådets direktiv (EU) 2017/541 ([32]).

2. När medlemsstaternas riskbedömningar görs ska medlemsstaterna åtminstone ta hänsyn till följande:

a) Den allmänna riskbedömning som har utförts enligt artikel 6.1 i beslut nr 1313/2013/EU.

b) Andra relevanta riskbedömningar som har utförts i enlighet med kraven i relevanta sektorsspecifika unionsrättsakter, inbegripet Europaparlamentets och rådets förordningar (EU) 2017/1938 ([33]) och (EU) 2019/941 ([34]) och Europaparlamentets och rådets direktiv 2007/60/EG ([35]) och 2012/18/EU ([36]).

([31]) Kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36).
([32]) Europaparlamentets och rådets direktiv (EU) 2017/541 av den 15 mars 2017 om bekämpande av terrorism, om ersättande av rådets rambeslut 2002/475/RIF och om ändring av rådets beslut 2005/671/RIF (EUT L 88, 31.3.2017, s. 6).
([33]) Europaparlamentets och rådets förordning (EU) 2017/1938 av den 25 oktober 2017 om åtgärder för att säkerställa försörjningstryggheten för gas och om upphävande av förordning (EU) nr 994/2010 (EUT L 280, 28.10.2017, s. 1).
([34]) Europaparlamentets och rådets förordning (EU) 2019/941 av den 5 juni 2019 om riskberedskap inom elsektorn och om upphävande av direktiv 2005/89/EG (EUT L 158, 14.6.2019, s. 1).
([35]) Europaparlamentets och rådets direktiv 2007/60/EG av den 23 oktober 2007 om bedömning och hantering av översvämningsrisker (EUT L 288, 6.11.2007, s. 27).
([36]) Europaparlamentets och rådets direktiv 2012/18/EU av den 4 juli 2012 om åtgärder för att förebygga och begränsa faran för allvarliga olyckshändelser där farliga ämnen ingår och om ändring och senare upphävande av rådets direktiv 96/82/EG (EUT L 197, 24.7.2012, s. 1).

c) De relevanta risker som uppstår till följd av den grad till vilken de sektorer som anges i bilagan är beroende av varandra, inbegripet den grad till vilken de är beroende av entiteter som är belägna i andra medlemsstater och tredjeländer, samt de konsekvenser en betydande störning i en sektor kan få för andra sektorer, inklusive eventuella betydande risker för medborgare och den inre marknaden.

d) Information om incidenter som har anmälts i enlighet med artikel 15.

Vid tillämpning av första stycket c ska medlemsstaterna samarbeta med de behöriga myndigheterna i andra medlemsstater och de behöriga myndigheterna i tredjeländer, när så är lämpligt.

3. Medlemsstaterna ska, i förekommande fall genom sina gemensamma kontaktpunkter, göra de relevanta delarna i medlemsstaternas riskbedömningar tillgängliga för de kritiska entiteter som de har identifierat i enlighet med artikel 6. Medlemsstaterna ska säkerställa att den information som tillhandahålls kritiska entiteter hjälper dem när de utför sina riskbedömningar enligt artikel 12 och vidtar åtgärder för att säkerställa sin motståndskraft enligt artikel 13.

4. Inom tre månader från det att en medlemsstats riskbedömning utfördes ska en medlemsstat förse kommissionen med relevant information om de typer av risker som har identifierats till följd av, och resultatet av, den medlemsstatens riskbedömning, per sektor och undersektor som anges bilagan.

5. Kommissionen ska i samarbete med medlemsstaterna utveckla en frivillig gemensam rapporteringsmall som kan användas för att uppfylla punkt 4.

Artikel 6

Identifiering av kritiska entiteter

1. Senast den 17 juli 2026 ska medlemsstaterna identifiera de kritiska entiteterna för de sektorer och undersektorer som anges i bilagan.

2. När en medlemsstat identifierar kritiska entiteter enligt punkt 1 ska den ta hänsyn till resultatet av sin riskbedömning samt sin strategi och tillämpa samtliga följande kriterier:

a) Entiteten tillhandahåller en eller flera samhällsviktiga tjänster.

b) Entiteten bedriver verksamhet, och dess kritiska infrastruktur är belägen, på denna medlemsstats territorium.

c) En incident skulle få betydande störande effekter, enligt vad som fastställs i enlighet med artikel 7.1, för entitetens tillhandahållande av en eller flera samhällsviktiga tjänster eller för tillhandahållandet av andra samhällsviktiga tjänster i de sektorer som anges i bilagan och som är beroende av den eller de samhällsviktiga tjänsterna.

3. Varje medlemsstat ska upprätta en förteckning över de kritiska entiteter som har identifierats enligt punkt 2 och säkerställa att dessa kritiska entiteter underrättas om att de har identifierats som kritiska entiteter inom en månad från identifieringen. Medlemsstaterna ska informera dessa kritiska entiteter om deras skyldigheter enligt kapitlen III och IV och om det datum från och med vilket dessa skyldigheter är tillämpliga på dem, utan att detta påverkar tillämpningen av artikel 8. Medlemsstaterna ska informera kritiska entiteter i de sektorer som anges i punkterna 3, 4 och 8 i tabellen i bilagan om att de inte har några skyldigheter enligt kapitlen III och IV såvida inte nationella åtgärder föreskriver något annat.

För de berörda kritiska entiteterna ska kapitel III vara tillämpligt från och med tio månader efter dagen för den underrättelse som avses i första stycket i denna punkt.

4. Medlemsstaterna ska säkerställa att deras behöriga myndigheter enligt detta direktiv underrättar de behöriga myndigheterna enligt direktiv (EU) 2022/2555 om identiteten på de kritiska entiteter som de har identifierat enligt denna artikel inom en månad från den identifieringen. Denna underrättelse ska, i tillämpliga fall, innehålla information om att de berörda kritiska entiteterna är entiteter i de sektorer som anges i punkterna 3, 4 och 8 i tabellen i bilagan till det här direktivet och inte har några skyldigheter enligt kapitlen III och IV i det här direktivet.

5. Medlemsstaterna ska när så är nödvändigt och minst vart fjärde år se över och när så är lämpligt uppdatera förteckningen över identifierade kritiska entiteter som avses i punkt 3. Om dessa uppdateringar leder till att ytterligare kritiska entiteter identifieras ska punkterna 3 och 4 tillämpas på dessa ytterligare kritiska entiteter. Dessutom ska medlemsstaterna säkerställa att entiteter som inte längre identifieras som kritiska entiteter till följd av en sådan uppdatering i god tid underrättas om detta och om att de inte längre omfattas av skyldigheterna enligt kapitel III från och med dagen för mottagandet av denna underrättelse.

6. Kommissionen ska i samarbete med medlemsstaterna utarbeta rekommendationer och icke-bindande riktlinjer för att stödja medlemsstaterna i arbetet med att identifiera kritiska entiteter.

Artikel 7

Betydande störande effekt

1. När medlemsstaterna fastställer om en störande effekt som avses i artikel 6.2 c är betydande, ska de beakta följande kriterier:

a) Antalet användare som är beroende av den samhällsviktiga tjänst som den berörda entiteten tillhandahåller.

b) Den grad till vilken andra sektorer och undersektorer som anges i bilagan är beroende av den samhällsviktiga tjänsten i fråga.

c) Vilken effekt incidenter skulle kunna ha på ekonomisk och samhällelig verksamhet, miljön, den allmänna säkerheten och tryggheten eller befolkningens hälsa, uttryckt i grad och varaktighet.

d) Entitetens marknadsandel på marknaden för den eller de berörda samhällsviktiga tjänsterna.

e) Det geografiska område som skulle kunna påverkas av en incident, inbegripet eventuella gränsöverskridande konsekvenser, med beaktande av den sårbarhet som är förknippad med graden av isolering för vissa typer av geografiska områden, såsom öregioner, avlägsna områden eller bergsområden.

f) Entitetens betydelse för upprätthållandet av en tillräcklig nivå på den samhällsviktiga tjänsten, med beaktande av tillgången till alternativa sätt för att tillhandahålla den samhällsviktiga tjänsten.

2. Efter identifieringen av de kritiska entiteterna enligt artikel 6.1 ska varje medlemsstat utan onödigt dröjsmål lämna följande information till kommissionen:

a) En förteckning över samhällsviktiga tjänster i den medlemsstaten, om det finns ytterligare samhällsviktiga tjänster jämfört med den förteckning över samhällsviktiga tjänster som avses i artikel 5.1.

b) Det antal kritiska entiteter som har identifierats för varje sektor och undersektor som anges i bilagan och för varje samhällsviktig tjänst.

c) Eventuella tröskelvärden som har tillämpats för att närmare fastställa ett eller flera av de kriterier som anges i punkt 1.

De tröskelvärden som avses i första stycket c får presenteras som sådana eller i aggregerad form.

Därefter ska medlemsstaterna lämna den information som avses i första stycket när så är nödvändigt och minst vart fjärde år.

3. Kommissionen ska efter samråd med den grupp för kritiska entiteters motståndskraft som avses i artikel 19 anta icke-bindande riktlinjer för att underlätta tillämpningen av de kriterier som avses i punkt 1 i den här artikeln, med beaktande av den information som avses i punkt 2 i den här artikeln.

Artikel 8

Kritiska entiteter inom sektorerna för bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur

Medlemsstaterna ska säkerställa att artikel 11 och kapitlen III, IV och VI inte är tillämpliga på kritiska entiteter som de har identifierat inom de sektorer som anges i punkterna 3, 4 och 8 i tabellen i bilagan. Medlemsstaterna får anta eller behålla bestämmelser i nationell rätt för att uppnå en högre grad av motståndskraft för dessa kritiska entiteter, förutsatt att dessa bestämmelser är förenliga med tillämplig unionsrätt.

Artikel 9

Behöriga myndigheter och gemensam kontaktpunkt

1. Varje medlemsstat ska utse eller inrätta en eller flera behöriga myndigheter som ansvariga för den korrekta tillämpningen och, vid behov, efterlevnadskontrollen avseende reglerna i detta direktiv på nationell nivå.

När det gäller de kritiska entiteterna inom de sektorer som anges i punkterna 3 och 4 i tabellen i bilagan till detta direktiv ska de behöriga myndigheterna i princip vara de behöriga myndigheter som avses i artikel 46 i förordning (EU) 2022/2554. När det gäller de kritiska entiteterna inom den sektor som anges i punkt 8 i tabellen i bilagan till detta direktiv ska de behöriga myndigheterna i princip vara de behöriga myndigheterna enligt direktiv (EU) 2022/2555. Medlemsstaterna får utse en annan behörig myndighet för de sektorer som anges i punkterna 3, 4 och 8 i tabellen i bilagan till det här direktivet i enlighet med befintliga nationella ramar.

Om medlemsstaterna utser eller inrättar mer än en behörig myndighet ska de tydligt fastställa uppgifterna för var och en av de berörda myndigheterna och säkerställa att de samarbetar effektivt för att fullgöra sina uppgifter enligt detta direktiv, inbegripet vad gäller utseendet av och verksamheten inom den gemensamma kontaktpunkt som avses i punkt 2.

2. Varje medlemsstat ska utse eller inrätta en gemensam kontaktpunkt, som ska ha en sambandsfunktion för att säkerställa gränsöverskridande samarbete med de gemensamma kontaktpunkterna i andra medlemsstater och den grupp för kritiska entiteters motståndskraft som avses i artikel 19 (*gemensam kontaktpunkt*). I förekommande fall ska en medlemsstat utse sin gemensamma kontaktpunkt inom en behörig myndighet. I förekommande fall får en medlemsstat föreskriva att dess gemensamma kontaktpunkt även ska ha en sambandsfunktion med kommissionen och säkerställa samarbete med tredjeländer.

3. De gemensamma kontaktpunkterna ska senast den 17 juli 2028, och därefter vartannat år, lämna en sammanfattande rapport till kommissionen och den grupp för kritiska entiteters motståndskraft som avses i artikel 19 om de anmälningar som de har mottagit, inklusive antalet anmälningar, de anmälda incidenternas art och vilka åtgärder som vidtagits i enlighet med artikel 15.3.

Kommissionen ska i samarbete med gruppen för kritiska entiteters motståndskraft utveckla en gemensam rapporteringsmall. De behöriga myndigheterna får på frivillig basis använda den gemensamma rapporteringsmallen för att lämna in de sammanfattande rapporter som avses i första stycket.

4. Varje medlemsstat ska säkerställa att dess behöriga myndighet och gemensamma kontaktpunkt har de befogenheter och tillräckliga ekonomiska, personella och tekniska resurser som krävs för att på ett effektivt och ändamålsenligt sätt fullgöra de uppgifter som de har ålagts.

5. Varje medlemsstat ska säkerställa att dess behöriga myndighet när så är lämpligt och i enlighet med unionsrätten och nationell rätt samråder och samarbetar med andra relevanta nationella myndigheter, inbegripet de som ansvarar för civilskydd, brottsbekämpning och skydd av personuppgifter, samt med kritiska entiteter och relevanta berörda parter.

6. Varje medlemsstat ska säkerställa att dess behöriga myndighet enligt detta direktiv samarbetar och utbyter information med de behöriga myndigheterna enligt direktiv 2022/2555 om cybersäkerhetsrisker, cyberhot och cyberincidenter och icke-cyberrelaterade risker, hot och incidenter som påverkar kritiska entiteter, inbegripet avseende relevanta åtgärder som har vidtagits av dess behöriga myndigheter och de behöriga myndigheterna enligt direktiv (EU) 2022/2555.

7. Inom tre månader från det att den behöriga myndigheten och den gemensamma kontaktpunkten har utsetts eller inrättats ska varje medlemsstat underrätta kommissionen om deras identitet och deras uppgifter och ansvarsområden enligt detta direktiv, deras kontaktuppgifter samt alla senare ändringar av dessa. Om medlemsstaterna har beslutat att utse en annan myndighet än de behöriga myndigheter som avses i punkt 1 andra stycket som behöriga myndigheter med avseende på de kritiska entiteterna i de sektorer som anges i punkterna 3, 4 och 8 i tabellen i bilagan ska de underrätta kommissionen om detta. Varje medlemsstat ska offentliggöra identiteten på dess behöriga myndighet och gemensamma kontaktpunkt.

8. Kommissionen ska offentliggöra en förteckning över de gemensamma kontaktpunkterna.

Artikel 10

Medlemsstaternas stöd till kritiska entiteter

1. Medlemsstaterna ska stödja kritiska entiteter för att stärka deras motståndskraft. Stödet får innefatta utveckling av vägledningsmaterial och metoder, stöd till anordnande av övningar för att testa deras motståndskraft och tillhandahållande av rådgivning och utbildning för kritiska entiteters personal. Utan att det påverkar tillämpningen av gällande regler för statligt stöd får medlemsstaterna tillhandahålla ekonomiska resurser till kritiska entiteter, om det är nödvändigt och motiverat av mål av allmänt intresse.

2. Varje medlemsstat ska säkerställa att dess behöriga myndighet samarbetar och utbyter information och god praxis med kritiska entiteter i de sektorer som anges i bilagan.

3. Medlemsstaterna ska underlätta frivillig informationsdelning mellan kritiska entiteter i frågor som omfattas av detta direktiv, i enlighet med unionsrätten och nationell rätt, särskilt i fråga om sekretessbelagd och känslig information, konkurrens och skydd av personuppgifter.

Artikel 11

Samarbete mellan medlemsstater

1. När så är lämpligt ska medlemsstaterna samråda med varandra om kritiska entiteter i syfte att säkerställa att detta direktiv tillämpas på ett konsekvent sätt. Sådana samråd ska äga rum i synnerhet med avseende på kritiska entiteter som

a) använder kritisk infrastruktur som är fysiskt sammankopplad mellan två eller flera medlemsstater,

b) ingår i företagsstrukturer som är sammankopplade eller sammanlänkade med kritiska entiteter i andra medlemsstater,

c) har identifierats som kritiska entiteter i en medlemsstat och tillhandahåller samhällsviktiga tjänster för eller i andra medlemsstater.

2. De samråd som avses i punkt 1 ska syfta till att stärka kritiska entiteters motståndskraft och, om möjligt, minska deras administrativa börda.

KAPITEL III

KRITISKA ENTITETERS MOTSTÅNDSKRAFT

Artikel 12

Riskbedömning av kritiska entiteter

1. Utan hinder av den tidsfrist som anges i artikel 6.3 andra stycket ska medlemsstaterna säkerställa att kritiska entiteter gör en riskbedömning inom nio månader från mottagandet av den underrättelse som avses i artikel 6.3 och därefter när det är nödvändigt och minst vart fjärde år, på grundval av medlemsstaternas riskbedömningar och andra relevanta informationskällor, för att bedöma alla relevanta risker som kan störa tillhandahållandet av deras samhällsviktiga tjänster (*riskbedömning av kritiska entiteter*).

2. Riskbedömningar av kritiska entiteter ska innehålla en redogörelse för alla relevanta risker för naturolyckor och risker orsakade av människan som skulle kunna leda till en incident, inbegripet risker av sektorsövergripande eller gränsöverskridande slag, olyckor, naturkatastrofer, hot mot folkhälsan och hybridhot samt andra antagonistiska hot, inklusive terroristbrott enligt direktiv (EU) 2017/541. En riskbedömning av kritiska entiteter ska beakta den grad till vilken andra sektorer som anges i bilagan är beroende av den samhällsviktiga tjänst som tillhandahålls av den kritiska entiteten och den grad till vilken den kritiska entiteten är beroende av samhällsviktiga tjänster som tillhandahålls av andra entiteter i sådana andra sektorer, inbegripet i angränsande medlemsstater och tredjeländer i förekommande fall.

Om en kritisk entitet, i enlighet med skyldigheter som föreskrivs i andra rättsakter, har gjort andra riskbedömningar eller utarbetat dokument som är relevanta för dess riskbedömning av kritiska entiteter får den använda dessa bedömningar och dokument för att uppfylla kraven i denna artikel. När den behöriga myndigheten utövar sina tillsynsfunktioner får den slå fast att en befintlig riskbedömning som gjorts av en kritisk entitet och som omfattar de risker och den beroendegrad som avses i första stycket i denna punkt helt eller delvis uppfyller skyldigheterna enligt denna artikel.

Artikel 13

Kritiska entiteters åtgärder för motståndskraft

1. Medlemsstaterna ska säkerställa att kritiska entiteter vidtar lämpliga och proportionella tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa sin motståndskraft, på grundval av den relevanta information som tillhandahålls av medlemsstaterna om medlemsstaternas riskbedömning samt resultatet av riskbedömningen av kritiska entiteter, inbegripet åtgärder som är nödvändiga för att

a) förhindra incidenter från att uppstå, med vederbörlig hänsyn till åtgärder för katastrofriskreducering och klimatanpassning,

b) säkerställa ett tillfredsställande fysiskt skydd av deras lokaler och kritiska infrastruktur, med vederbörlig hänsyn till exempelvis stängsel, barriärer, verktyg och rutiner för övervakning av områdesgränser, detektionsutrustning och åtkomstkontroller,

c) reagera på, stå emot och begränsa konsekvenserna av incidenter, med vederbörlig hänsyn till genomförandet av risk- och krishanteringsförfaranden och protokoll samt varningsrutiner,

d) återhämta sig från incidenter, med vederbörlig hänsyn till åtgärder för driftskontinuitet och identifiering av alternativa försörjningskedjor, för att återuppta tillhandahållandet av den samhällsviktiga tjänsten,

e) säkerställa en ändamålsenlig hantering av personalsäkerhet, med vederbörlig hänsyn till åtgärder såsom fastställande av kategorier av personal som utför kritiska funktioner, fastställande av åtkomsträttigheter till lokaler, kritisk infrastruktur och känslig information, inrättande av förfaranden för bakgrundskontroller i enlighet med artikel 14 och fastställande av de kategorier av personer som måste genomgå sådana bakgrundskontroller samt fastställande av lämpliga utbildningskrav och kvalifikationer,

f) öka medvetenheten om de åtgärder som anges i leden a–e hos berörd personal, med vederbörlig hänsyn till utbildningskurser, informationsmaterial och övningar.

Vid tillämpning av första stycket e ska medlemsstaterna säkerställa att kritiska entiteter beaktar externa tjänsteleverantörers personal vid fastställandet av kategorier av personal som utför kritiska funktioner.

2. Medlemsstaterna ska säkerställa att kritiska entiteter har och tillämpar en plan för motståndskraft eller ett eller flera likvärdiga dokument med en beskrivning av de åtgärder som vidtagits enligt punkt 1. Om kritiska entiteter har utarbetat dokument eller vidtagit åtgärder i enlighet med skyldigheter som anges i andra rättsakter som är relevanta för de åtgärder som avses i punkt 1 får de använda dessa dokument och åtgärder för att uppfylla kraven i denna artikel. När den behöriga myndigheten utövar sina tillsynsfunktioner får den slå fast att befintliga motståndskraftsstärkande åtgärder som vidtagits av en kritisk entitet och som på ett lämpligt och proportionerligt sätt adresserar de tekniska, säkerhetsmässiga och organisatoriska åtgärder som avses i punkt 1 helt eller delvis uppfyller skyldigheterna enligt denna artikel.

3. Medlemsstaterna ska säkerställa att varje kritisk entitet utser en sambandsansvarig eller motsvarande som kontaktpunkt med de berörda myndigheterna.

4. På begäran av den medlemsstat som identifierade den kritiska entiteten och med den berörda kritiska entitetens samtycke ska kommissionen anordna rådgivande uppdrag i enlighet med de arrangemang som fastställs i artikel 18.6, 18.8 och 18.9 för att tillhandahålla rådgivning för den berörda kritiska entiteten avseende uppfyllandet av dess skyldigheter enligt kapitel III. Det rådgivande uppdraget ska rapportera sina slutsatser till kommissionen, medlemsstaten och den berörda kritiska entiteten.

5. Kommissionen ska efter samråd med den grupp för kritiska entiteters motståndskraft som avses i artikel 19 anta icke-bindande riktlinjer för att närmare fastställa de tekniska, säkerhetsmässiga och organisatoriska åtgärder som får vidtas enligt punkt 1 i den här artikeln.

6. Kommissionen ska anta genomförandeakter för att fastställa de nödvändiga tekniska och metodrelaterade specifikationerna för tillämpningen av de åtgärder som avses i punkt 1 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 24.2.

Artikel 14

Bakgrundskontroller

1. Medlemsstaterna ska ange de villkor enligt vilka en kritisk entitet, i vederbörligen motiverade fall och med beaktande av medlemsstatens riskbedömning, får ansöka om bakgrundskontroller av personer som

a) innehar känsliga roller i eller till förmån för den kritiska entiteten, särskilt när det gäller den kritiska entitetens motståndskraft,

b) är bemyndigade att direkt eller på distans få tillgång till den kritiska entitetens lokaler eller dess informations- eller kontrollsystem, inbegripet när det gäller den kritiska entitetens säkerhet,

c) övervägs för rekrytering till tjänster som omfattas av de kriterier som anges i led a eller b.

2. De ansökningar som avses i punkt 1 i denna artikel ska bedömas inom en rimlig tidsram och hanteras i enlighet med nationell rätt och nationella förfaranden samt relevant och tillämplig unionsrätt, inbegripet förordning (EU) 2016/679 och Europaparlamentets och rådets direktiv (EU) 2016/680 ([37]). Bakgrundskontroller ska vara proportionella och strikt begränsade till vad som är nödvändigt. De ska utföras enbart i syfte att utvärdera en potentiell säkerhetsrisk för den berörda kritiska entiteten.

3. En bakgrundskontroll enligt punkt 1 ska åtminstone

a) bekräfta identiteten på den person som är föremål för bakgrundskontrollen,

b) kontrollera uppgifter ur kriminalregistret för den personen avseende brott som är relevanta för en viss tjänst.

När de utför bakgrundskontroller ska medlemsstaterna använda det europeiska informationssystemet för utbyte av uppgifter ur kriminalregister i enlighet med de förfaranden som fastställs i rambeslut 2009/315/RIF och, i förekommande och tillämpliga fall, förordning (EU) 2019/816 för att inhämta uppgifter ur kriminalregister som innehas av andra medlemsstater. De centralmyndigheter som avses i artikel 3.1 i rambeslut 2009/315/RIF och i artikel 3.5 i förordning (EU) 2019/816 ska besvara begäranden om sådana uppgifter inom tio arbetsdagar från och med den dag då begäran togs emot i enlighet med artikel 8.1 i rambeslut 2009/315/RIF.

([37]) Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89).

Artikel 15

Incidentanmälan

1. Medlemsstaterna ska säkerställa att kritiska entiteter utan onödigt dröjsmål lämnar in en anmälan till den behöriga myndigheten om incidenter som medför en betydande störning eller kan medföra en betydande störning i tillhandahållandet av samhällsviktiga tjänster. Medlemsstaterna ska säkerställa att de kritiska entiteterna, om det inte är operativt omöjligt för dem, lämnar in en första anmälan inom 24 timmar efter det att de har fått kännedom om en incident, åtföljd, i förekommande fall, av en detaljerad rapport senast en månad därefter. För att fastställa huruvida störningen är betydande ska i synnerhet följande parametrar tas i beaktande:

a) Antal och andel användare som berörs av störningen.

b) Störningens varaktighet.

c) Det geografiska område som påverkas av störningen, med beaktande av huruvida området är geografiskt isolerat.

Om en incident har eller kan ha en betydande påverkan på kontinuiteten i tillhandahållandet av samhällsviktiga tjänster i minst sex medlemsstater ska de behöriga myndigheterna i de medlemsstater som berörs av incidenten anmäla den incidenten till kommissionen.

2. De anmälningar som avses i punkt 1 första stycket ska omfatta all tillgänglig information som är nödvändig för att den behöriga myndigheten ska kunna förstå incidentens art, orsak och möjliga konsekvenser, inbegripet eventuell information som krävs för att kunna fastställa incidentens eventuella gränsöverskridande verkningar. Sådana anmälningar ska inte medföra ett ökat ansvar för de kritiska entiteterna.

3. På grundval av den information som en kritisk entitet lämnar i den anmälan som avses i punkt 1 ska den relevanta behöriga myndigheten via den gemensamma kontaktpunkten informera den gemensamma kontaktpunkten i andra medlemsstater som påverkas om incidenten har eller kan ha en betydande påverkan på kritiska entiteter och kontinuiteten i tillhandahållandet av samhällsviktiga tjänster i en eller flera andra medlemsstater.

Gemensamma kontaktpunkter som skickar eller tar emot information enligt första stycket ska i enlighet med unionsrätten eller nationell rätt behandla den informationen på ett sätt som respekterar dess konfidentialitet och skyddar den berörda kritiska entitetens säkerhet och kommersiella intressen.

4. Så snart som möjligt efter en anmälan enligt punkt 1 ska den berörda behöriga myndigheten ge den berörda kritiska entiteten relevant uppföljningsinformation, inklusive information som skulle kunna hjälpa den kritiska entiteten att reagera ändamålsenligt på incidenten i fråga. Medlemsstaterna ska informera allmänheten om de anser att det skulle ligga i allmänhetens intresse.

Artikel 16

Standarder

För att främja ett enhetligt genomförande av detta direktiv ska medlemsstaterna, när det är användbart och utan att föreskriva eller gynna användning av en viss typ av teknik, uppmuntra användningen av europeiska och internationellt erkända standarder och tekniska specifikationer som är relevanta för åtgärder för säkerhet och motståndskraft som är tillämpliga på kritiska entiteter.

KAPITEL IV

KRITISKA ENTITETER AV SÄRSKILD EUROPEISK BETYDELSE

Artikel 17

Identifiering av kritiska entiteter av särskild europeisk betydelse

1. En entitet ska betraktas som en kritisk entitet av särskild europeisk betydelse om

a) den har identifierats som en kritisk entitet enligt artikel 6.1,

b) den tillhandahåller samma eller liknande samhällsviktiga tjänster till eller i minst sex medlemsstater, och

c) den har mottagit en underrättelse enligt punkt 3 i denna artikel.

2. Medlemsstaterna ska säkerställa att en kritisk entitet, efter den underrättelse som avses i artikel 6.3, informerar sin behöriga myndighet om den tillhandahåller samhällsviktiga tjänster till eller i minst sex medlemsstater. I ett sådant fall ska medlemsstaterna säkerställa att den kritiska entiteten underrättar sin behöriga myndighet om de samhällsviktiga tjänster som den tillhandahåller till eller i dessa medlemsstater och till eller i vilka medlemsstater den tillhandahåller sådana samhällsviktiga tjänster. Medlemsstaterna ska utan onödigt dröjsmål underrätta kommissionen om identiteten på dessa kritiska entiteter och den information som de tillhandahåller enligt denna punkt.

Kommissionen ska samråda med den behöriga myndigheten i den medlemsstat som identifierat en kritisk entitet som avses i första stycket, den behöriga myndigheten i andra berörda medlemsstater samt den kritiska entiteten i fråga. Vid dessa samråd ska varje medlemsstat informera kommissionen om den bedömer att de tjänster som den kritiska entiteten tillhandahåller den medlemsstaten är samhällsviktiga tjänster.

3. Om kommissionen, på grundval av de samråd som avses i punkt 2 i denna artikel, fastställer att den berörda kritiska entiteten tillhandahåller samhällsviktiga tjänster till eller i fler än sex medlemsstater, ska kommissionen underrätta den berörda entiteten, genom dess behöriga myndighet, om att den betraktas som en kritisk entitet av särskild europeisk betydelse och informera den kritiska entiteten om dess skyldigheter enligt detta kapitel samt från och med vilken dag dessa skyldigheter är tillämpliga på den. När kommissionen underrättar den behöriga myndigheten om sitt beslut att betrakta en kritisk entitet som en kritisk entitet av särskild europeisk betydelse ska den behöriga myndigheten utan onödigt dröjsmål vidarebefordra den underrättelsen till den kritiska entiteten.

4. Detta kapitel ska tillämpas på den berörda kritiska entiteten av särskild europeisk betydelse från och med dagen för mottagandet av den underrättelse som avses i punkt 3 i denna artikel.

Artikel 18

Rådgivande uppdrag

1. På begäran av den medlemsstat som har identifierat en kritisk entitet av särskild europeisk betydelse som en kritisk entitet enligt artikel 6.1 ska kommissionen anordna ett rådgivande uppdrag för att bedöma de åtgärder som den kritiska entiteten har infört för att uppfylla sina skyldigheter enligt kapitel III.

2. På eget initiativ eller på begäran av en eller flera medlemsstater till eller i vilka den samhällsviktiga tjänsten tillhandahålls, och under förutsättning att den medlemsstat som har identifierat en kritisk entitet av särskild europeisk betydelse som en kritisk entitet enligt artikel 6.1 samtycker till detta, ska kommissionen anordna ett sådant rådgivande uppdrag som avses i punkt 1 i den här artikeln.

3. På motiverad begäran från kommissionen eller från en eller flera medlemsstater till eller i vilka den samhällsviktiga tjänsten tillhandahålls, ska den medlemsstat som har identifierat en kritisk entitet av särskild europeisk betydelse som en kritisk entitet enligt artikel 6.1 tillhandahålla kommissionen följande:

a) Relevanta delar av riskbedömningen av kritiska entiteter.

b) En förteckning över relevanta åtgärder som vidtagits i enlighet med artikel 13.

c) Tillsyns- eller efterlevnadskontrollåtgärder, inbegripet bedömningar av efterlevnad eller utfärdade förelägganden, som dess behöriga myndighet har vidtagit enligt artiklarna 21 och 22 med avseende på den kritiska entiteten.

4. Det rådgivande uppdraget ska rapportera sina slutsatser till kommissionen, den medlemsstat som har identifierat en kritisk entitet av särskild europeisk betydelse som en kritisk entitet enligt artikel 6.1, de medlemsstater till eller i vilka den samhällsviktiga tjänsten tillhandahålls och den berörda kritiska entiteten inom tre månader efter det att det rådgivande uppdraget har avslutats.

De medlemsstater till eller i vilka den samhällsviktiga tjänsten tillhandahålls ska analysera den rapport som avses i första stycket och, om så är nödvändigt, ge kommissionen råd om huruvida den berörda kritiska entiteten av särskild europeisk betydelse uppfyller sina skyldigheter enligt kapitel III och, i förekommande fall, vilka åtgärder som skulle kunna vidtas för att förbättra den kritiska entitetens motståndskraft.

Kommissionen ska på grundval av den rådgivning som avses i andra stycket i denna punkt meddela sitt yttrande till den medlemsstat som har identifierat en kritisk entitet av särskild europeisk betydelse som en kritisk entitet enligt artikel 6.1, de medlemsstater till eller i vilka den samhällsviktiga tjänsten tillhandahålls och den kritiska entiteten om huruvida den kritiska entiteten uppfyller sina skyldigheter enligt kapitel III och i förekommande fall vilka åtgärder som skulle kunna vidtas för att förbättra den kritiska entitetens motståndskraft.

Den medlemsstat som har identifierat en kritisk entitet av särskild europeisk betydelse som en kritisk entitet enligt artikel 6.1 ska säkerställa att dess behöriga myndighet och den berörda kritiska entiteten tar vederbörlig hänsyn till det yttrande som avses i tredje stycket i den här punkten och lämna information till kommissionen och de medlemsstater till eller i vilka den samhällsviktiga tjänsten tillhandahålls om åtgärder som den har vidtagit i enlighet med det yttrandet.

5. Varje rådgivande uppdrag ska bestå av experter från den medlemsstat där den kritiska entiteten av särskild europeisk betydelse är belägen, experter från de medlemsstater till eller i vilka den samhällsviktiga tjänsten tillhandahålls och företrädare för kommissionen. Dessa medlemsstater får föreslå kandidater för att delta i ett rådgivande uppdrag. Kommissionen ska, efter samråd med den medlemsstat som har identifierat en kritisk entitet av särskild europeisk betydelse som en kritisk entitet enligt artikel 6.1, välja ut och utnämna medlemmarna i varje rådgivande uppdrag i enlighet med deras yrkesmässiga kapacitet och, när så är möjligt, säkerställa en geografiskt balanserad representation från alla dessa medlemsstater. Medlemmarna i det rådgivande uppdraget ska när så krävs ha ett giltigt och lämpligt säkerhetsgodkännande. Kommissionen ska täcka kostnaderna i samband med deltagandet i rådgivande uppdrag.

Kommissionen ska anordna programmet för varje rådgivande uppdrag i samråd med deltagarna i det rådgivande uppdraget i fråga och i överenskommelse med den medlemsstat som har identifierat en kritisk entitet av särskild europeisk betydelse som en kritisk entitet enligt artikel 6.1.

6. Kommissionen ska anta en genomförandeakt om regler för förfaranden för begäranden om att anordna rådgivande uppdrag, för hantering av sådana begäranden, för genomförande av och rapportering från rådgivande uppdrag och för hantering av kommunikationen av kommissionens yttrande som avses i punkt 4 tredje stycket i denna artikel samt om de åtgärder som vidtagits, med vederbörlig hänsyn tagen till de berörda uppgifternas konfidentialitet och kommersiella känslighet. Denna genomförandeakt ska antas i enlighet med det granskningsförfarande som avses i artikel 24.2.

7. Medlemsstaterna ska säkerställa att kritiska entiteter av särskild europeisk betydelse ger det rådgivande uppdraget åtkomst till uppgifter, system och anläggningar som rör tillhandahållandet av deras samhällsviktiga tjänster som är nödvändiga för utförandet av det berörda rådgivande uppdraget.

8. Rådgivande uppdrag ska genomföras i enlighet med tillämplig nationell rätt i den medlemsstat där de äger rum, med respekt för den medlemsstatens ansvar för den nationella säkerheten och skyddet av sina säkerhetsintressen.

9. När kommissionen anordnar rådgivande uppdrag ska den ta hänsyn till rapporterna från inspektioner som kommissionen har genomfört enligt förordningarna (EG) nr 725/2004 och (EG) nr 300/2008 och till rapporterna från övervakning som kommissionen har utfört enligt direktiv 2005/65/EG med avseende på den berörda kritiska entiteten.

10. Kommissionen ska underrätta den grupp för kritiska entiteters motståndskraft som avses i artikel 19 när ett rådgivande uppdrag anordnas. Den medlemsstat där det rådgivande uppdraget ägde rum och kommissionen ska även informera gruppen för kritiska entiteters motståndskraft om de viktigaste resultaten av det rådgivande uppdraget och de tillvaratagna erfarenheterna i syfte att underlätta ett ömsesidigt lärande.

KAPITEL V

SAMARBETE OCH RAPPORTERING

Artikel 19

Gruppen för kritiska entiteters motståndskraft

1. En grupp för kritiska entiteters motståndskraft inrättas härmed. Gruppen för kritiska entiteters motståndskraft ska ge kommissionen stöd och underlätta samarbete mellan medlemsstaterna och informationsutbyte om frågor som rör detta direktiv.

2. Gruppen för kritiska entiteters motståndskraft ska bestå av företrädare för medlemsstaterna och kommissionen, vid behov med säkerhetsgodkännande. Gruppen för kritiska entiteters motståndskraft får bjuda in andra berörda parter att delta i sitt arbete när detta är relevant för fullgörandet av gruppens uppgifter. Om Europaparlamentet så begär får kommissionen bjuda in experter från Europaparlamentet att närvara vid möten i gruppen för kritiska entiteters motståndskraft.

Kommissionens företrädare ska vara ordförande för gruppen för kritiska entiteters motståndskraft.

3. Gruppen för kritiska entiteters motståndskraft ska ha följande uppgifter:

a) Stödja kommissionen med att bistå medlemsstaterna för att stärka deras kapacitet att bidra till att säkerställa kritiska entiteters motståndskraft i enlighet med detta direktiv.

b) Analysera strategierna för att identifiera bästa praxis för strategierna.

c) Underlätta utbyte av bästa praxis i fråga om medlemsstaternas identifiering av kritiska entiteter enligt artikel 6.1, inbegripet i förhållande till gränsöverskridande och sektorsöverskridande beroenden och med avseende på risker och incidenter.

d) När så är lämpligt, bidra i frågor som rör detta direktiv till dokument om motståndskraft på unionsnivå.

e) Bidra till utarbetandet av de riktlinjer som avses i artiklarna 7.3 och 13.5 och, på begäran, eventuella delegerade akter eller genomförandeakter som antas enligt detta direktiv.

f) Analysera de sammanfattande rapporter som avses i artikel 9.3 i syfte att främja utbyte av bästa praxis om de åtgärder som vidtagits i enlighet med artikel 15.3.

g) Utbyta bästa praxis angående den incidentanmälan som avses i artikel 15.

h) Diskutera de sammanfattande rapporterna från rådgivande uppdrag och tillvaratagna erfarenheter i enlighet med artikel 18.10.

i) Utbyta information och bästa praxis om innovation, forskning och utveckling som rör kritiska entiteters motståndskraft i enlighet med detta direktiv.

j) Vid behov utbyta information om frågor som rör kritiska entiteters motståndskraft med unionens berörda institutioner, organ och byråer.

4. Gruppen för kritiska entiteters motståndskraft ska, senast den 17 januari 2025 och därefter vartannat år, utarbeta ett arbetsprogram med åtgärder som ska vidtas för att genomföra dess mål och uppgifter. Det arbetsprogrammet ska överensstämma med kraven i och målen för detta direktiv.

5. Gruppen för kritiska entiteters motståndskraft ska regelbundet och under alla omständigheter minst en gång om året sammanträda med den samarbetsgrupp som inrättats enligt direktiv (EU) 2022/2555 för att främja och underlätta samarbete och informationsutbyte.

6. Kommissionen får anta genomförandeakter i vilka fastställs de förfaranden som krävs för verksamheten i gruppen för kritiska entiteters motståndskraft, under iakttagande av artikel 1.4. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 24.2.

7. Kommissionen ska till gruppen för kritiska entiteters motståndskraft lämna en sammanfattande rapport om den information som har lämnats av medlemsstaterna enligt artiklarna 4.3 och 5.4 senast den 17 januari 2027 och därefter vid behov och minst vart fjärde år.

Artikel 20

Kommissionens stöd till behöriga myndigheter och kritiska entiteter

1. Kommissionen ska när så är lämpligt ge medlemsstaterna och kritiska entiteter stöd för att uppfylla deras skyldigheter enligt detta direktiv. Kommissionen ska utarbeta en översikt på unionsnivå över gränsöverskridande och sektorsöverskridande risker för tillhandahållandet av samhällsviktiga tjänster, anordna rådgivande uppdrag enligt artiklarna 13.4 och 18 och underlätta informationsutbyte mellan medlemsstater och experter i hela unionen.

2. Kommissionen ska komplettera medlemsstaternas verksamhet som avses i artikel 10 genom att utveckla bästa praxis, vägledningsmaterial och metoder samt gränsöverskridande utbildningstillfällen och övningar för att testa kritiska entiteters motståndskraft.

3. Kommissionen ska informera medlemsstaterna om de ekonomiska resurser på unionsnivå som finns tillgängliga för medlemsstaterna för att stärka kritiska entiteters motståndskraft.

KAPITEL VI

TILLSYN OCH EFTERLEVNADSKONTROLL

Artikel 21

Tillsyn och efterlevnadskontroll

1. För att bedöma om de entiteter som medlemsstaterna har identifierat som kritiska entiteter enligt artikel 6.1 fullgör de skyldigheter som fastställs i detta direktiv ska medlemsstaterna säkerställa att de behöriga myndigheterna har befogenheter och medel för att

a) genomföra inspektioner på plats av den kritiska infrastruktur och de lokaler som den kritiska entiteten använder för att tillhandahålla sina samhällsviktiga tjänster och tillsyn på distans av de åtgärder som vidtagits av kritiska entiteter i enlighet med artikel 13,

b) utföra eller beställa revisioner av kritiska entiteter.

2. Medlemsstaterna ska säkerställa att de behöriga myndigheterna har befogenheter och medel för att, när så är nödvändigt för att fullgöra deras uppgifter enligt detta direktiv, kräva att entiteter enligt direktiv (EU) 2022/2555 som medlemsstaterna har identifierat som kritiska entiteter enligt det här direktivet inom en rimlig tidsfrist, som fastställs av dessa myndigheter, lämnar

a) den information som är nödvändig för att bedöma om de åtgärder som entiteterna har vidtagit för att säkerställa sin motståndskraft uppfyller kraven i artikel 13,

b) bevis på att de åtgärderna faktiskt har genomförts, inklusive resultatet av en revision som har utförts av en oberoende och kvalificerad revisor som har valts av entiteten och som har utförts på entitetens bekostnad.

När de behöriga myndigheterna begär denna information ska de ange syftet med kravet och specificera vilken information som krävs.

3. Utan att det påverkar möjligheten att ålägga sanktioner i enlighet med artikel 22 får de behöriga myndigheterna, efter de tillsynsåtgärder som avses i punkt 1 i den här artikeln eller den bedömning av information som avses i punkt 2 i den här artikeln, beordra de berörda kritiska entiteterna att vidta de åtgärder som är nödvändiga och proportionella för att avhjälpa konstaterade överträdelser av detta direktiv, inom en rimlig tidsfrist som fastställs av de myndigheterna, och att lämna information om de åtgärder som har vidtagits till de myndigheterna. Sådana föreläggande ska framför allt ta hänsyn till hur allvarlig överträdelsen är.

4. Medlemsstaterna ska säkerställa att de befogenheter som anges i punkterna 1, 2 och 3 endast kan utövas om de omfattas av lämpliga skyddsåtgärder. Sådana skyddsåtgärder ska särskilt garantera att befogenheterna utövas på ett objektivt, öppet och proportionerligt sätt och att de berörda kritiska entiteternas rättigheter och legitima intressen, såsom skyddet av handels- och affärshemligheter, skyddas på vederbörligt sätt, däribland rätten att höras, rätten till försvar och rätten till rättslig prövning inför en oberoende domstol.

5. Medlemsstaterna ska säkerställa att när en behörig myndighet enligt detta direktiv bedömer efterlevnaden hos en kritisk entitet enligt denna artikel ska den behöriga myndigheten informera de behöriga myndigheterna i de berörda medlemsstaterna enligt direktiv (EU) 2022/2555. I detta syfte ska medlemsstaterna säkerställa att de behöriga myndigheterna enligt det här direktivet kan begära att de behöriga myndigheterna enligt direktiv (EU) 2022/2555 ska utöva sina tillsyns- och efterlevnadskontrollbefogenheter med avseende på en entitet enligt det direktivet som har identifierats som en kritisk entitet enligt det här direktivet. För det ändamålet ska medlemsstaterna säkerställa att de behöriga myndigheterna enligt det här direktivet samarbetar och utbyter information med de behöriga myndigheterna enligt direktiv (EU) 2022/2555.

Artikel 22

Sanktioner

Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av de nationella åtgärder som antagits enligt detta direktiv och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska till kommissionen anmäla dessa regler och åtgärder senast den 17 oktober 2024 samt utan dröjsmål eventuella ändringar som berör dem.

KAPITEL VII

DELEGERADE AKTER OCH GENOMFÖRANDEAKTER

Artikel 23

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artikel 5.1 ska ges till kommissionen för en period på fem år från och med den 16 januari 2023.

3. Den delegering av befogenhet som avses i artikel 5.1 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. Innan kommissionen antar en delegerad akt ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning.

5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

6. En delegerad akt som antas enligt artikel 5.1 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.

Artikel 24

Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

KAPITEL VIII

SLUTBESTÄMMELSER

Artikel 25

Rapportering och översyn

Kommissionen ska senast den 17 juli 2027 överlämna en rapport till Europaparlamentet och rådet med en bedömning av i vilken utsträckning varje medlemsstat har vidtagit de åtgärder som är nödvändiga för att följa detta direktiv.

Kommissionen ska regelbundet se över hur detta direktiv fungerar och rapportera resultaten till Europaparlamentet och rådet. Rapporten ska framför allt bedöma mervärdet av detta direktiv, dess effekt när det gäller att säkerställa kritiska entiteters motståndskraft och huruvida bilagan till detta direktiv bör ändras. Kommissionen ska lämna den första rapporten senast den 17 juni 2029. Vid rapportering enligt denna artikel ska kommissionen beakta relevanta dokument från gruppen för kritiska entiteters motståndskraft.

Artikel 26

Införlivande

1. Medlemsstaterna ska senast den 17 oktober 2024 anta och offentliggöra de bestämmelser som är nödvändiga för att följa detta direktiv. De ska genast underrätta kommissionen om detta.

De ska tillämpa dessa bestämmelser från och med den 18 oktober 2024.

2. När en medlemsstat antar de bestämmelser som avses i punkt 1 ska de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen ska göras ska varje medlemsstat själv utfärda.

Artikel 27

Upphävande av direktiv 2008/114/EG

Direktiv 2008/114/EG ska upphöra att gälla med verkan från och med den 18 oktober 2024.

Hänvisningar till det upphävda direktivet ska anses som hänvisningar till det här direktivet.

Artikel 28

Ikraftträdande

Detta direktiv träder i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Artikel 29

Adressater

Detta direktiv riktar sig till medlemsstaterna.

Utfärdat i Strasbourg den 14 december 2022.

På Europaparlamentets vägnar	*På rådets vägnar*
R. METSOLA	M. BEK
Ordförande	*Ordförande*

BILAGA

SEKTORER, UNDERSEKTORER OCH KATEGORIER AV ENTITETER

Sektorer	Undersektorer	Kategorier av entiteter
1. Energi	a) Elektricitet	— Elföretag enligt definitionen i artikel 2.57 i Europaparlamentets och rådets direktiv (EU) 2019/944 ([1]) som bedriver *leverans* enligt definitionen i artikel 2.12 i det direktivet
		— Systemansvariga för distributionssystem enligt definitionen i artikel 2.29 i direktiv (EU) 2019/944
		— Systemansvariga för överföringssystem enligt definitionen i artikel 2.35 i direktiv (EU) 2019/944
		— Producenter enligt definitionen i artikel 2.38 i direktiv (EU) 2019/944
		— Nominerade elmarknadsoperatörer enligt definitionen i artikel 2.8 i Europaparlamentets och rådets förordning (EU) 2019/943 ([2])
		— Marknadsaktörer enligt definitionen i artikel 2.25 i förordning (EU) 2019/943 som tillhandahåller aggregering, efterfrågeflexibilitet eller energilagringstjänster enligt definitionerna i artikel 2.18, 2.20 och 2.59 i direktiv (EU) 2019/944
	b) Fjärrvärme eller fjärrkyla	— Operatörer av fjärrvärme eller fjärrkyla enligt definitionen i artikel 2.19 i Europaparlamentets och rådets direktiv (EU) 2018/2001 ([3])
	c) Olja	— Operatörer av oljeledningar
		— Operatörer av anläggningar för oljeproduktion, raffinaderier, bearbetningsanläggningar och anläggningar för lagring och överföring av olja
		— Centrala lagringsenheter enligt definitionen i artikel 2 f i rådets direktiv 2009/119/EG ([4])

Sektorer	Undersektorer	Kategorier av entiteter
	d) Gas	— Gashandelsföretag eller gashandlare enligt definitionen i artikel 2.8 i Europaparlamentets och rådets direktiv 2009/73/EG ([5])
		— Systemansvariga för distributionssystemet enligt definitionen i artikel 2.6 i direktiv 2009/73/EG
		— Systemansvariga för överföringssystemet enligt definitionen i artikel 2.4 i direktiv 2009/73/EG
		— Systemansvariga för lagringssystemet enligt definitionen i artikel 2.10 i direktiv 2009/73/EG
		— Systemansvariga för en LNG-anläggning enligt definitionen i artikel 2.12 i direktiv 2009/73/EG
		— Naturgasföretag enligt definitionen i artikel 2.1 i direktiv 2009/73/EG
		— Operatörer av raffinaderier och bearbetningsanläggningar för naturgas
	e) Vätgas	— Operatörer av produktion, lagring och överföring av vätgas
2. Transport	a) Luftfart	— Lufttrafikföretag enligt definitionen i artikel 3.4 i förordning (EG) nr 300/2008 och som används för kommersiella syften
		— Flygplatsens ledningsenheter enligt definitionen i artikel 2.2 i Europaparlamentets och rådets direktiv 2009/12/EG ([6]), flygplatser enligt definitionen i artikel 2.1 i det direktivet, inbegripet de huvudflygplatser som förtecknas i avsnitt 2 i bilaga II till Europaparlamentets och rådets förordning (EU) nr 1315/2013 ([7]) och entiteter som driver kringliggande installationer vid flygplatser
		— Operatörer inom trafikstyrning och trafikledning som tillhandahåller flygkontrolltjänster enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EG) nr 549/2004 ([8])

Sektorer	Undersektorer	Kategorier av entiteter
	b) Järnväg	— Infrastrukturförvaltare enligt definitionen i artikel 3.2 i Europaparlamentets och rådets direktiv 2012/34/EU ([9])
		— Järnvägsföretag enligt definitionen i artikel 3.1 i direktiv 2012/34/EU och tjänsteleverantörer enligt definitionen i artikel 3.12 i det direktivet
	c) Vatten	— Transportföretag som bedriver persontrafik och godstrafik på inre vattenvägar, till havs och längs kuster, enligt definitionerna för sjötransport i bilaga I till Europaparlamentets och rådets förordning (EG) nr 725/2004, exklusive de enskilda fartyg som drivs av dessa företag
		— Ledningsenheter för hamnar enligt definitionen i artikel 3.1 i direktiv 2005/65/EG, inbegripet deras hamnanläggningar enligt definitionen i artikel 2.11 i förordning (EG) nr 725/2004, och entiteter som sköter anläggningar och utrustning i hamnar
		— Operatörer av sjötrafikinformationstjänst (VTS) enligt definitionen i artikel 3 o i Europaparlamentets och rådets direktiv 2002/59/EG ([10])
	d) Väg	— Vägmyndigheter enligt definitionen i artikel 2.12 i kommissionens delegerade förordning (EU) 2015/962 ([11]) med ansvar för trafikstyrning, med undantag för offentliga entiteter för vilka trafikstyrning eller driften av intelligenta transportsystem är en icke väsentlig del av deras allmänna verksamhet
		— Operatörer av intelligenta transportsystem enligt definitionen i artikel 4.1 i Europaparlamentets och rådets direktiv 2010/40/EU ([12])
	e) Kollektivtrafik	— Kollektivtrafikföretag enligt definitionen i artikel 2 d i Europaparlamentets och rådets förordning (EG) nr 1370/2007 ([13])
3. Bankverksamhet		— Kreditinstitut enligt definitionen i artikel 4.1 i förordning (EU) nr 575/2013
4. Finansmarknadsinfrastruktur		— Operatörer av handelsplatser enligt definitionen i artikel 4.24 i direktiv 2014/65/EU
		— Centrala motparter enligt definitionen i artikel 2.1 i förordning (EU) nr 648/2012

Sektorer	Undersektorer	Kategorier av entiteter
5. Hälso- och sjukvård		— Vårdgivare enligt definitionen i artikel 3 g i Europaparlamentets och rådets direktiv 2011/24/EU ([14])
		— EU-referenslaboratorier som avses i artikel 15 i Europaparlamentets och rådets förordning (EU) 2022/2371 ([15])
		— Entiteter som bedriver forskning och utveckling avseende läkemedel enligt definitionen i artikel 1.2 i Europaparlamentets och rådets direktiv 2001/83/EG ([16])
		— Entiteter som tillverkar farmaceutiska basprodukter och läkemedel som avses i huvudgrupp 21 avsnitt C i Nace Rev. 2
		— Entiteter som tillverkar medicintekniska produkter som betraktas som kritiska vid ett hot mot folkhälsan (*förteckning över kritiska medicintekniska produkter vid ett hot mot folkhälsan*) i den mening som avses i artikel 22 i Europaparlamentets och rådets förordning (EU) 2022/123 ([17])
		— Entiteter med tillstånd att bedriva partihandel i den mening som avses i artikel 79 i direktiv 2001/83/EG
6. Dricksvatten		— Leverantörer och distributörer av dricksvatten enligt definitionen i artikel 2.1 a i Europaparlamentets och rådets direktiv (EU) 2020/2184 ([18]), undantaget distributörer för vilka distribution av dricksvatten utgör en icke väsentlig del av deras allmänna verksamhet, som består i distribution av andra förnödenheter och varor
7. Avloppsvatten		— Verksamheter som samlar ihop, släpper ut och renar avloppsvatten från tätbebyggelse, hushållsspillvatten eller industrispillvatten enligt definitionerna i artikel 2.1, 2.2 och 2.3 i rådets direktiv 91/271/EEG ([19]), undantaget verksamheter som samlar in, släpper ut eller renar avloppsvatten från tätbebyggelse, hushållsspillvatten eller industrispillvatten som en icke väsentlig del av sin allmänna verksamhet

Sektorer	Undersektorer	Kategorier av entiteter
8. Digital infrastruktur		— Leverantörer av internetknutpunkter enligt definitionen i artikel 6.18 i direktiv (EU) 2022/2555
		— Leverantörer av DNS-tjänster enligt definitionen i artikel 6.20 i direktiv (EU) 2022/2555, med undantag för operatörer av rotnamnsservrar
		— Registreringsenheter för toppdomäner enligt definitionen i artikel 6.21 i direktiv (EU) 2022/2555
		— Leverantörer av molntjänster enligt definitionen i artikel 6.30 i direktiv (EU) 2022/2555
		— Tillhandahållare av datacentralstjänster enligt definitionen i artikel 6.31 i direktiv (EU) 2022/2555
		— Tillhandahållare av nätverk för innehållsleverans enligt definitionen i artikel 6.32 i direktiv (EU) 2022/2555
		— Tillhandahållare av betrodda tjänster enligt definitionen i artikel 3.19 i Europaparlamentets och rådets förordning (EU) nr 910/2014 ([20]).
		— Tillhandahållare av allmänna elektroniska kommunikationsnät enligt definitionen i artikel 2.8 i Europaparlamentets och rådets direktiv (EU) 2018/1972 ([21])
		— Tillhandahållare av elektroniska kommunikationstjänster i den mening som avses i artikel 2.4 i direktiv (EU) 2018/1972 i den mån deras tjänster är allmänt tillgängliga
9. Offentlig förvaltning		— Offentliga förvaltningsentiteter hos nationella regeringar såsom de definieras av en medlemsstat i enlighet med nationell rätt
10. Rymden		— Operatörer av markbaserad infrastruktur som ägs, förvaltas och drivs av medlemsstater eller privata parter och som stöder tillhandahållandet av rymdbaserade tjänster, undantaget tillhandahållare av allmänna elektroniska kommunikationsnät enligt definitionen i artikel 2.8 i direktiv (EU) 2018/1972

Sektorer	Undersektorer	Kategorier av entiteter
11. Produktion, bearbetning och distribution av livsmedel		— Livsmedelsföretag enligt definitionen i artikel 3.2 i Europaparlamentets och rådets förordning (EG) nr 178/2002 ([22]) som uteslutande bedriver logistikverksamhet och grossisthandel samt storskalig industriell produktion och bearbetning

([1]) Europaparlamentets och rådets direktiv (EU) 2019/944 av den 5 juni 2019 om gemensamma regler för den inre marknaden för el och om ändring av direktiv 2012/27/EU (EUT L 158, 14.6.2019, s. 125).
([2]) Europaparlamentets och rådets förordning (EU) 2019/943 av den 5 juni 2019 om den inre marknaden för el (EUT L 158, 14.6.2019, s. 54).
([3]) Europaparlamentets och rådets direktiv (EU) 2018/2001 av den 11 december 2018 om främjande av användningen av energi från förnybara energikällor (EUT L 328, 21.12.2018, s. 82).
([4]) Rådets direktiv 2009/119/EG av den 14 september 2009 om skyldighet för medlemsstaterna att inneha minimilager av råolja och/eller petroleumprodukter (EUT L 265, 9.10.2009, s. 9).
([5]) Europaparlamentets och rådets direktiv 2009/73/EG av den 13 juli 2009 om gemensamma regler för den inre marknaden för naturgas och om upphävande av direktiv 2003/55/EG (EUT L 211, 14.8.2009, s. 94).
([6]) Europaparlamentets och rådets direktiv 2009/12/EG av den 11 mars 2009 om flygplatsavgifter (EUT L 70, 14.3.2009, s. 11).
([7]) Europaparlamentets och rådets förordning (EU) nr 1315/2013 av den 11 december 2013 om unionens riktlinjer för utbyggnad av det transeuropeiska transportnätet och om upphävande av beslut nr 661/2010/EU (EUT L 348, 20.12.2013, s. 1).
([8]) Europaparlamentets och rådets förordning (EG) nr 549/2004 av den 10 mars 2004 om ramen för inrättande av det gemensamma europeiska luftrummet ("ramförordning") (EUT L 96, 31.3.2004, s. 1).
([9]) Europaparlamentets och rådets direktiv 2012/34/EU av den 21 november 2012 om inrättande av ett gemensamt europeiskt järnvägsområde (EUT L 343, 14.12.2012, s. 32).
([10]) Europaparlamentets och rådets direktiv 2002/59/EG av den 27 juni 2002 om inrättande av ett övervaknings- och informationssystem för sjötrafik i gemenskapen och om upphävande av rådets direktiv 93/75/EEG (EGT L 208, 5.8.2002, s. 10).
([11]) Kommissionens delegerade förordning (EU) 2015/962 av den 18 december 2014 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller tillhandahållande av EU-omfattande realtidstrafikinformationstjänster (EUT L 157, 23.6.2015, s. 21).
([12]) Europaparlamentets och rådets direktiv 2010/40/EU av den 7 juli 2010 om ett ramverk för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportslag (EUT L 207, 6.8.2010, s. 1).
([13]) Europaparlamentets och rådets förordning (EG) nr 1370/2007 av den 23 oktober 2007 om kollektivtrafik på järnväg och väg och om upphävande av rådets förordning (EEG) nr 1191/69 och (EEG) nr 1107/70 (EUT L 315, 3.12.2007, s. 1).
([14]) Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård (EUT L 88, 4.4.2011, s. 45).
([15]) Europaparlamentets och rådets förordning (EU) 2022/2371 av den 23 november 2022 om allvarliga gränsöverskridande hot mot människors hälsa och om upphävande av beslut nr 1082/2013/EU (EUT L 314, 6.12.2022, s 26).
([16]) Europaparlamentets och rådets direktiv 2001/83/EG av den 6 november 2001 om upprättande av gemenskapsregler för humanläkemedel (EGT L 311, 28.11.2001, s. 67).
([17]) Europaparlamentets och rådets förordning (EU) 2022/123 av den 25 januari 2022 om en förstärkt roll för Europeiska läkemedelsmyndigheten vid krisberedskap och krishantering avseende läkemedel och medicintekniska produkter (EUT L 20, 31.1.2022, s. 1).
([18]) Europaparlamentets och rådets direktiv (EU) 2020/2184 av den 16 december 2020 om kvaliteten på dricksvatten, (EUT L 435, 23.12.2020, s. 1).
([19]) Rådets direktiv 91/271/EEG av den 21 maj 1991 om rening av avloppsvatten från tätbebyggelse (EGT L 135, 30.5.1991, s. 40).
([20]) Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EUT L 257, 28.8.2014, s. 73).
([21]) Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (EUT L 321, 17.12.2018, s. 36).
([22]) Europaparlamentets och rådets förordning (EG) nr 178/2002 av den 28 januari 2002 om allmänna principer och krav för livsmedelslagstiftning, om inrättande av Europeiska myndigheten för livsmedelssäkerhet och om förfaranden i frågor som gäller livsmedelssäkerhet (EGT L 31, 1.2.2002, s. 1).

Sammanfattning av betänkandet Motståndskraft i samhällsviktiga tjänster (SOU 2024:64)

CER-direktivet

Europaparlamentet och rådet antog den 14 december 2022 CER-direktivet[1]. Direktivets syfte är att stärka kritiska verksamhetsutövares motståndskraft och förmåga att tillhandahålla samhällsviktiga tjänster på den inre marknaden.

Enligt direktivet ska medlemsstaterna senast den 17 juli 2026 identifiera verksamhetsutövare som erbjuder samhällsviktiga tjänster inom sektorerna energi, transport, bankverksamhet, finansmarknads-infrastruktur, hälso- och sjukvård, dricksvatten, avloppsvatten, digital infrastruktur, offentlig förvaltning, rymden samt produktion, bearbetning och distribution av livsmedel. Medlemsstaterna ska senast den 17 januari 2026 ta fram en nationell riskbedömning och en strategi för kritiska verksamhetsutövares motståndskraft.

Direktivet ställer krav på kritiska verksamhetsutövare, de ska göra en riskbedömning och vidta åtgärder för motståndskraft inklusive bakgrundskontroller i syfte att stärka motståndskraften samt rapportera incidenter. Riskbedömningen ska göras inom nio månader från mottagandet av underrättelsen om identifiering. Kravet på åtgärder för motståndskraft ska tillämpas först tio månader efter att den kritiska verksamhetsutövaren har underrättats om identifieringen. I direktivet finns också bestämmelser om kritiska verksamhetsutövare av särskild europeisk betydelse.

Direktivet innehåller vidare bestämmelser om tillsyn och sanktioner samt en ram för samarbete mellan medlemsstaterna.

Direktivet är ett minimidirektiv med innebörd att den svenska lagstiftningen skulle kunna innehålla mer långtgående skyldigheter.

Medlemsstaterna ska senast den 17 oktober 2024 anta och offentliggöra de bestämmelser som är nödvändiga för att följa direktivet. Bestämmelserna ska tillämpas från och med den 18 oktober 2024.

Direktivet ersätter rådets direktiv 2008/114/EG om identifiering av, klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna som upphör att gälla med verkan från och med den 18 oktober 2024. Hänvisningar i det upphävda direktivet ska anses som hänvisningar till det här direktivet.

Utredningens uppdrag

Utredningen redovisar i detta slutbetänkande förslag om införlivning av CER-direktivet i svensk rätt samt förslag till ändring i offentlighets- och sekretessbestämmelserna, ändring i säkerhetsskyddslagen samt i lagen om

[1] Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.

cybersäkerhet. Utredningen redovisade i delbetänkandet Nya regler om cybersäkerhet, SOU 2024:18 förslag om införlivning av NIS2-direktivet[2].

Utredningens uppdrag har varit att föreslå de anpassningar av svensk rätt som är nödvändiga för att CER-direktivet ska kunna genomföras. Det har innefattat att föreslå hur identifiering och krav på verksamhetsutövare som omfattas av direktivet ska regleras samt rollfördelningen mellan svenska myndigheter med avseende på de olika uppgifter och ansvarsområden som föreskrivs i CER-direktivet.

I utredningens uppdrag har även ingått att ta ställning till om bestämmelserna i offentlighets- och sekretesslagen (2009:400) innebär ett tillräckligt skydd för sådana uppgifter som kan komma att behandlas enligt NIS2- och CER-direktiven, föreslå de ändringar som behövs för en mer sammanhållen systematik mellan säkerhetsskyddslagen, lagen om cybersäkerhet och lagen om motståndskraft hos kritiska verksamhetsutövare, särskilt vad gäller tillsynsmyndigheternas befogenheter och sanktionsavgifternas storlek.

Utredningen ska vidare beakta de frågor som är gemensamma för NIS2- och CER-direktiven i den mån dessa är hänförliga till genomförandet av CER-direktivet.

Utredningens förslag

Lagen om motståndskraft hos kritiska verksamhetsutövare

Utredningen föreslår att CER-direktivet införlivas genom en ny lag, lagen om motståndskraft hos kritiska verksamhetsutövare. Utredningen föreslår inte några skyldigheter utöver vad som följer av direktivet.

Vem omfattas av reglerna om motståndskraft hos kritiska verksamhetsutövare?

Regelverket ska tillämpas på enskilda och offentliga verksamhetsutövare som tillhandahåller en samhällsviktig tjänst som omfattas av bilagan till direktivet. Vidare krävs att verksamhetsutövaren har identifierats som kritisk av tillsynsmyndigheten. För kritiska verksamhetsutövare inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur gäller endast vissa begränsade delar av regelverket.

I förslaget görs vissa undantag från lagens tillämpningsområde. Lagen gäller inte för sådant som regleras i förslaget till lag om cybersäkerhet och inte heller om det i annan författning finns bestämmelser om krav på riskbedömning, åtgärder för motståndskraft, bakgrundskontroll och incidentrapportering om kraven har minst motsvarande verkan. Lagen gäller inte heller för regeringen, Regeringskansliet, utlandsmyndigheter, kommittéväsendet, Riksrevisionen, Riksdagens ombudsmän, Sveriges Riksbank, Riksdagsförvaltningen eller Sveriges domstolar.

Lagen gäller inte för statliga myndigheter som till övervägande del bedriver brottsbekämpning eller säkerhetskänslig verksamhet. För övriga

[2] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

verksamhetsutövare gäller inte 3–6 kap. i lagen för den del av den samhällsviktiga tjänsten som är säkerhetskänslig. Det innebär att dessa verksamhetsutövare bland annat omfattas av bestämmelserna om identifiering i 2 kap. i den föreslagna lagen.

Identifiering av kritiska verksamhetsutövare

Tillsynsmyndigheterna ska genom beslut identifiera kritiska verksamhetsutövare inom sina tillsynsområden. För att en verksamhetsutövare ska identifieras som kritisk enligt direktivet ska tre kriterier vara uppfyllda. För det första ska verksamhetsutövaren tillhandahålla en eller flera samhällsviktiga tjänster inom någon av sektorerna som finns i bilagan till direktivet, för det andra ska verksamhetsutövaren ha en kritisk infrastruktur belägen i Sverige och för det tredje ska en incident få betydande störande effekter för tillhandahållandet av den samhällsviktiga tjänsten. Myndigheten för samhällsskydd och beredskap ska meddela föreskrifter om när en störande effekt är betydande.

Vid identifieringen ska tillsynsmyndigheten beakta den nationella riskbedömningen och strategin för kritiska verksamhetsutövares motståndskraft.

Tillsynsmyndigheten ska upprätta en förteckning över kritiska verksamhetsutövare inom sitt tillsynsområde. Myndigheten för samhällsskydd och beredskap ska upprätta en samlad förteckning över samtliga kritiska verksamhetsutövare.

Kritiska verksamhetsutövare av särskild europeisk betydelse

Kritiska verksamhetsutövare som tillhandahåller en samhällsviktig tjänst till eller i minst sex medlemsstater ska anmäla detta till tillsynsmyndigheten. Dessa verksamhetsutövare ska delta i kommissionens samråd. På grundval av samrådet fastställer kommissionen om den kritiska verksamhetsutövaren är av särskild europeisk betydelse.

Myndigheten för samhällsskydd och beredskap tar emot kommissionens underrättelse om att en kritisk verksamhetsutövare är av särskild europeisk betydelse och vidarebefordrar den till tillsynsmyndigheten. Tillsynsmyndigheten underrättar den kritiska verksamhetsutövaren.

Kommissionen anordnar rådgivande uppdrag för att bedöma de åtgärder som den kritiska verksamhetsutövaren har infört för att uppfylla sina skyldigheter. Ett rådgivande uppdrag får endast genomföras om MSB efter samråd med den kritiska verksamhetsutövaren och dennas tillsynsmyndighet, lämnat samtycke.

Krav på riskbedömning, åtgärder för motståndskraft och incidentrapportering

Utredningen föreslår att Myndigheten för samhällsskydd och beredskap ska göra en nationell riskbedömning.

En kritisk verksamhetsutövare ska göra en riskbedömning nio månader efter att den fått del av beslutet om identifiering. Riskbedömningen ska

innehålla en redogörelse för alla relevanta risker som skulle kunna leda till en incident.

Verksamhetsutövaren ska vidare vidta tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa sin motståndskraft. Åtgärderna ska vidtas på grundval av riskbedömningen, utgå från ett allriskperspektiv och vara proportionella i förhållande till risken. Det ska finnas en plan som beskriver åtgärder som vidtagits eller ska vidtas. Tillsynsmyndigheterna får meddela föreskrifter om riskbedömning, åtgärder och planer för motståndskraft. Myndigheten för samhällsskydd och beredskap får meddela föreskrifter för sektorn offentlig förvaltning.

Kritiska verksamhetsutövare ska utan dröjsmål rapportera incidenter som medför eller kan medföra en betydande störning i tillhandahållandet av den samhällsviktiga tjänsten till Myndigheten för samhällsskydd och beredskap. En första rapport ska lämnas inom 24 timmar. Myndigheten för samhällsskydd och beredskap får meddela föreskrifter om vad som utgör en betydande störning och om incidentrapportering.

Skyldigheterna avseende åtgärder och incidentrapportering börjar gälla först tio månader efter den dag verksamhetsutövaren fått del av tillsynsmyndighetens beslut om identifiering.

Kritiska verksamhetsutövare ska också utse en samverkansansvarig som utgör kontaktpunkt för berörda myndigheter.

Bakgrundskontroll

Syftet med en bakgrundskontroll är att endast den som bedöms lämplig ska få vara anställd eller på annat sätt delta i befattningar där deltagandet kan orsaka mer än ringa skada på den samhällsviktiga tjänsten.

Utredningen föreslår att kritiska verksamhetsutövare ska göra en befattningsanalys där det framgår för vilka befattningar det finns ett krav på bakgrundskontroll. Analysen ska dokumenteras.

Den kritiska verksamhetsutövaren ska genomföra bakgrundskontrollen och bedöma om personen som kontrollen avser är lämplig. En bakgrundskontroll innebär att den som kontrolleras ska styrka sin identitet och visa upp ett särskilt utdrag från belastningsregistret. Av förordningen (1999:1134) om belastningsregister framgår vilka uppgifter ett utdrag ska innehålla.

Det ska dokumenteras att en bakgrundskontroll genomförts och anteckningen ska bevaras i två år.

Tillsyn

Utredningen föreslår att den tillsynsmyndighet som är tillsynsmyndighet enligt den föreslagna lagen om cybersäkerhet även blir tillsynsmyndighet enligt lagen om motståndskraft hos kritiska verksamhetsutövare. Ett fåtal tillsynsmyndigheter har fått ny undersektor eller kategori av entitet. Vidare ingår i sektorn offentlig förvaltning endast statliga myndigheter. Följande tillsynsmyndigheter föreslås.

Tillsynsmyndighet	Sektor
Statens energimyndighet	Energi
Transportstyrelsen	Transport
Finansinspektionen	Bankverksamhet

	Finansmarknadsinfrastruktur
Inspektionen för vård och omsorg	Vårdgivare[3] i Hälso- och sjukvårdssektorn
Läkemedelsverket	Hälso- och sjukvårdssektorn, med undantag för vårdgivare
Livsmedelsverket	Avloppsvatten Dricksvatten Produktion, bearbetning och distribution av livsmedel
Post- och telestyrelsen	Digital infrastruktur Rymden
Länsstyrelserna i Norrbottens, Skåne, Stockholms och Västra Götalands län	Offentlig förvaltning

Tillsynsmyndigheten ska utöva tillsyn över att lagen och föreskrifter som meddelats i anslutning till lagen följs.

Kritiska verksamhetsutövare ska tillhandahålla tillsynsmyndigheten den information som behövs för tillsynen och den nationella riskbedömningen. Tillsynsmyndigheten har också rätt att få tillträde till områden, lokaler och andra utrymmen i den omfattning som behövs för tillsynen. Undantag görs för uppgifter som är säkerhetsskyddsklassificerade och tillträde till verksamhet där säkerhetskänslig verksamhet bedrivs.

MSB ska leda ett samarbetsforum där tillsynsmyndigheterna ingår för att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn.

Inom ramen för tillsyn ska tillsynsmyndigheten även genomföra rådgivande uppdrag som anordnas av kommissionen avseende kritiska verksamhetsutövare av särskild europeisk betydelse.

Tillsynsmyndigheten ska även bidra med underlag till den nationella riskbedömningen.

Gemensam kontaktpunkt

Myndigheten för samhällsskydd och beredskap ska vara gemensam kontaktpunkt. Den gemensamma kontaktpunkten ska ha en sambandsfunktion för att säkerställa det gränsöverskridande samarbetet med gemensamma kontaktpunkter i andra medlemsstater och med kommissionen.

Ingripande och sanktioner

Utredningen föreslår att ingripande sker genom att tillsynsmyndigheten beslutar om föreläggande, sanktionsavgift eller anmärkning. Tillsynsmyndigheten ska ingripa mot den som åsidosatt skyldigheten att anmäla att man tillhandahåller tjänsten till minst sex medlemsstater, göra en riskbedömning, vidta åtgärder och plan för motståndskraft, utse

[3] Vårdgivare enligt definitionen i artikel 3 g i Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård.

samverkansansvarig, rapportera incidenter, göra en befattningsanalys, genomföra en bakgrundskontroll och bevara viss information.

Nivåerna på sanktionsavgiften föreslås vara desamma som för väsentliga verksamhetsutövare i lagen om cybersäkerhet. Det innebär att sanktionsavgiften för enskilda kritiska verksamhetsutövare ska bestämmas till lägst 5 000 kronor och högst till det högsta av:

- 2 procent av den kritiska verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
- 10 000 000 euro.

För offentliga kritiska verksamhetsutövare ska avgiften bestämmas till lägst 5 000 kronor och högst till 10 000 000 kronor.

Vid bedömning av sanktionsavgiftens storlek ska särskild hänsyn tas till den skada eller risk för skada som uppstått till följd av överträdelsen, om den kritiska verksamhetsutövaren tidigare har begått en överträdelse och de kostnader som verksamhetsutövaren har undvikit till följd av överträdelsen.

Om tillsynsmyndigheten inte finner skäl att ingripa med föreläggande eller sanktionsavgift ska den i stället meddela en anmärkning. Tillsynsmyndigheten får i vissa fall avstå från att ingripa.

Lagen om cybersäkerhet

Den som identifierats som en kritisk verksamhetsutövare enligt lagen om motståndskraft hos kritiska verksamhetsutövare ska oavsett storlek omfattas av lagen om cybersäkerhet om verksamheten omfattas av bilaga 1 eller 2 i NIS2-direktivet och verksamhetsutövaren är etablerad i Sverige.

Sekretess och tystnadsplikt

För att MSB och tillsynsmyndigheterna ska kunna lämna ut uppgifter som härrör från andra medlemsstater och EU:s institutioner och som omfattas av sekretess enligt 15 kap. 1 a § offentlighets- och sekretesslagen (2009:400), OSL, till varandra, föreslår utredningen en ny sekretessbrytande bestämmelse i 15 kap.

Utredningen föreslår vidare att sekretesskyddet ska stärkas och föreslår att en ny bestämmelse om sekretess införs i 18 kap. OSL för uppgift i incidentrapporter enligt lagen om cybersäkerhet och lagen om motståndskraft hos kritiska verksamhetsutövare samt för uppgift om åtgärd som följer av en sådan incident. Bestämmelsen förslås få ett omvänt skaderekvisit och rätten att meddela och offentliggöra uppgifterna begränsas. Vidare föreslås att diarium över incidenter hos rapporterande myndigheter, tillsynsmyndigheter och MSB ska kunna omfattas av sekretess.

När det gäller bakgrundskontroller föreslås en bestämmelse om tystnadsplikt för uppgifter som förekommer i angelägenheter som avser bakgrundskontroll i den nya lagen. En motsvarande bestämmelse införs i 35 kap. OSL för det allmännas verksamhet.

Sekretesskyddet för uppgifter som tillsynsmyndigheten kommer att hantera behöver kompletteras när det gäller uppgifter som rör enskilds affärs- eller driftsförhållanden. Utredningen föreslår därför att det i bilagan

till offentlighets- och sekretessförordningen (2009:641) införs en bestämmelse om att sekretess gäller för dessa uppgifter i verksamhet som består i tillsyn och utredning enligt lagen om motståndskraft hos enskilda verksamhetsutövare.

Sanktionsavgift enligt säkerhetsskyddslagen med mera

Utredningen föreslår att sanktionsavgifternas storlek i säkerhetsskyddslagen (2018:585) ska höjas för enskilda verksamhetsutövare. Det innebär att sanktionsavgiften ska bestämmas till lägst 25 000 kronor och högst till det högsta av 120 000 000 kronor eller 2 procent av verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår.

Utredningen föreslår inga ändringar i säkerhetsskyddslagen avseende tillsynsmyndighetens befogenheter.

Utredningen har bedömt att ingripande genom att ansöka om förbud att utöva ledningsfunktion och att meddela en anmärkning inte ska införas i säkerhetsskyddslagen.

Anger en kritisk verksamhetsutövare att den samhällsviktiga tjänsten till någon del är säkerhetskänslig ska tillsynsmyndigheten enligt säkerhetsskyddslagen underrättas. Tillsynsmyndigheten ska inom fem dagar meddela tillsynsmyndigheten enligt lagen om motståndskraft hos kritiska verksamhetsutövare huruvida den kritiska verksamhetsutövaren har anmält att den bedriver säkerhetskänslig verksamhet.

Konsekvenser

Utredningens förslag medför ekonomiska konsekvenser för tillsynsmyndigheterna, MSB, Polismyndigheten och kritiska verksamhetsutövare.

Utredningen föreslår att

- tillsynsmyndigheterna för år 2025 och 2026 tilldelas ett förstärkt anslag. Kostnader för löpande tillsyn föreslås beräknas när identifieringen av kritiska verksamhetsutövare är genomförd.
- MSB för år 2025 och 2026 får ett förstärkt anslag. Kostnader för stöd vid incidenter får klarläggas när identifieringen av kritiska verksamhetsutövare är genomförd.
- Polismyndighetens kostnader för den löpande hanteringen av utdrag ur belastningsregistret föreslås beräknas när identifieringen av kritiska verksamhetsutövare är genomförd och dessa har gjort den föreskrivna befattningsanalysen.

När det gäller kostnader för offentliga verksamhetsutövare föreslår utredningen att dessa finansieras inom befintlig budgetram. Avseende kostnader för enskilda verksamhetsutövare föreslår utredningen, när antalet kritiska verksamhetsutövare har identifierats och riskbedömningarna har genomförts, att det kan finnas anledning att överväga om det finns behov av att införa statligt stöd.

Ikraftträdande

Utredningen föreslår att lagen om motståndskraft hos kritiska verksamhetsutövare och tillhörande förordning ska träda i kraft den 1 augusti 2025.

Förslagen i offentlighets- och sekretesslagen och offentlighets- och sekretessförordningen som gäller lagen om cybersäkerhet föreslås träda i kraft den 1 januari 2025.

Övriga förslag föreslås träda i kraft den 1 augusti 2025.

Betänkandets lagförslag

Förslag till lag om motståndskraft hos kritiska verksamhetsutövare

Härigenom föreskrivs följande.

1 kap. Inledande bestämmelser

Syftet med lagen

1 § Syftet med denna lag är att stärka kritiska verksamhetsutövares motståndskraft och förmåga att tillhandahålla samhällsviktiga tjänster inom sektorerna energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, dricksvatten, avloppsvatten, digital infrastruktur, offentlig förvaltning, rymden samt produktion, bearbetning och distribution av livsmedel.

Genom denna lag genomförs Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG, utom vad gäller Sveriges skyldighet att anta en strategi för kritiska entiteters motståndskraft.

Uttryck i lagen

2 § I lagen avses med

1. *CER-direktivet*: Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG,
2. *enskild verksamhetsutövare*: en juridisk eller fysisk person som bedriver verksamhet och som inte är en statlig myndighet, region eller kommun,
3. *incident*: varje händelse som kan medföra en betydande störning, eller som medför en störning, av tillhandahållandet av en samhällsviktig tjänst,
4. *kritisk infrastruktur*: en tillgång, en anläggning, utrustning, ett nätverk eller ett system, eller en del av en tillgång, en anläggning, utrustning, ett nätverk eller ett system, som krävs för tillhandahållandet av en samhällsviktig tjänst,
5. *kritisk verksamhetsutövare*: en offentlig eller enskild verksamhetsutövare som har identifierats enligt 2 kap. 1 § i denna lag,
6. *kritisk verksamhetsutövare av särskild europeisk betydelse*: en kritisk verksamhetsutövare som tillhandahåller den samhällsviktiga tjänsten till eller i minst sex medlemsstater samt har mottagit en underrättelse från kommissionen om detta,
7. *motståndskraft*: en kritisk verksamhetsutövares förmåga att förebygga, skydda mot, reagera på, stå emot, begränsa, absorbera, anpassa sig till och återhämta sig från en incident,
8. *NIS2-direktivet*: Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr

910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS2-direktivet),

9. *offentlig verksamhetsutövare*: en aktör som bedriver verksamhet och som är en statlig myndighet, region eller kommun,

10. *risk*: risk för förlust eller störning orsakad av en incident, som ska uttryckas som en kombination av omfattningen av förlusten eller störningen och sannolikheten för att incidenten inträffar,

11. *riskbedömning*: den övergripande processen för att fastställa arten och omfattningen av en risk genom att identifiera och analysera potentiella relevanta hot, sårbarheter och faror som skulle kunna leda till en incident och genom att utvärdera den potentiella förlusten eller störningen i samband med tillhandahållandet av en samhällsviktig tjänst till följd av den incidenten,

12. *samhällsviktig tjänst*: en tjänst som är avgörande för att upprätthålla viktiga samhällsfunktioner, ekonomisk verksamhet, folkhälsa och allmän säkerhet, eller miljön,

13. *standard*: en standard enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EU) nr 1025/2012[1],

14. *teknisk specifikation*: en teknisk specifikation enligt definitionen i artikel 2.4 i förordning (EU) nr 1025/2012.

Lagens tillämpningsområde

3 § Lagen gäller för enskilda och offentliga verksamhetsutövare som har identifierats som kritiska enligt 2 kap. 1 §.

4 § För kritiska verksamhetsutövare inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur gäller inte 3–6 kap.

Undantag från lagens tillämpningsområde

Krav i andra författningar

5 § Lagen gäller inte för sådant som regleras i lagen om cybersäkerhet (2025:000).

6 § Om annan författning innehåller bestämmelser om krav på riskbedömning, åtgärder för motståndskraft, bakgrundskontroller och incidentrapportering ska de bestämmelserna gälla om kraven minst motsvarar verkan av skyldigheterna enligt denna lag. Vid bedömningen ska bestämmelsernas omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till kraven i bestämmelserna beaktas.

Regeringen får i föreskrifter ange vilka bestämmelser om riskbedömning, åtgärder för motståndskraft, bakgrundskontroller och incidentrapportering som har motsvarande verkan.

[1] Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG (EUT L 316, 14.11.2012, s. 12).

Offentliga verksamhetsutövare

7 § Lagen gäller inte för regeringen, Regeringskansliet, utlandsmyndigheter, kommittéväsendet, Riksrevisionen, Riksdagens ombudsmän, Sveriges Riksbank, Riksdagsförvaltningen och Sveriges domstolar.

Brottsbekämpning eller Sveriges säkerhet

8 § Lagen gäller inte för statliga myndigheter som till övervägande del bedriver brottsbekämpning eller säkerhetskänslig verksamhet enligt säkerhetsskyddslagen (2018:585).

För offentliga verksamhetsutövare som utövar brottsbekämpning eller säkerhetskänslig verksamhet, men utan att göra detta till övervägande del, gäller inte 3–6 kap. för den del av den samhällsviktiga tjänsten som utgör brottsbekämpning eller är säkerhetskänslig.

Regeringen får i föreskrifter ange vilka statliga myndigheter som till övervägande del bedriver brottsbekämpning eller säkerhetskänslig verksamhet.

För enskilda verksamhetsutövare som bedriver säkerhetskänslig verksamhet gäller inte 3–6 kap. för den del av den samhällsviktiga tjänsten som är säkerhetskänslig.

9 § Skyldighet att lämna uppgifter enligt denna lag gäller inte uppgifter som är säkerhetsskyddsklassificerade enligt säkerhetsskyddslagen (2018:585).

10 § Tillsynsmyndighetens undersökningsbefogenheter i denna lag omfattar inte sådana delar av områden, lokaler eller andra utrymmen där säkerhetskänslig verksamhet enligt säkerhetsskyddslagen (2018:585) bedrivs.

Nationell riskbedömning

11 § Regeringen eller den myndighet regeringen bestämmer ska göra en nationell riskbedömning. Den nationella riskbedömningen ska uppdateras vid behov men minst vart fjärde år.

Den nationella riskbedömningen ska åtminstone ange:

1. Vilka relevanta risker som uppstår till följd av beroendet mellan de sektorer som anges i bilagan till CER-direktivet. Bedömningen ska även ta hänsyn till sektorernas beroende till verksamhetsutövare i EU och i tredje land.
2. Konsekvenserna som en betydande störning i en sektor kan få för andra sektorer, inklusive betydande risker för medborgare och den inre marknaden.
3. Information om de incidenter som har rapporterats enligt 5 kap.

Vid framtagandet av den nationella riskbedömningen ska alla relevanta risker beaktas, och åtminstone de riskbedömningar som gjorts enligt artikel 6.1 i Europaparlamentets och rådets beslut nr 1313/2013/EU,

Europaparlamentets och rådets förordningar (EU) 2017/1938[2] och (EU) 2019/941[3] och Europaparlamentets och rådets direktiv 2007/60/EG[4] och 2012/18/EU[5].

2 kap. Identifiering av kritiska verksamhetsutövare

1 § Tillsynsmyndigheten ska genom beslut identifiera kritiska verksamhetsutövare inom sitt tillsynsområde.

Skyldigheten att göra en riskbedömning enligt 4 kap. 1 § börjar gälla nio månader efter den dag verksamhetsutövaren har fått del av beslutet i första stycket. Övriga skyldigheter i 4–6 kap. börjar gälla tio månader efter den dag verksamhetsutövaren fått del av samma beslut.

2 § För att identifieras som kritisk verksamhetsutövare enligt 1 § krävs att

1. verksamhetsutövaren tillhandahåller en samhällsviktig tjänst i eller till Sverige och som omfattas av någon av sektorerna som finns i bilagan till CER-direktivet,
2. verksamhetsutövaren har kritisk infrastruktur belägen i Sverige, och
3. en incident skulle få en betydande störande effekt för verksamhetsutövarens tillhandahållande av den samhällsviktiga tjänsten.

Vid identifiering ska tillsynsmyndigheten beakta den nationella riskbedömningen och strategin för kritiska verksamhetsutövares motståndskraft samt kommissionens genomförandeakter på området.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om när en störande effekt är betydande enligt första stycket 3.

3 § Tillsynsmyndigheten ska i sitt beslut enligt 1 § upplysa den kritiska verksamhetsutövaren om

1. tidsfristerna som följer av 1 § andra stycket, och
2. bestämmelserna i 1 kap. 7 § och 2 kap. 1 § 8 lagen (2025:000) om cybersäkerhet.

Om den kritiska verksamhetsutövaren är verksam inom sektorerna bankverksamhet, finansmarknadsinfrastruktur eller digital infrastruktur ska det framgå av beslutet att verksamhetsutövaren inte är skyldig att vidta sådana åtgärder som följer av 3–6 kap.

[2] Europaparlamentets och rådets förordning (EU) 2017/1938 av den 25 oktober 2017 om åtgärder för att säkerställa försörjningstryggheten för gas och om upphävande av förordning (EU) nr 994/2010 (EUT L 280, 28.10.2017, s. 1).
[3] Europaparlamentets och rådets förordning (EU) 2019/941 av den 5 juni 2019 om riskberedskap inom elsektorn och om upphävande av direktiv 2005/89/EG (EUT L 158, 14.6.2019, s. 1).
[4] Europaparlamentets och rådets direktiv 2007/60/EG av den 23 oktober 2007 om bedömning och hantering av översvämningsrisker (EUT L 288, 6.11.2007, s. 27).
[5] Europaparlamentets och rådets direktiv 2012/18/EU av den 4 juli 2012 om åtgärder för att förebygga och begränsa faran för allvarliga olyckshändelser där farliga ämnen ingår och om ändring och senare upphävande av rådets direktiv 96/82/EG (EUT L 197, 24.7.2012, s. 1).

Underrättelse om säkerhetskänslig verksamhet

4 § Om en kritisk verksamhetsutövare anger att den samhällsviktiga tjänsten till någon del träffas av bestämmelserna i säkerhetsskyddslagen (2018:585) ska tillsynsmyndigheten enligt denna lag underrätta ansvarig tillsynsmyndighet enligt säkerhetsskyddslagen (2018:585) om detta förhållande.

Underrättelse om avidentifiering

5 § Om tillsynsmyndigheten beslutar att en verksamhetsutövare inte längre är kritisk ska den omedelbart underrätta verksamhetsutövaren om detta.

Förteckning över kritiska verksamhetsutövare

6 § Den myndighet regeringen bestämmer ska upprätta en förteckning över kritiska verksamhetsutövare. Förteckningen ska uppdateras vid behov men minst vart fjärde år.

3 kap. Kritiska verksamhetsutövare av särskild europeisk betydelse

Anmälningsskyldighet för vissa kritiska verksamhetsutövare

1 § En kritisk verksamhetsutövare som identifierats enligt 2 kap. 1 § och som tillhandahåller den samhällsviktiga tjänsten till eller i minst sex medlemsstater ska utan dröjsmål anmäla detta till tillsynsmyndigheten. Anmälningsskyldigheten gäller inte kritiska verksamhetsutövare inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur.

Av anmälan ska det framgå vilken samhällsviktig tjänst som tillhandahålls och till eller i vilka medlemsstater den tillhandahålls.

Samråd med kommissionen

2 § Den myndighet regeringen bestämmer ska delta i kommissionens samråd enligt artikel 17.2 i CER-direktivet.

En kritisk verksamhetsutövare som har anmält sig enligt 1 § ska delta i kommissionens samråd enligt artikel 17.2 i CER-direktivet.

Underrättelse om identifiering

3 § Den myndighet regeringen bestämmer ska underrätta en kritisk verksamhetsutövare om kommissionens underrättelse om att denna är att betrakta som kritisk verksamhetsutövare av särskild europeisk betydelse.

Bestämmelsen om skyldigheter i 5 § ska tillämpas från och med den dagen den kritiska verksamhetsutövaren mottagit kommissionens underrättelse.

Rådgivande uppdrag

4 § Ett rådgivande uppdrag anordnas av kommissionen och genomförs inom ramen för en tillsyn.

Syftet med ett rådgivande uppdrag är att bedöma de åtgärder som den kritiska verksamhetsutövaren av särskild europeisk betydelse har vidtagit för att uppfylla skyldigheterna i 4–6 kap.

5 § En kritisk verksamhetsutövare av särskild europeisk betydelse ska på begäran av Myndigheten för samhällsskydd och beredskap tillhandahålla riskbedömning enligt 4 kap. 1 § och en förteckning över relevanta åtgärder som vidtagits enligt 4 kap. 2 §.

4 kap. Riskbedömning och åtgärder för motståndskraft

1 § En verksamhetsutövare ska göra en riskbedömning senast nio månader efter att den har fått del av beslutet om att den identifierats som en kritisk verksamhetsutövare.

Riskbedömningen ska innehålla en redogörelse för alla relevanta risker som skulle kunna leda till en incident.

Riskbedömningen ska uppdateras vid behov men minst vart fjärde år.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om riskbedömning.

2 § Kritiska verksamhetsutövare ska vidta tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa sin motståndskraft. Åtgärderna ska utgå från ett allriskperspektiv och vara proportionella i förhållande till risken. De ska vidtas på grundval av verksamhetsutövarens riskbedömning samt annan relevant information och inkludera åtgärder som är nödvändiga för att

1. förhindra incidenter från att uppstå,
2. reagera på, stå emot och begränsa konsekvenserna av incidenter,
3. återhämta sig från incidenter,
4. säkerställa ett tillfredsställande fysiskt skydd av lokaler och kritisk infrastruktur,
5. säkerställa en ändamålsenlig hantering av personalsäkerhet, och
6. öka kunskapen om åtgärderna för motståndskraft hos berörd personal.

Kritiska verksamhetsutövare ska upprätta och tillämpa en plan för motståndskraft eller ett eller flera likvärdiga dokument som beskriver de åtgärder som vidtagits eller ska vidtas enligt första stycket.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om åtgärder och planer för motståndskraft.

3 § Kritiska verksamhetsutövare ska utse en samverkansansvarig som utgör kontaktpunkt för berörda myndigheter.

5 kap. Incidentrapportering

1 § Kritiska verksamhetsutövare ska utan onödigt dröjsmål rapportera incidenter som medför eller kan medföra en betydande störning i tillhandahållandet av samhällsviktiga tjänster.

En första rapport ska lämnas inom 24 timmar efter det att verksamhetsutövaren fått kännedom om en incident. En detaljerad rapport ska lämnas senast en månad efter att den första rapporten lämnades.

Rapporteringen ska göras till den myndighet som regeringen bestämmer.

2 § Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om vad som utgör en betydande störning och om incidentrapporteringen enligt 1 §.

6 kap. Bakgrundskontroll

1 § Syftet med en bakgrundskontroll är att endast den som bedöms vara lämplig ska få vara anställd eller på annat sätt delta i befattningar där deltagandet kan orsaka mer än ringa skada på den samhällsviktiga tjänsten.

2 § Kritiska verksamhetsutövare ska föra en förteckning över befattningar med krav på bakgrundskontroll (befattningsanalys). Befattningsanalysen ska utgå från den kritiska verksamhetsutövarens riskbedömning och åtminstone innehålla uppgift om vilka befattningar där deltagande kan orsaka mer än ringa skada på den samhällsviktiga tjänsten.

Befattningsanalysen ska dokumenteras och uppdateras vid behov, men minst en gång om året.

3 § Kritiska verksamhetsutövare ska säkerställa att en person som deltar i verksamhet där deltagandet kan orsaka mer än ringa skada på en samhällsviktig tjänst har genomgått en bakgrundskontroll och bedömts som lämplig för sådant deltagande. Detsamma gäller den som övervägs för rekrytering till sådan befattning.

Endast den som har genomgått bakgrundskontroll och har bedömts lämplig enligt första stycket får anställas eller på annat sätt delta i sådan verksamhet.

En förnyad bakgrundskontroll och bedömning av lämplighet ska göras när det finns skäl för det, men senast inom två år från att den senaste bakgrundskontrollen genomfördes.

4 § Vid en bakgrundskontroll ska den person kontrollen avser på förfrågan från den kritiska verksamhetsutövaren

1. styrka sin identitet genom att visa en giltig och godtagbar identitetshandling för verksamhetsutövaren, och
2. visa upp ett särskilt utdrag från belastningsregistret enligt 9 § andra stycket 7 lagen (1998:620) om belastningsregister för verksamhetsutövaren. Utdraget får högst vara ett år gammalt vid tidpunkten för bakgrundskontrollen.

5 § Vid bakgrundskontroll ska den kritiska verksamhetsutövaren anteckna om den person kontrollen avser har visat upp giltig och godtagbar identitetshandling, samt sådant särskilt utdrag ur belastningsregistret som avses i 4 §.

Anteckningar enligt första stycket ska bevaras i två år från tidpunkten för bakgrundskontrollen.

6 § Ett säkerhetsgodkännande enligt CER-direktivet ska ha samma innebörd som en bakgrundskontroll enligt denna lag.

Regeringen får genomföra bakgrundskontroll och utfärda säkerhetsgodkännande för personer som ska företräda Sverige i Gruppen för kritiska entiteters motståndskraft enligt artikel 19 i CER-direktivet.

7 § Regeringen eller den myndighet regeringen bestämmer får genomföra bakgrundskontroll och utfärda säkerhetsgodkännande för personer som föreslås delta i ett rådgivande uppdrag enligt artikel 18 i CER-direktivet.

7 kap. Tillsyn

Tillsynsmyndighet

1 § Den myndighet som regeringen bestämmer ska vara tillsynsmyndighet.

Tillsynsmyndighetens uppdrag

2 § Tillsynsmyndigheten ska utöva tillsyn över att denna lag och föreskrifter som meddelats i anslutning till lagen följs samt inom ramen för tillsyn genomföra rådgivande uppdrag enligt 3 kap. 4 §.

Tillsynsmyndigheten ska även bidra med underlag till den nationella riskbedömningen enligt 1 kap. 11 §.

Tillsynsmyndighetens undersökningsbefogenheter

3 § Den som står under tillsyn ska på begäran tillhandahålla tillsynsmyndigheten den information som behövs för tillsynen och den nationella riskbedömningen enligt 1 kap. 11 §.

4 § Tillsynsmyndigheten har i den omfattning det behövs för tillsynen rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamheten.

5 § Tillsynsmyndigheten får förelägga den som står under tillsyn att tillhandahålla information och ge tillträde enligt 3 och 4 §§.

Ett sådant föreläggande får förenas med vite.

6 § Tillsynsmyndigheten får begära handräckning av Kronofogdemyndigheten. Vid handräckning gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande.

8 kap. Ingripande och sanktioner

Överträdelser som kan leda till sanktioner

1 § Tillsynsmyndigheten ska ingripa om en kritisk verksamhetsutövare har åsidosatt sina skyldigheter enligt denna lag, eller föreskrifter som har meddelats med stöd av bestämmelserna om

1. anmälan enligt 3 kap. 1 §,
2. riskbedömning enligt 4 kap. 1 §,
3. åtgärder och plan för motståndskraft enligt 4 kap. 2 §,
4. samverkansansvarig enligt 4 kap. 3 §,
5. incidentrapportering enligt 5 kap. 1 §,
6. befattningsanalys enligt 6 kap. 2 §,
7. genomförande av bakgrundskontroll enligt 6 kap. 3 § eller antecknande samt bevarande av viss information vid bakgrundskontroll enligt 6 kap. 5 §.

2 § Ingripanden sker genom att tillsynsmyndigheten beslutar om

1. föreläggande enligt 4 §,
2. sanktionsavgift enligt 5 §, eller
3. anmärkning.

Om tillsynsmyndigheten inte finner skäl att besluta om sanktioner enligt första stycket 1 eller 2 ska den i stället besluta om en anmärkning.

3 § Tillsynsmyndigheten får avstå från att ingripa enligt 2 § om överträdelsen är ringa eller ursäktlig, eller om det annars med hänsyn till omständigheterna vore oskäligt att besluta om sanktion.

Förelägganden

4 § Tillsynsmyndigheten får besluta att förelägga den kritiska verksamhetsutövaren att vidta åtgärder för att uppfylla skyldigheterna som följer av 1 §.

Ett sådant föreläggande får förenas med vite.

Sanktionsavgift

5 § Tillsynsmyndigheten får besluta att en kritisk verksamhetsutövare ska betala en sanktionsavgift till följd av en överträdelse enligt 1 §.

6 § Sanktionsavgiften ska för enskilda kritiska verksamhetsutövare bestämmas till lägst 5 000 kronor och högst till det högsta av:

1. 2 procent av den kritiska verksamhetsutövarens totala globala årsomsättning under föregående räkenskapsår, eller
2. 10 000 000 euro.

7 § Sanktionsavgiften ska för offentliga kritiska verksamhetsutövare bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor.

Vad som ska beaktas särskilt vid bestämmande av sanktionsavgiftens storlek

8 § När sanktionsavgiftens storlek bestäms ska särskild hänsyn tas till den skada eller risk för skada som uppstått till följd av överträdelsen, om den kritiska verksamhetsutövaren tidigare har begått en överträdelse och de kostnader som den kritiska verksamhetsutövaren har undvikit till följd av överträdelsen.

Hinder mot att ta ut sanktionsavgift

9 § En sanktionsavgift får inte beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

Betalning, verkställighet och preskription

10 § En sanktionsavgift får endast tas ut om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Beslut om sanktionsavgift ska delges.

11 § Sanktionsavgiften ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas i rätt tid, ska tillsynsmyndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m. Vid indrivning ska verkställighet få ske enligt utsökningsbalken.

Sanktionsavgift tillfaller staten.

12 § En beslutad sanktionsavgift ska falla bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

9 kap. Övriga bestämmelser

Tystnadsplikt

1 § Den som med stöd av denna lag har fått del av uppgifter som förekommer i angelägenhet som avser bakgrundskontroller får inte obehörigen röja eller utnyttja dessa uppgifter.

I det allmännas verksamhet tillämpas i stället bestämmelserna i offentlighets- och sekretesslagen (2009:400).

Förordnande om att beslut ska gälla omedelbart

2 § Tillsynsmyndigheten får bestämma att ett beslut om föreläggande enligt denna lag ska gälla omedelbart.

Överklagande

3 § Beslut enligt denna lag eller anslutande föreskrifter får överklagas till allmän förvaltningsdomstol. När tillsynsmyndighetens beslut överklagas är tillsynsmyndigheten motpart i domstolen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Denna lag träder i kraft den 1 augusti 2025.

Förslag till lag om ändring i lagen (1998:620) om belastningsregister

Härigenom föreskrivs i fråga om lagen (1998:620) om belastningsregister att 9 § och 12 a § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

9 §[1]

En enskild har rätt att på begäran skriftligen få ta del av samtliga uppgifter ur registret om sig själv. Om sådana uppgifter finns har den enskilde även rätt att få sådan skriftlig information som anges i 4 kap. 3 § första stycket 1–8 brottsdatalagen (2018:1177). Uppgifterna ska på begäran lämnas ut utan avgift en gång per kalenderår.

En enskild som behöver ett registerutdrag om sig själv har rätt att få ett begränsat utdrag ur registret

1. för att kunna ta till vara sin rätt i ett främmande land eller få tillstånd att resa in, bosätta sig eller arbeta där,
2. enligt bestämmelser i skollagen (2010:800),
3. enligt bestämmelser i lagen (2018:1219) om försäkringsdistribution,
4. enligt bestämmelser i lagen (2007:171) om registerkontroll av personal vid vissa boenden som tar emot barn,

5. enligt bestämmelser i lagen (2010:479) om registerkontroll av personal som utför vissa insatser åt barn med funktionshinder, *eller*	5. enligt bestämmelser i lagen (2010:479) om registerkontroll av personal som utför vissa insatser åt barn med funktionshinder,
6. enligt bestämmelser i lagen (2013:852) om registerkontroll av personer som ska arbeta med barn.	6. enligt bestämmelser i lagen (2013:852) om registerkontroll av personer som ska arbeta med barn, *eller*
	7. enligt bestämmelser i lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare.
Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om vilka uppgifter ett sådant utdrag som avses i andra stycket 1–3 ska innehålla.	Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om vilka uppgifter ett sådant utdrag som avses i andra stycket 1–3 *och 7* ska innehålla.

Regeringen får meddela föreskrifter om vilka uppgifter ett sådant utdrag som avses i andra stycket 4–6 ska innehålla.

En begäran om uppgifter ur registret ska vara skriftlig. Polismyndigheten ska säkerställa att begäran görs av en behörig person.

12 a §[2]

Uppgifter ur registret får efter en begäran som sker med stöd av rådets rambeslut 2009/315/RIF av den 26 februari 2009 om organisationen av

[1] Senaste lydelse 2019:431.
[2] Senaste lydelse 2022:735.

medlemsstaternas utbyte av uppgifter ur kriminalregistret och uppgifternas innehåll lämnas ut till en myndighet i en annan medlemsstat i Europeiska unionen för något annat ändamål än att användas i ett brottmålsförfarande om motsvarande rätt att få del av uppgifterna finns för en svensk myndighet.

En uppgift som har förts in i registret med stöd av 4 a § får dock inte lämnas ut om Polismyndigheten har underrättats av en behörig myndighet i den stat som har överfört uppgiften om att uppgiften har gallrats i den staten.

Trots att motsvarande rätt saknas för en svensk myndighet enligt första stycket får uppgifter ur registret lämnas ut till en annan medlemsstat i Europeiska unionen om begäran görs med stöd av Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG.

Denna lag träder i kraft den 1 augusti 2025.

Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs i fråga om offentlighets- och sekretesslagen (2009:400)

dels att det ska införas två nya paragrafer, 15 kap. 3 c § och 18 kap. 8 d § av följande lydelse,

dels att 18 kap. 19 § ska ha följande lydelse,

dels att det i 35 kap. 1 § ska införas en ny punkt 10, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	15 kap.
	3 c §
	Sekretessen enligt 1 a § hindrar inte att Myndigheten för samhällsskydd och beredskap lämnar en uppgift som avses där till tillsynsmyndigheten enligt lagen (2025:000) om cybersäkerhet och lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare om uppgiften behövs för att tillsynsmyndigheten ska kunna fullgöra sitt uppdrag
	Detsamma gäller när en tillsynsmyndighet lämnar sådana uppgifter till Myndigheten för samhällsskydd och beredskap.
	En uppgift får lämnas endast om intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.
	18 kap.
	8 d §
	Utöver vad som följer av 8 § gäller sekretess för uppgift i en incidentrapport enligt 3 kap. 5–7 §§ lagen (2025:000) om cybersäkerhet och 5 kap. 1 § lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare samt för uppgift om åtgärd som följer av en sådan incident om det inte står klart att uppgiften kan röjas utan att den rapporterande verksamhetsutövarens verksamhet skadas eller de åtgärder som vidtagits motverkas.

19 §[1]

Den tystnadsplikt som följer av 5–7, 8, 9 och 10 §§, 11 § första stycket, 12, 12 a och 13 §§ inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Den tystnadsplikt som följer av 5–7, 8, *8 d*, 9 och 10 §§, 11 § första stycket, 12, 12 a och 13 §§ inskränker rätten enligt 1 kap. 1 och 7 §§ tryckfrihetsförordningen och 1 kap. 1 och 10 §§ yttrandefrihetsgrundlagen att meddela och offentliggöra uppgifter.

Den tystnadsplikt som följer av 1–3 §§ inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning på grund av beslut av domstol, undersökningsledare eller åklagare eller inhämtning av uppgifter enligt lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet.

Den tystnadsplikt som följer av 17 § inskränker rätten att meddela och offentliggöra uppgifter, när det är fråga om uppgift om kvarhållande av försändelse på befordringsföretag, hemlig avlyssning av elektronisk kommunikation, hemlig övervakning av elektronisk kommunikation, hemlig kameraövervakning, hemlig rumsavlyssning eller hemlig dataavläsning på grund av beslut av domstol eller åklagare.

Att den tystnadsplikt som följer av 1–3 §§ i vissa fall inskränker rätten att meddela och offentliggöra uppgifter utöver det som anges i andra stycket följer av 7 kap. 10 §, 12–18 §§, 20 § 3 och 22 § första stycket 1 och andra stycket tryckfrihetsförordningen samt 5 kap. 1 § och 4 § första stycket 1 och andra stycket yttrandefrihetsgrundlagen.

35 kap.

1 §[2]

Sekretess gäller för uppgift om en enskilds personliga och ekonomiska förhållanden, om det inte står klart att uppgiften kan röjas utan att den enskilde eller någon närstående till honom eller henne lider skada eller men och uppgiften förekommer i

1. utredning enligt bestämmelserna om förundersökning i brottmål,
2. angelägenhet som avser användning av tvångsmedel i brottmål eller i annan verksamhet för att förebygga brott,
3. angelägenhet som avser säkerhetsprövning enligt säkerhetsskyddslagen (2018:585),
4. annan verksamhet som syftar till att förebygga, uppdaga, utreda eller beivra brott eller verkställa uppbörd och som bedrivs av en

[1] Senaste lydelse 2024:477.
[2] Senaste lydelse 2024:328.

åklagarmyndighet, Polismyndigheten, Säkerhetspolisen, Skatteverket, Tullverket eller Kustbevakningen,

5. register som förs av Polismyndigheten enligt 5 kap. lagen (2018:1693) om polisens behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas med stöd av de bestämmelserna, eller uppgifter som behandlas av Säkerhetspolisen eller Polismyndigheten med stöd av lagen (2019:1182) om Säkerhetspolisens behandling av personuppgifter,

6. register som förs enligt lagen (1998:621) om misstankeregister,

7. register som förs av Skatteverket enligt lagen (2018:1696) om Skatteverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag,

8. särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 5 kap. 1 §, *eller*

9. register som förs av Tullverket enligt lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag.

8. särskilt ärenderegister över brottmål som förs av åklagarmyndighet, om uppgiften inte hänför sig till registrering som avses i 5 kap. 1 §,

9. register som förs av Tullverket enligt lagen (2018:1694) om Tullverkets behandling av personuppgifter inom brottsdatalagens område eller som annars behandlas där med stöd av samma lag, *eller*

10. angelägenhet som rör bakgrundskontroll enligt lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare.

Första stycket gäller inte om annat följer av 2, 6 eller 7 §.

För uppgift i en allmän handling gäller sekretessen i högst sjuttio år.

Denna lag träder i kraft den 1 januari 2025 i fråga om lagen (2025:000) om cybersäkerhet och i övrigt den 1 augusti 2025.

Förslag till lag om ändring i säkerhetsskyddslagen (2018:585)

Härigenom föreskrivs i fråga om säkerhetsskyddslagen (2018:585)

dels att 7 kap. 4 § ska ha följande lydelse

dels att det ska införas en ny paragraf 8 kap. 5 §, och närmast före 8 kap. 5 § en ny rubrik av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	7 kap.
	4 §[1]
En sanktionsavgift ska bestämmas till lägst 25 000 kronor och högst *50 000 000 kronor*. Sanktionsavgiften för en statlig myndighet, kommun eller region ska dock bestämmas till högst 10 000 000 kronor.	En sanktionsavgift ska bestämmas till lägst 25 000 kronor och högst *till det högsta av 120 000 000 kronor eller 2 procent av verksamhetsutövarens totala globala årsomsättning under föregående räkenskapsår*. Sanktionsavgiften för en statlig myndighet, kommun eller region ska dock bestämmas till högst 10 000 000 kronor.
	8 kap.
	Underrättelse om kritiska verksamhetsutövare
	5 §
	Tillsynsmyndigheten ska inom fem arbetsdagar från att en underrättelse enligt 2 kap. 4 § lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare har mottagits meddela tillsynsmyndigheten enligt lagen om motståndskraft hos kritiska verksamhetsutövare huruvida den kritiska verksamhetsutövaren har anmält att den bedriver säkerhetskänslig verksamhet enligt 2 kap. 6 § säkerhetsskyddslagen (2018:585).

Denna lag träder i kraft den 1 augusti 2025

[1] Senaste lydelse 2021:952.

Förslag till lag om ändring i lagen (2025:000) om cybersäkerhet

Härigenom föreskrivs i fråga om lagen (2025:000) om cybersäkerhet att 1 kap. 7 § och 2 kap. 1 § ska följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 kap.	
7 §	
Verksamhetsutövare som uppfyller kraven i 4 § med undantag för storlekskravet i 3 och som erbjuder allmänna elektroniska kommunikationsnät, allmänt tillgängliga elektroniska kommunikationstjänster, betrodda tjänster, registreringsenhet för toppdomäner, DNS-tjänster *eller* domännamnsregistrering omfattas av lagen.	Verksamhetsutövare som uppfyller kraven i 4 § med undantag för storlekskravet i 3 och som erbjuder allmänna elektroniska kommunikationsnät, allmänt tillgängliga elektroniska kommunikationstjänster, betrodda tjänster, registreringsenhet för toppdomäner, DNS-tjänster, domännamnsregistrering *eller som beslutats vara kritiska enligt 2 kap. 1 § lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare omfattas av lagen.* *För verksamhetsutövare som beslutats vara kritiska enligt 2 kap. 1 § lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare och som inte uppfyller storlekskravet i 4 § 3, börjar skyldigheterna i 3 kap. gälla tio månader efter den dag verksamhetsutövaren fått del av beslutet.*

2 kap.

1 §

Följande verksamhetsutövare är väsentliga:

1. Statliga myndigheter,

2. verksamhetsutövare som bedriver verksamhet enligt bilaga 1 till NIS2-direktivet, är en kommun eller ett lärosäte med examenstillstånd och vars verksamhet överstiger trösklarna för medelstora företag enligt artikel 2 och 3.1–3 i bilagan till kommissionens rekommendation 2003/361/EG,

3. verksamhetsutövare som erbjuder allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster och vars verksamhet är medelstora företag enligt artikel 2 och 3.1–3 i bilagan till kommissionens rekommendation 2003/361/EG,

4. kvalificerade tillhandahållare av betrodda tjänster,	
5. registreringsenheter för toppdomäner,	
6. verksamhetsutövare som erbjuder DNS-tjänster *och*	6. verksamhetsutövare som erbjuder DNS-tjänster,
7. verksamhetsutövare som anges i 1 kap. 8 § och identifierats som väsentliga enligt 33 § förordning om cybersäkerhet.	7. verksamhetsutövare som anges i 1 kap. 8 § och identifierats som väsentliga enligt 33 § förordning om cybersäkerhet, *och*
	8. verksamhetsutövare som beslutats vara kritiska verksamhetsutövare enligt lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare.

Denna lag träder i kraft den 1 augusti 2025.

Förteckning över remissinstanserna

Efter remiss har yttrande över slutbetänkandet inkommit från Affärsverket svenska kraftnät, Arbetsgivarverket, Bevakningsbranschens Yrkes- och Arbetsmiljönämnd (BYA), Bolagsverket, Brottsförebyggande rådet, Domstolsverket, Drivkraft Sverige, E-hälsomyndigheten, Energiföretagen Sverige, Energimarknadsinspektionen, Enköpings kommun, Finansiell ID-Teknik BID AB, Finansinspektionen, Fortifikationsverket, Försvarets materielverk, Försvarets radioanstalt, Försvarshögskolan, Försvarsmakten, Försvarsunderrättelsedomstolen, Försäkringskassan, Förvaltningsrätten i Linköping, Förvaltningsrätten i Umeå, Gotlands kommun, Gävle kommun, Göteborgs kommun, IKEM Innovations- och kemiindustrierna i Sverige, Inspektionen för strategiska produkter, Inspektionen för vård och omsorg, Integritetsskyddsmyndigheten, Jönköpings kommun, Kalix kommun, Kammarkollegiet, Kammarrätten i Jönköping, Karlstads kommun, Karolinska institutet, Kemikalieinspektionen, Kommerskollegium, Konkurrensverket, Kriminalvården, Kustbevakningen, Landsorganisationen i Sverige (LO), Lantbrukarnas riksförbund, Linköpings kommun, Livsmedelsverket, Luftfartsverket, Luleå kommun, Läkemedelsindustriföreningen, Läkemedelsverket, Länsstyrelsen i Blekinge län, Länsstyrelsen i Dalarnas län, Länsstyrelsen i Gotlands län, Länsstyrelsen i Gävleborgs län, Länsstyrelsen i Hallands län, Länsstyrelsen i Jönköpings län, Länsstyrelsen i Kalmar län, Länsstyrelsen i Kronobergs län, Länsstyrelsen i Norrbottens län, Länsstyrelsen i Skåne län, Länsstyrelsen i Stockholms län, Länsstyrelsen i Södermanlands län, Länsstyrelsen i Uppsala län, Länsstyrelsen i Värmlands län, Länsstyrelsen i Västerbottens län, Länsstyrelsen i Västernorrlands län, Länsstyrelsen i Västmanlands län, Länsstyrelsen i Västra Götalands län, Länsstyrelsen i Örebro län, Länsstyrelsen i Östergötlands län, Malmö kommun, Myndigheten för civilt försvar (tidigare Myndigheten för samhällsskydd och beredskap), Myndigheten för digital förvaltning, Myndigheten för psykologiskt försvar, Myndigheten för säkerhet och integritetsskydd (tidigare Säkerhets- och integritetsskyddsnämnden), Naturvårdsverket, Netnod AB, Nynäshamns kommun, Patent- och registreringsverket, Pensionsmyndigheten, Polismyndigheten, Post- och telestyrelsen, Regelrådet, Region Jönköpings län, Region Norrbotten, Region Stockholm, Region Sörmland, Region Östergötland, Rymdstyrelsen, Salems kommun, Sjöfartsverket, Skatteverket, Socialstyrelsen, Sparbankernas Riksförbund, Statens energimyndighet, Statens inspektion för försvarsunderrättelseverksamheten, Statens jordbruksverk, Statens servicecenter, Statskontoret, Stockholms kommun, Stockholms universitet, Strålsäkerhetsmyndigheten, Svensk Dagligvaruhandel, Svensk Handel, Svenska Bankföreningen, Svenska Journalistförbundet, Svenska stadsnätsföreningen, Svenska Tidningsutgivareföreningen (TU), Svenskt Näringsliv, Svenskt Vatten, Sveriges advokatsamfund, Sveriges akademikers centralorganisation (Saco), Sveriges Kommuner och Regioner, Sveriges meteorologiska och hydrologiska institut (SMHI), Säffle kommun, Säkerhets- och försvarsföretagen, Säkerhetspolisen, Tech Sverige, Teknikföretagen, Tillväxtverket, Totalförsvarets forskningsinstitut, Totalförsvarets plikt- och prövningsverk, Trafikverket, Transportföre-

tagen, Transportstyrelsen, Trelleborgs kommun, Tullverket, Umeå kommun, Uppsala universitet, Verket för innovationssystem (Vinnova), Vetenskapsrådet, Växjö kommun och Östersunds kommun.

Därutöver har yttranden inkommit från Advokatfirman Kahn Pedersen, Almega Säkerhetsföretagen, Defensify AB, GovSec Sweden AB, LawSec Sweden AB, Prolegia Research AB, Stiftelsen för Internetinfrastruktur, SJ AB, Svenska Transportarbetareförbundet, Sveriges universitets- och högskoleförbund, Sydvatten, SäkerhetsBranschen, Tågföretagen och Vattenfall AB.

Följande remissinstanser har inte svarat eller angett att de avstår från att lämna några synpunkter: Arelion Sweden AB, Chalmers tekniska högskola AB, Energigas Sverige, Falkenbergs kommun, Falu kommun, Finansbolagens Förening, Flens kommun, GlobalConnect AB, Industriarbetsgivarna i Sverige Service AB, Kalmar kommun, Karlskoga kommun, Karlskrona kommun, Kungl. Tekniska högskolan, Lantmännen, Leksands kommun, Lilla Edets kommun, Livsmedelsföretagen, Livsmedelsgrossisterna, Länsstyrelsen i Jämtlands län, Myndigheten för totalförsvarsanalys, On Tower Sweden AB/Cellnex Sverige, Region Skåne, Riksdagens ombudsmän, RISE Research Institutes of Sweden AB, Scrive AB, Stockholm Vatten och Avfall AB, Strängnäs kommun, Sundsvalls kommun, Svenska Regionala Flygplatser AB, Svenska rymdaktiebolaget (SSC), Sveriges Hamnar, Swedavia AB, Tjänstemännens centralorganisation (TCO), Västerås kommun och Östhammars kommun.

Lagrådsremissens lagförslag

Förslag till lag om motståndskraft hos kritiska verksamhetsutövare

Härigenom föreskrivs[1] följande.

1 kap. Inledande bestämmelser

Lagens tillämpningsområde och syfte

1 § Denna lag gäller för verksamhetsutövare som har identifierats som kritiska med stöd av lagen (kritiska verksamhetsutövare). Syftet med lagen är att stärka kritiska verksamhetsutövares motståndskraft och förmåga att tillhandahålla samhällsviktiga tjänster.

Bestämmelserna i lagen genomför delvis Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (här benämnt CER-direktivet).

Uttryck i lagen

2 § I denna lag betyder

1. *enskild verksamhetsutövare*: en kritisk verksamhetsutövare som inte är en offentlig verksamhetsutövare,
2. *incident*: en händelse som kan medföra en betydande störning eller som medför en störning i den kritiska verksamhetsutövarens tillhandahållande av en samhällsviktig tjänst,
3. *kritisk infrastruktur*: en tillgång, en anläggning, utrustning, ett nätverk eller ett system, eller en del av en tillgång, en anläggning, utrustning, ett nätverk eller ett system, som krävs för tillhandahållandet av en samhällsviktig tjänst,
4. *motståndskraft*: förmågan att förebygga, skydda mot, reagera på, stå emot, begränsa konsekvenserna av, absorbera, anpassa sig till och återhämta sig från en incident,
5. *offentlig verksamhetsutövare*: en kritisk verksamhetsutövare som är
   a) en statlig myndighet, eller
   b) en region, en kommun eller ett kommunalförbund,
6. *samhällsviktig tjänst*: en tjänst som är avgörande för att upprätthålla centrala samhällsfunktioner, ekonomisk verksamhet, folkhälsa, allmän säkerhet eller miljön och som omfattas av bilagan till CER-direktivet, i den ursprungliga lydelsen.

[1] Jfr Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG, i den ursprungliga lydelsen.

Undantag från lagens tillämpningsområde

3 § Om det i lag eller annan författning finns bestämmelser som innehåller krav på åtgärder för motståndskraft ska de bestämmelserna gälla om verkan av kraven minst motsvarar verkan av skyldigheterna enligt denna lag med beaktande av bestämmelsernas omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till kraven i bestämmelserna.

4 § För en verksamhetsutövare som har identifierats som kritisk inom någon eller några av sektorerna bankverksamhet, finansmarknadsinfrastruktur eller digital infrastruktur i bilagan till CER-direktivet, i den ursprungliga lydelsen, gäller inte skyldigheterna enligt denna lag för den delen av verksamheten.

5 § Denna lag gäller inte för en statlig myndighet som till övervägande del bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen (2018:585) eller som till övervägande del bedriver brottsbekämpande verksamhet.

För en enskild verksamhetsutövare som enbart bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen eller som enbart erbjuder tjänster till sådana statliga myndigheter som avses i första stycket gäller inte skyldigheterna enligt denna lag.

För andra verksamhetsutövare som till någon del bedriver sådan verksamhet eller erbjuder sådana tjänster som avses i första eller andra stycket gäller inte skyldigheterna enligt denna lag för den delen av verksamheten.

6 § Skyldigheterna att lämna uppgifter enligt denna lag gäller inte uppgifter som är säkerhetsskyddsklassificerade enligt säkerhetsskyddslagen (2018:585).

7 § Denna lag gäller inte för regeringen, Regeringskansliet, utlandsmyndigheter, kommittéväsendet, myndigheter under riksdagen, domstolar och inte heller för nämnder som utövar rättskipning.

Lagen gäller inte heller för förbundsfullmäktige eller förbundsdirektion i ett kommunalförbund, kommunfullmäktige och regionfullmäktige.

Uppdrag enligt CER-direktivet

8 § Den myndighet som regeringen bestämmer ska göra en nationell riskbedömning och vara gemensam kontaktpunkt enligt artiklarna 5 och 9 i CER-direktivet, i den ursprungliga lydelsen.

Bemyndigande

9 § Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om vad som utgör en incident enligt 2 § 2.

2 kap. Identifiering av kritiska verksamhetsutövare

1 § Den eller de myndigheter som regeringen bestämmer ska i enskilda fall besluta om identifiering av kritiska verksamhetsutövare.

2 § För att identifieras som kritisk verksamhetsutövare enligt 1 § krävs att

1. verksamhetsutövaren tillhandahåller en eller flera samhällsviktiga tjänster,

2. verksamhetsutövaren

a) omfattas av någon av kategorierna i bilagan till CER-direktivet, i den ursprungliga lydelsen, eller

b) är en statlig myndighet som regeringen i övrigt bestämmer ska kunna omfattas av lagen,

3. verksamhetsutövaren bedriver verksamhet i och har kritisk infrastruktur belägen i Sverige, och

4. en incident skulle få en betydande störande effekt för

a) verksamhetsutövarens tillhandahållande av en eller flera samhällsviktiga tjänster, eller

b) tillhandahållandet av andra samhällsviktiga tjänster som är beroende av den eller de samhällsviktiga tjänster som verksamhetsutövaren tillhandahåller.

3 § En kritisk verksamhetsutövares skyldigheter enligt 3 kap. 3–9 §§ börjar gälla tio månader efter det att verksamhetsutövaren har fått del av ett sådant beslut som avses i 1 §.

4 § En sådan myndighet som avses i 1 § ska så snart det kan ske fatta beslut om att en verksamhetsutövare inte längre ska anses som en kritisk verksamhetsutövare, om myndigheten bedömer att kraven enligt 2 § inte längre är uppfyllda.

Ett beslut enligt första stycket ska gälla omedelbart.

5 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om vad som utgör en betydande störande effekt enligt 2 § 4.

3 kap. Skyldigheter för kritiska verksamhetsutövare

Anmälningsskyldighet

1 § En kritisk verksamhetsutövare som tillhandahåller en samhällsviktig tjänst till eller i minst sex medlemsstater inom Europeiska unionen ska så snart det kan ske anmäla detta till den eller de myndigheter som regeringen bestämmer.

Riskbedömning

2 § En kritisk verksamhetsutövare ska göra en riskbedömning senast nio månader efter det att denne har fått del av ett sådant beslut som avses i 2 kap. 1 §.

Riskbedömningen ska dokumenteras och innehålla en redogörelse för alla relevanta risker som skulle kunna leda till en incident.

Riskbedömningen ska uppdateras vid behov och minst vart fjärde år.

Åtgärder för motståndskraft

3 § En kritisk verksamhetsutövare ska vidta lämpliga och proportionella tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa sin motståndskraft (åtgärder för motståndskraft). Åtgärderna för motståndskraft ska vidtas på grundval av verksamhetsutövarens riskbedömning och annan relevant information samt inkludera åtgärder som är nödvändiga för att

1. förhindra att incidenter inträffar,
2. säkerställa ett tillfredsställande fysiskt skydd av lokaler och kritisk infrastruktur,
3. reagera på, stå emot och begränsa konsekvenserna av incidenter,
4. återhämta sig från incidenter,
5. säkerställa en ändamålsenlig hantering av personalsäkerhet, inbegripet åtgärder enligt 4–7 §§, och
6. öka kunskapen och medvetenheten om åtgärderna för motståndskraft hos berörd personal.

Verksamhetsutövaren ska upprätta och följa en plan för motståndskraft som beskriver de åtgärder som har vidtagits eller ska vidtas enligt första stycket.

4 § En kritisk verksamhetsutövare ska göra en analys av vilka befattningar hos verksamhetsutövaren som ska omfattas av krav på bakgrundskontroll enligt 5 § (befattningsanalys).

Befattningsanalysen ska dokumenteras och innehålla uppgifter om sådana befattningar där deltagandet i verksamheten innebär möjlighet att orsaka mer än ringa störning i den kritiska verksamhetsutövarens tillhandahållande av en eller flera samhällsviktiga tjänster.

Befattningsanalysen ska uppdateras vid behov och minst en gång om året.

5 § En kritisk verksamhetsutövare ska säkerställa att en person som deltar i eller ska delta i verksamheten, i den mån det följer av verksamhetsutövarens befattningsanalys, har genomgått en bakgrundskontroll.

En bakgrundskontroll innebär att den person som kontrollen avser ska

1. styrka sin identitet, och
2. genomgå en registerkontroll enligt 6 §.

En förnyad bakgrundskontroll ska göras när det finns skäl för det, och senast inom två år efter det att den senaste bakgrundskontrollen genomfördes.

6 § En sådan person som avses i 5 § ska på begäran av den kritiska verksamhetsutövaren visa upp ett utdrag ur det register som förs enligt lagen (1998:620) om belastningsregister för verksamhetsutövaren.

Utdraget får inte vara äldre än sex månader när det visas upp.

7 § Vid en bakgrundskontroll ska den kritiska verksamhetsutövaren anteckna om den person som kontrollen avser har styrkt sin identitet och visat upp ett sådant utdrag som avses i 6 §. Någon annan dokumentation om kontrollen får inte göras.

Anteckningar enligt första stycket ska bevaras i två år från tidpunkten för bakgrundskontrollen.

8 § En kritisk verksamhetsutövare ska utse en kontaktpunkt för tillsynsmyndigheten.

Incidentrapportering

9 § En kritisk verksamhetsutövare ska till den myndighet som regeringen bestämmer anmäla sådana incidenter som medför eller kan medföra en betydande störning i den kritiska verksamhetsutövarens tillhandahållande av en samhällsviktig tjänst.

En incidentanmälan enligt första stycket ska lämnas så snart det kan ske, dock senast 24 timmar efter det att verksamhetsutövaren har fått kännedom om incidenten. Senast en månad efter incidentanmälan ska verksamhetsutövaren lämna en rapport om incidenten till samma myndighet.

Bakgrundskontroller inför deltagande i samverkan enligt CER-direktivet

10 § Regeringen eller den myndighet som regeringen bestämmer får genomföra bakgrundskontroller enligt 5 § av personer som föreslås delta i ett rådgivande uppdrag eller företräda Sverige i gruppen för kritiska entiteters motståndskraft enligt artiklarna 18 och 19 i CER-direktivet, i den ursprungliga lydelsen.

Bemyndigande

11 § Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om riskbedömning enligt 2 §, åtgärder för motståndskraft enligt 3–8 §§ och incidentrapportering enligt 9 §.

4 kap. Tillsyn

Tillsynsmyndigheterna och tillsynsmyndigheternas uppdrag

1 § Den eller de myndigheter som regeringen bestämmer ska vara tillsynsmyndighet.

2 § En tillsynsmyndighet ska

1. utöva tillsyn över att denna lag och föreskrifter som meddelats i anslutning till lagen följs,
2. utöva tillsyn över att sådana rättsakter följs som har antagits med stöd av artikel 13.6 i CER-direktivet, i den ursprungliga lydelsen, och
3. inom ramen för sin tillsyn medverka till att rådgivande uppdrag genomförs i enlighet med artikel 18 i CER-direktivet, i den ursprungliga lydelsen.

Tillsynsmyndigheternas befogenheter

3 § Den som står under tillsyn ska på begäran tillhandahålla en tillsynsmyndighet de uppgifter eller handlingar som behövs för tillsynen.

4 § En tillsynsmyndighet har i den omfattning det behövs för tillsynen rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamhet som omfattas av tillsynen.

5 § En tillsynsmyndighet får besluta att förelägga den som står under tillsyn att tillhandahålla uppgifter eller handlingar eller ge tillträde enligt 3 och 4 §§.

Ett föreläggande får förenas med vite. Ett vitesföreläggande får även riktas mot staten.

6 § En tillsynsmyndighet får begära handräckning av Kronofogdemyndigheten för de tillsynsåtgärder som avses i 3 och 4 §§. Vid handräckning gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande.

5 kap. Ingripanden

När och hur tillsynsmyndigheterna ska ingripa

1 § En tillsynsmyndighet ska ingripa om en kritisk verksamhetsutövare har åsidosatt sina skyldigheter enligt 3 kap. 1–9 §§ eller enligt föreskrifter som meddelats i anslutning till de paragraferna eller enligt sådana rättsakter som antagits med stöd av artikel 13.6 i CER-direktivet, i den ursprungliga lydelsen.

Ett ingripande sker genom ett beslut om föreläggande enligt 2 §, ett beslut om sanktionsavgift enligt 3 § eller, om det inte finns skäl att ingripa mot en överträdelse på något annat sätt, genom anmärkning.

Tillsynsmyndigheten får avstå från ett ingripande om överträdelsen är ringa eller ursäktlig, eller om det annars med hänsyn till omständigheterna vore oskäligt att ingripa.

Förelägganden

2 § En tillsynsmyndighet får besluta de förelägganden som behövs för att en kritisk verksamhetsutövare ska uppfylla skyldigheterna som avses i 1 § första stycket.

Ett föreläggande får förenas med vite. Ett vitesföreläggande får även riktas mot staten.

Sanktionsavgift

3 § En tillsynsmyndighet får besluta att ta ut en sanktionsavgift av en kritisk verksamhetsutövare till följd av en överträdelse av de skyldigheter som avses i 1 § första stycket.

4 § Sanktionsavgiften ska bestämmas till lägst 5 000 kronor och till högst

1. det högsta av 2 procent av den kritiska verksamhetsutövarens totala globala årsomsättning under närmast föregående räkenskapsår, eller ett belopp i kronor motsvarande 10 000 000 euro för en enskild verksamhetsutövare, eller

2. 10 000 000 kronor för en offentlig verksamhetsutövare.

5 § När sanktionsavgiftens storlek bestäms ska särskild hänsyn tas till

1. den skada eller risk för skada som har uppstått till följd av överträdelsen,
2. om den kritiska verksamhetsutövaren tidigare har gjort sig skyldig till en överträdelse, och
3. den ekonomiska fördel som överträdelsen har inneburit för verksamhetsutövaren.

6 § En sanktionsavgift får inte beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

7 § En sanktionsavgift får beslutas endast om den som avgiften ska tas ut av har fått tillfälle att yttra sig inom två år från det att överträdelsen ägde rum.

Ett beslut om sanktionsavgift ska delges.

8 § En sanktionsavgift ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.

Om sanktionsavgiften inte betalas i rätt tid, ska tillsynsmyndigheten lämna den obetalda avgiften för indrivning. Bestämmelser om indrivning finns i lagen (1993:891) om indrivning av statliga fordringar m.m.

Sanktionsavgiften tillfaller staten.

9 § En sanktionsavgift faller bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

6 kap. Överklagande

1 § Tillsynsmyndighetens beslut enligt denna lag får överklagas till allmän förvaltningsdomstol. När ett sådant beslut överklagas är tillsynsmyndigheten motpart i domstolen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

Denna lag träder i kraft den 1 januari 2027.

Förslag till lag om ändring i lagen (1998:620) om belastningsregister

Härigenom föreskrivs[1] att 9 och 12 a §§ lagen (1998:620) om belastningsregister ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
9 §[2]	
En enskild har rätt att på begäran skriftligen få ta del av samtliga uppgifter ur registret om sig själv. Om sådana uppgifter finns har den enskilde även rätt att få sådan skriftlig information som anges i 4 kap. 3 § första stycket 1–8 brottsdatalagen (2018:1177). Uppgifterna ska på begäran lämnas ut utan avgift en gång per kalenderår.	
En enskild som behöver ett registerutdrag om sig själv har rätt att få ett begränsat utdrag ur registret	
1. för att kunna ta till vara sin rätt i ett främmande land eller få tillstånd att resa in, bosätta sig eller arbeta där,	
2. enligt bestämmelser i skollagen (2010:800),	
3. enligt bestämmelser i lagen (2018:1219) om försäkringsdistribution,	
4. enligt bestämmelser i lagen (2007:171) om registerkontroll av personal vid vissa boenden som tar emot barn,	
5. enligt bestämmelser i lagen (2010:479) om registerkontroll av personal som utför vissa insatser åt barn med funktionshinder,	
6. enligt bestämmelser i lagen (2013:852) om registerkontroll av personer som ska arbeta med barn,	
7. enligt bestämmelser i lagen (2026:43) om registerkontroll vid arbete i hemmet åt äldre personer eller vuxna personer med funktionsnedsättning, *eller*	7. enligt bestämmelser i lagen (2026:43) om registerkontroll vid arbete i hemmet åt äldre personer eller vuxna personer med funktionsnedsättning,
8. enligt bestämmelser i lagen (2026:44) om registerkontroll vid anställning till ledande befattningar i kommuner.	8. enligt bestämmelser i lagen (2026:44) om registerkontroll vid anställning till ledande befattningar i kommuner*, eller*
	9. enligt bestämmelser i lagen (2026:000) om motståndskraft hos kritiska verksamhetsutövare.
Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om vilka uppgifter ett sådant utdrag som avses i andra stycket 1–3 ska innehålla.	
Regeringen får meddela föreskrifter om vilka uppgifter ett sådant utdrag som avses i andra stycket 4–*8* ska innehålla.	Regeringen får meddela föreskrifter om vilka uppgifter ett sådant utdrag som avses i andra stycket 4–*9* ska innehålla.

[1] Jfr Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG, i den ursprungliga lydelsen.
[2] Senaste lydelse 2026:46.

En begäran om uppgifter ur registret ska vara skriftlig. Polismyndigheten ska säkerställa att begäran görs av en behörig person.

12 a §[3]

Uppgifter ur registret får efter en begäran som sker med stöd av rådets rambeslut 2009/315/RIF av den 26 februari 2009 om organisationen av medlemsstaternas utbyte av uppgifter ur kriminalregistret och uppgifternas innehåll lämnas ut till en myndighet i en annan medlemsstat i Europeiska unionen för något annat ändamål än att användas i ett brottmålsförfarande om motsvarande rätt att få del av uppgifterna finns för en svensk myndighet.

En uppgift som har förts in i registret med stöd av 4 a § får dock inte lämnas ut om Polismyndigheten har underrättats av en behörig myndighet i den stat som har överfört uppgiften om att uppgiften har gallrats i den staten.

Uppgifter ur registret får lämnas ut till en annan medlemsstat i Europeiska unionen om begäran görs med stöd av Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG, i den ursprungliga lydelsen. Detta gäller även om motsvarande rätt att få del av uppgifterna saknas för en svensk myndighet.

Denna lag träder i kraft den 1 januari 2027.

[3] Senaste lydelse 2022:735.

Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs[1] i fråga om offentlighets- och sekretesslagen (2009:400)

dels att 18 kap. 8 b § ska ha följande lydelse,

dels att det ska införas en ny paragraf, 15 kap. 3 d §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	15 kap.
	3 d §
	Sekretessen enligt 1 a § hindrar inte att Myndigheten för civilt försvar i egenskap av en sådan gemensam kontaktpunkt som avses i 1 kap. 8 § lagen (2026:000) om motståndskraft hos kritiska verksamhetsutövare lämnar en uppgift till en tillsynsmyndighet enligt samma lag, om uppgiften behövs för att tillsynsmyndigheten ska kunna fullgöra sitt uppdrag.
	Sekretessen hindrar inte heller att en sådan tillsynsmyndighet som avses i första stycket lämnar en uppgift till Myndigheten för civilt försvar, om uppgiften behövs för att Myndigheten för civilt försvar ska kunna fullgöra sitt uppdrag som sådan gemensam kontaktpunkt som avses i första stycket.
	En uppgift enligt första eller andra stycket får lämnas endast om intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.
	18 kap.
	8 b §[2]
Sekretess gäller för uppgift i en incidentrapport enligt cybersäkerhetslagen (2025:1506) och för uppgift om vilka åtgärder som en verksamhetsutövare har vidtagit till	Sekretess gäller för uppgift i en incidentrapport enligt cybersäkerhetslagen (2025:1506) *och lagen (2026:000) om motståndskraft hos kritiska verksamhets-*

[1] Jfr Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG, i den ursprungliga lydelsen.

[2] Senaste lydelse 2025:1508.

följd av incidenten, om det inte står klart att uppgiften kan röjas utan att den rapporterande verksamhetsutövarens framtida verksamhet skadas eller syftet med vidtagen åtgärd motverkas.	*utövare samt* för uppgift om vilka åtgärder som en verksamhetsutövare har vidtagit till följd av incidenten, om det inte står klart att uppgiften kan röjas utan att den rapporterande verksamhetsutövarens framtida verksamhet skadas eller syftet med vidtagen åtgärd motverkas.

För uppgift i en allmän handling gäller sekretessen i högst fyrtio år.

Denna lag träder i kraft den 1 januari 2027.

Förslag till lag om ändring i säkerhetsskyddslagen (2018:585)

Härigenom föreskrivs att 7 kap. 4 § säkerhetsskyddslagen (2018:585) ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
7 kap.	
4 §[1]	
En sanktionsavgift ska bestämmas till lägst 25 000 kronor och högst *50 000 000 kronor*. Sanktionsavgiften för en statlig myndighet, kommun eller region ska dock bestämmas till högst 10 000 000 kronor.	En sanktionsavgift ska bestämmas till lägst 25 000 kronor och högst *till det högsta av 120 000 000 kronor eller 2 procent av verksamhetsutövarens totala globala årsomsättning under närmast föregående räkenskapsår*. Sanktionsavgiften för en statlig myndighet, kommun eller region ska dock bestämmas till högst 10 000 000 kronor.

1. Denna lag träder i kraft den 1 januari 2027.
2. Äldre bestämmelser gäller fortfarande för överträdelser som har ägt rum före ikraftträdandet.

[1] Senaste lydelse 2021:952.

Förslag till lag om ändring i cybersäkerhetslagen (2025:1506)

Härigenom föreskrivs[1] i fråga om cybersäkerhetslagen (2025:1506)

dels att 1 kap. 9 § ska ha följande lydelse,

dels att det ska införas en ny paragraf, 1 kap. 8 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 kap.
	8 a §
	Lagen gäller också för en verksamhetsutövare som har identifierats som en kritisk verksamhetsutövare enligt 2 kap. 1 § lagen (2026:000) om motståndskraft hos kritiska verksamhetsutövare.
	9 §
Som väsentlig verksamhetsutövare räknas	
1. en verksamhetsutövare som är en statlig myndighet,	
2. en verksamhetsutövare som är större än ett medelstort företag och som	
a) är en kommun eller en region,	
b) i övrigt omfattas av bilaga 1 till NIS 2-direktivet i den ursprungliga lydelsen men inte av 7 § 2 eller 3, eller	
c) är en enskild utbildningsanordnare med tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina,	
3. en verksamhetsutövare som avses i 6 § och som storleksmässigt motsvarar eller är större än ett medelstort företag,	
4. en verksamhetsutövare som avses i 7 § 2 eller 3,	
5. en verksamhetsutövare som är en kvalificerad tillhandahållare av betrodda tjänster*, och*	5. en verksamhetsutövare som är en kvalificerad tillhandahållare av betrodda tjänster*,*
6. en verksamhetsutövare som räknas som väsentlig enligt föreskrifter som har meddelats med stöd av 15 § andra stycket.	6. en verksamhetsutövare som räknas som väsentlig enligt föreskrifter som har meddelats med stöd av 15 § andra stycket*, och*
	7. en verksamhetsutövare som avses i 8 a §.
Verksamhetsutövare som inte är väsentliga är viktiga verksamhetsutövare.	

[1] Jfr Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148, i den ursprungliga lydelsen.

Denna lag träder i kraft den 1 januari 2027.

Lagrådets yttrande

Utdrag ur protokoll vid sammanträde 2026-06-18

Närvarande: F.d. justitieråden Martin Borgeke och Mahmut Baran samt justitierådet Marie Jönsson

En ny lag för ökad motståndskraft hos kritiska verksamhetsutövare

Enligt en lagrådsremiss den 21 maj 2026 har regeringen (Försvarsdepartementet) beslutat inhämta Lagrådets yttrande över förslag till

1. lag om motståndskraft hos kritiska verksamhetsutövare,
2. lag om ändring i lagen (1998:620) om belastningsregister,
3. lag om ändring i offentlighets- och sekretesslagen (2009:400),
4. lag om ändring i säkerhetsskyddslagen (2018:585),
5. lag om ändring i cybersäkerhetslagen (2025:1506).

Förslagen har inför Lagrådet föredragits av ämnesrådet Charlotta Fröcklin och rättssakkunnige Alfred Pucek.

Förslagen föranleder följande yttrande.

Allmänt

Europaparlamentet och rådet antog den 14 december 2022 direktivet (EU) 2022/2557 om kritiska entiteters motståndskraft, det s.k. CER-direktivet. I syfte att genomföra delar av direktivet i svensk rätt har regeringen i denna lagrådsremiss lagt fram förslag till en ny lag om motståndskraft hos kritiska verksamhetsutövare.

Den föreslagna lagen innebär att offentliga och enskilda verksamhetsutövare som tillhandahåller samhällsviktiga tjänster inom vissa utpekade sektorer ska identifieras som kritiska verksamhetsutövare. De som på detta sätt är identifierade ska vidta åtgärder för en ökad motståndskraft och ska även ha en skyldighet att i vissa fall rapportera om inträffade incidenter. Den nya lagen ska också innehålla bestämmelser om tillsyn av och ingripandemöjligheter mot verksamhetsutövare som inte följer lagens bestämmelser.

Dessutom föreslås bl.a. en ändring i säkerhetsskyddslagen.

Den nya lagen och lagändringarna föreslås träda i kraft den 1 januari 2027.

Inledningsvis finns skäl att nämna att riksdagen år 2025 antog cybersäkerhetslagen. Den lagen grundar sig också på ett EU-direktiv, nämligen det som kallas för NIS 2-direktivet (direktiv [EU] 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen). Den i remissen föreslagna lagen har likheter med cybersäkerhetslagen.

Det har inte varit någon enkel uppgift att genomföra de olika artiklarna i direktivet på ett sätt som överensstämmer med svensk lagstiftningstradition. Att hitta rätt svensk beteckning eller lämpliga språkliga uttryckssätt avseende sådant som det talas om i direktivet är i en del fall svårt. Samtidigt är det viktigt att den svenska lagstiftningen i alla olika delar stämmer överens med innebörden av CER-direktivet.

En svårighet som aktualiseras direkt är vilket namn som den föreslagna lagen bör ges. I remissen föreslås som framgått ”lag om motståndskraft hos kritiska verksamhetsutövare”.

I CER-direktivets svenska text talas det om kritiska entiteter. Ordet entitet betyder enligt SAOL ”ting eller föremål”. I bilagan till CER-direktivet finns det en förteckning över kategorier av entiteter som avses. Det rör sig om olika slags företag, producenter, operatörer, systemansvariga, ledningsenheter, myndigheter, vårdgivare, offentliga förvaltningsentiteter och s.k. tillhandahållare. Dessa subjekt åläggs enligt direktivet och enligt lagförslaget skyldigheter av olika slag och ska också vara underkastade tillsyn och kunna bli föremål för ingripanden i form av förelägganden eller sanktionsavgifter.

I allmänmotiveringen har regeringen diskuterat vilken beteckning som i den svenska lagtexten bör användas för de entiteter som ska omfattas av lagen. Slutsatsen har blivit att uttrycket verksamhetsutövare är bäst. Det är den term som används i cybersäkerhetslagen.

Det är naturligtvis en fördel om terminologin i den nu föreslagna lagen i möjligaste mån överensstämmer med den som används i cybersäkerhetslagen. Lagrådet vill därför inte motsätta sig att lagen riktar sig till ”verksamhetsutövare”. Däremot anser Lagrådet att man av språkliga skäl inte gärna kan tala om ”kritiska verksamhetsutövare”. Tanken är ju att det är den verksamhet eller de funktioner som lagen tar sikte på som är ”kritiska” på så sätt att angrepp mot dessa inverkar negativt på samhällets motståndskraft. Verksamhetsutövarna kan inte sägas vara kritiska.

Uttrycket kritiska verksamhetsutövare bör alltså ersättas med något annat. Lagrådet föreslår att man i stället talar om ”verksamhetsutövare som omfattas av lagen”. Lagens namn bör kunna vara *lag om motståndskraft i samhällsviktiga tjänster*.

Innan Lagrådet kommer in på granskningen av den föreslagna nya lagen och lagändringarna vill Lagrådet något diskutera vad som i lagens 5 kap. föreslås beträffande sanktionsavgifter mot verksamhetsutövare som åsidosätter skyldigheter som de har enligt lagen. Som framgår av det följande riktar Lagrådet kritik mot förslaget i den delen. Lagrådets allmänna uppfattning är att reglerna om sanktionsavgifter hade bort utformas mera som motsvarande regler i cybersäkerhetslagen. Men frågan är större än så.

Bestämmelser om sanktionsavgifter finns numera i ett ganska stort antal olika författningar. Som Lagrådet ser det finns det därmed behov av en sammanhållande lagstiftning som behandlar de övergripande materiella och processuella förutsättningarna för sanktionsavgifter. Här kan jämföras med lagen (1985:206) om viten som innehåller generella regler som gäller för alla de bestämmelser om vite som finns i skilda lagar. Utan en sådan grundläggande lagstiftning uppkommer risker för omotiverade skillnader mellan olika lagar exempelvis beträffande förutsättningarna för sanktionsavgifter och i fråga om vad som ska beaktas när nivån på avgiften bestäms i det enskilda fallet. Det här förslaget bär syn för sägen.

Också när det gäller de processuella reglerna för sanktionsavgifter vore mera enhetliga regler en fördel.

Lagrådet har tagit upp problematiken tidigare och vill hänvisa till sitt yttrande den 26 januari 2023 över remissen Mottagningsanordningar i hamn för avfall från fartyg.

Förslaget till lag om motståndskraft hos kritiska verksamhetsutövare

Som nyss sagts bör lagens namn kunna vara lag om motståndskraft i samhällsviktiga tjänster.

1 kap. 1 §

I paragrafen anges lagens tillämpningsområde och syfte.

Med beaktande bl.a. av det som Lagrådet nyss har konstaterat avseende begreppet kritiska verksamhetsutövare föreslår Lagrådet att paragrafen ges följande lydelse.

> Syftet med denna lag är att stärka motståndskraften hos utövare av samhällsviktiga verksamheter och att värna sådana verksamheters förmåga att tillhandahålla samhällsviktiga tjänster. Lagen omfattar verksamhetsutövare som har pekats ut med stöd av lagen.
>
> Bestämmelserna i lagen genomför delvis Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (CER-direktivet). När det i lagen hänvisas till CER-direktivet avses direktivet i den ursprungliga lydelsen.

Som framgår innebär Lagrådets förslag till lydelse av paragrafen bl.a. att det redan inledningsvis anges att när det i lagen hänvisas till CER-direktivet så avses direktivet i den ursprungliga lydelsen.

1 kap. 2 §

I paragrafen finns ett antal definitioner. Vissa av de begrepp som definieras förekommer endast ett par gånger i lagen. Det kan därför ifrågasättas om någon inledande definition behövs. Beträffande definitionen av begreppet incident uppstår också den komplikationen att den används i en paragraf – 2 kap. 2 § – som en del av en av förutsättningarna för att en verksamhet ska omfattas av lagen, vilket har fört med sig att regleringen är svår att

förstå. Lagrådet återkommer till detta vid den aktuella paragrafen, men motsätter sig inte de föreslagna definitionerna.

Med tanke bl.a. på det som sagts inledningsvis i detta yttrande om uttrycket kritiska verksamhetsutövare behövs en del justeringar av lagtexten. Lagrådet föreslår följande lydelse.

I denna lag betyder
1. *enskild verksamhetsutövare*: en med stöd av lagen utpekad verksamhetsutövare som inte är en offentlig verksamhetsutövare,
2. *incident:* en händelse som kan medföra en betydande störning eller som medför en störning i tillhandahållandet av en eller flera samhällsviktiga tjänster,
3. *kritisk infrastruktur*: en tillgång, en anläggning, utrustning, ett nätverk eller ett system, eller en del av en tillgång, en anläggning, utrustning, ett nätverk eller ett system, som krävs för tillhandahållandet av en eller flera samhällsviktiga tjänster,
4. *motståndskraft*: förmågan att förebygga, skydda mot, reagera på, stå emot, begränsa konsekvenserna av, absorbera, anpassa sig till och återhämta sig från en incident,
5. *offentlig verksamhetsutövare*: en med stöd av lagen utpekad verksamhetsutövare som är
a) en statlig myndighet, eller
b) en region, en kommun eller ett kommunalförbund, och
6. *samhällsviktig tjänst*: en tjänst som är avgörande för upprätthållandet av centrala samhällsfunktioner, ekonomisk verksamhet, folkhälsa, allmän säkerhet eller för skyddet av miljön och som omfattas av bilagan till CER-direktivet.

Som framgått definieras incident bl.a. som en händelse som kan medföra en betydande störning i tillhandahållandet av en eller flera samhällsviktiga tjänster. Redan risken för en störning kan alltså utgöra en incident, vilket är naturligt. Det bör i författningskommentaren utvecklas vilken nivå på risken som behövs för att det ska vara fråga om en incident och även i vad mån kravet beträffande risknivån är beroende av omfattningen av den störning som skulle kunna bli resultatet av incidenten.

1 kap. 3 §

I paragrafen anges att om det i lag eller annan författning finns bestämmelser som innehåller krav på åtgärder för motståndskraft ska de bestämmelserna gälla om verkan av kraven minst motsvarar verkan av skyldigheterna enligt denna lag med beaktande av bestämmelsernas omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till kraven i bestämmelserna.

Det är alltså fråga om en konkurrensregel av innebörd att annan lag gäller före den här lagen om kraven enligt den andra lagen motsvarar minst de skyldigheter som gäller för verksamhetsutövare enligt den nu föreslagna lagen. Vad som syftas på torde vara främst föreskrifterna i cybersäkerhetslagen. I den lagens 1 kap. 10 § finns emellertid en bestämmelse av motsvarande innebörd; om det i en lag eller annan författning finns bestämmelser som innehåller krav på säkerhetsåtgärder eller incidentrapportering ska de bestämmelserna gälla om verkan av kraven minst motsvarar verkan av skyldigheterna enligt vissa paragrafer i

cybersäkerhetslagen, med beaktande av bestämmelsernas utformning samt vilken tillsyn och vilka sanktioner som är kopplade till kraven i bestämmelserna.

Med den reglering som föreslås blir det otydligt vilken lag som ska tillämpas om cybersäkerhetslagen och den här lagen har samma verkan. I författningskommentaren sägs, utan reservationer, att cybersäkerhetslagen har företräde framför den i lagrådsremissen föreslagna lagen i den mån regleringarna överlappar varandra. Detta stämmer dock inte så som Lagrådet uppfattar den föreslagna lagtexten.

För att i någon mån förtydliga lagtexten föreslår Lagrådet följande formulering.

> Om det i någon annan lag eller författning finns bestämmelser som innehåller krav på åtgärder för motståndskraft ska de bestämmelserna ha företräde om inte verkan av skyldigheterna enligt denna lag ger en större motståndskraft. Vid avgörandet av vilken lag som har företräde ska beaktas omfattningen av tillsynen och de sanktioner som är kopplade till kraven i de båda författningarna.

Om avsikten är att cybersäkerhetslagen alltid ska ha företräde framför den här lagen bör det framgå direkt av lagtexten.

1 kap. 4 §

Innebörden av paragrafen är att sådana verksamhetsutövare inom sektorerna bankverksamhet, finansmarknadsinfrastruktur eller digital infrastruktur som tas upp i bilagan till CER-direktivet inte omfattas av skyldigheterna enligt lagen när det gäller den delen av verksamheten. Skulle det vara så att en verksamhetsutövare ägnar sig åt endast den angivna typen av verksamhet uppkommer det alltså inte några skyldigheter alls enligt lagen för denna verksamhetsutövare. Däremot innebär paragrafen inte att verksamhetsutövaren undantas från att omfattas av lagen, om förutsättningarna enligt 2 kap. 2 § är uppfyllda.

Konstruktionen att omfattas av en lag men inte ha några skyldigheter enligt lagen framstår som motsägelsefull. I författningskommentaren bör det förklaras vad lagen innebär för en verksamhetsutövare avses med paragrafen.

1 kap. 5 §

I första stycket föreskrivs undantag från lagens tillämpningsområde för en statlig myndighet som till övervägande del bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen eller som till övervägande del bedriver brottsbekämpande verksamhet. I författningskommentaren sägs bl.a. att med övervägande del avses myndighetens huvudsakliga verksamhet. Lagrådet vill påpeka att uttrycken ”övervägande del” och ”huvudsakliga verksamhet” knappast är synonymer. Det finns behov av ett klarläggande i författningskommentaren av vad som avses med ”till övervägande del”. Det vore också bra om det angavs praktiska exempel.

1 kap. 8 §

I paragrafen anges att den myndighet som regeringen bestämmer ska göra en nationell riskbedömning och vara gemensam kontaktpunkt enligt artiklarna 5 och 9 i CER-direktivet. Paragrafen avhandlar alltså två olika frågor som inte förefaller ha några direkta beröringspunkter.

Av författningskommentaren framgår att bestämmelsen är avsedd att vara en upplysning om den kompetens som regeringen har enligt regeringsformen att utse en myndighet för de angivna uppgifterna. Lagrådet ifrågasätter om det rör sig om endast en upplysningsbestämmelse. Som lagtexten är utformad föreligger det åtminstone den bundenheten att den myndighet som regeringen bestämmer ska vara både kontaktpunkt och göra en nationell riskbedömning. Texten i författningskommentaren bör därför övervägas på nytt.

Eftersom det rör sig om två olika väsensskilda uppdrag bör paragrafen delas upp i två stycken. Lagrådet föreslår att lagtexten blir följande.

> Den myndighet som regeringen bestämmer ska vara gemensam kontaktpunkt enligt artikel 9 i CER-direktivet.
>
> Det är en uppgift för den utsedda myndigheten att göra en nationell riskbedömning i enlighet med artikel 5 i CER-direktivet.

1 kap. 9 §

Enligt paragrafen får regeringen eller den myndighet som regeringen bestämmer meddela ytterligare föreskrifter om vad som utgör en incident enligt 2 § 2. Enligt paragrafrubriken och även enligt författningskommentaren är det fråga om ett bemyndigande för regeringen, vilket för Lagrådet framstår som en korrekt bedömning. Vad som utgör en incident är i och för sig definierat i 1 kap. 2 § 2. Det framgår där att en incident är en händelse som kan medföra en betydande störning eller som medför en störning i tillhandahållandet av en samhällsviktig tjänst. Hur en incident definieras får betydelse för vilka skyldigheter som enskilda kommer att ha enligt lagen. Därmed rör det sig om den typ av föreskrift som anges i 8 kap. 2 § första stycket 2 i regeringsformen. Sådana föreskrifter kan riksdagen med stöd av 8 kap. 3 § delegera. Formellt är det alltså möjligt att göra så som föreslås i remissen.

Lagrådet ifrågasätter emellertid om inte lagdefinitionen av incident eller i vart fall författningskommentaren avseende vad som utgör en incident borde göras mera detaljerad. Definitionen får stor betydelse för vilka skyldigheter som enligt lagen kommer att gälla för verksamhetsutövare. När bemyndigandet – som Lagrådet har uppfattat det – ska ge regeringen eller den myndighet regeringen bestämmer möjlighet att inte bara precisera vad som utgör en incident utan även att utvidga eller inskränka definitionen framstår en mera utförlig beskrivning i lagstiftningen av incidentbegreppet som motiverad. Saken bör övervägas i det fortsatta lagstiftningsarbetet. Se här även vad Lagrådet anför under 1 kap. 2 § och 2 kap. 2 § avseende incidentbegreppet.

2 kap.

Kapitlet inleds med överskriften **Identifiering av kritiska verksamhetsutövare**. Lagrådet föreslår att rubriken blir **Verksamhetsutövare som omfattas av lagen**.

2 kap. 1 §

Den föreslagna lagen innebär att en verksamhetsutövare omfattas av lagens bestämmelser först efter det att verksamhetsutövaren har pekats ut i ett särskilt beslut. Detta framgår av 1 kap. 1 §. I den här paragrafen anges att det är regeringen som utser den eller de myndigheter som ska fatta besluten.

Lagrådet föreslår att bestämmelsen formuleras så här:

> Den eller de myndigheter som regeringen bestämmer ska genom beslut i varje enskilt fall peka ut de verksamhetsutövare som ska omfattas av lagen.

2 kap. 2 §

I paragrafen anges vilka förutsättningar som ska gälla för att det ska få beslutas att en verksamhetsutövare ska omfattas av lagen.

En förutsättning för att en verksamhetsutövare ska ”identifieras som kritisk verksamhetsutövare”, dvs. ska omfattas av lagen, i punkt 4 är att en incident skulle få en betydande störande effekt för verksamhetsutövarens tillhandahållande av en eller flera samhällsviktiga tjänster eller för tillhandahållandet av andra samhällsviktiga tjänster som är beroende av den eller de samhällsviktiga tjänster som verksamhetsutövaren tillhandahåller. Denna konstruktion är problematisk.

Vad som utgör en incident är som framgått definierat i 1 kap. 2 § 2. Denna definition stämmer i stora delar överens med vad som anges i punkt 4 a). I definitionen i 1 kap. 2 § talas det visserligen om en händelse som kan medföra ”en betydande störning” medan det i förslaget till punkten 4 a) talas om att det ska röra sig om ”en incident som skulle få en betydande störande effekt”. Någon saklig skillnad mellan dessa uttryck går det emellertid knappast att utläsa och någon sådan har heller inte angetts i författningskommentaren. Det blir därmed delvis fråga om en dubbelreglering, som dessutom framstår som tämligen snårig och som även av det skälet bör undvikas.

Lagrådet föreslår, efter även några språkliga justeringar, att lagtexten blir denna:

> För att en verksamhetsutövare ska omfattas av lagen krävs att
> 1. verksamhetsutövaren tillhandahåller en eller flera samhällsviktiga tjänster,
> 2. verksamhetsutövaren
> a) omfattas av någon av kategorierna i bilagan till CER-direktivet eller
> b) är en statlig myndighet som regeringen därutöver bestämmer ska omfattas av lagen,
> 3. verksamhetsutövaren bedriver verksamhet i Sverige och har kritisk

infrastruktur belägen i Sverige, och
4. det hos verksamhetsutövaren skulle kunna inträffa en incident enligt definitionen i 1 kap. 2 § 2 eller i föreskrifter som har meddelats med stöd av denna lag eller en incident av det slaget, som skulle medföra en betydande störning för tillhandahållandet av samhällsviktiga tjänster som är beroende av den eller de samhällsviktiga tjänster som verksamhetsutövaren tillhandahåller.

Det ska medges att det av Lagrådet lämnade lagförslaget inte heller är alldeles lättläst. En dubbelreglering undviks dock. I stället används den i 1 kap. 2 § 2 givna definitionen av begreppet incident som grund för det som ska uttryckas. Någon saklig skillnad mellan remissförslaget och Lagrådets förslag är inte avsedd och finns inte heller som Lagrådet ser det.

2 kap. 3 §

I paragrafen anges när en verksamhetsutövares skyldigheter enligt 3 kap. 3 – 9 §§ börjar gälla. Lagrådet föreslår att regleringen flyttas till 3 kap.

2 kap. 5 §

Enligt paragrafen får regeringen eller den myndighet som regeringen bestämmer meddela föreskrifter om vad som utgör en betydande störande effekt enligt 2 § 4. Lagrådet har i det föregående – till undvikande av dubbelreglering – föreslagit en annan lydelse av 2 § 4. Därmed måste även den här paragrafen omformuleras.

Lagrådet föreslår följande.
Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om vad som utgör en betydande störning enligt 2 § 4.

Lagrådet har i det föregående noterat att det i 1 kap. 9 § föreslås att regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om vad som utgör en incident enligt 1 kap. 2 § 2. Som det framstår rör det sig om en delvis dubbelreglering. Frågan om hur 1 kap. 9 § förhåller sig till 2 kap. 5 § behöver övervägas i det fortsatta lagstiftningsarbetet.

Rubriken före 3 kap. bör vara: **Skyldigheter för verksamhetsutövare som omfattas av lagen.**

3 kap. 1 §

Paragrafen innehåller bestämmelser om en anmälningsskyldighet för en verksamhetsutövare som tillhandahåller ”en samhällsviktig tjänst” till eller i minst sex medlemsstater inom Europeiska unionen. Som framgår av författningskommentaren genomför paragrafen delvis artikel 17.2. I den artikeln talas det emellertid om samhällsviktiga tjänster i pluralis. Och hur man i sammanhanget ska uppfatta artikel 17 p. 1 b) i direktivet, där uttrycket ”samma eller liknande samhällsviktiga tjänster” används, förklaras inte. Lagrådet anser att dessa frågor bör redas ut i författningskommentaren.

3 kap. 2 §

I paragrafen finns regler för den riskbedömning som ska göras. Den föreslagna lydelsen av andra stycket kan, när det gäller risker för en incident, uppfattas som något av en pleonasm. Dessutom kan det diskuteras om paragrafen behöver vara indelad i så många som tre olika stycken.

Lagrådet föreslår följande formulering av paragrafen.

> En verksamhetsutövare ska göra en riskbedömning senast nio månader efter det att denne har fått del av ett sådant beslut som avses i 2 kap. 1 §.
>
> Riskbedömningen ska dokumenteras och innehålla en redogörelse för alla relevanta risker som finns för en incident. Den ska uppdateras vid behov och senast efter fyra år.

3 kap. 3 §

Paragrafen anger vilka åtgärder för motståndskraft som en verksamhetsutövare ska vidta. Den har samband med den definition av motståndskraft som finns i 1 kap. 2 §.

I första stycket 1 sägs bl.a. att åtgärderna för motståndskraft ska inkludera sådant som är nödvändigt för att förhindra att incidenter inträffar. En så hög ambitionsnivå är emellertid inte avsedd, och för övrigt knappast heller realistisk. Detta framgår i och för sig redan av den inledande delen av paragrafen där det står att det som krävs av verksamhetsutövaren är att denne vidtar ”lämpliga och proportionella åtgärder för att säkerställa sin motståndskraft”. I författningskommentaren sägs också att uttrycket ”nödvändiga” inte ska tolkas som att en verksamhetsutövare har en skyldighet att se till att det t.ex. aldrig inträffar en incident i verksamheten. Lagens innebörd bör avspeglas tydligare i lagtexten.

En annan fråga som det finns anledning att uppmärksamma är att en verksamhetsutövare, för att säkerställa sin motståndskraft, enligt första stycket 5 ska vidta åtgärder som är nödvändiga för säkerställandet av en ändamålsenlig hantering av personalsäkerhet. I detta inbegrips en skyldighet att i vissa fall agera arbetsrättsligt mot anställda. Lagrådet återkommer till denna fråga under 3 kap. 5 §.

Lagrådet föreslår att lagtexten i första stycket ges den här lydelsen:

> En verksamhetsutövare ska vidta lämpliga och proportionella tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa sin motståndskraft. Åtgärderna för motståndskraft ska vidtas på grundval av verksamhetsutövarens riskbedömning och annan relevant information samt inkludera sådant som syftar till att
> 1. förebygga att incidenter inträffar,
> 2. säkerställa ett tillfredsställande fysiskt skydd av lokaler och kritisk infrastruktur,
> 3. reagera på, stå emot och begränsa konsekvenserna av incidenter,
> 4. verksamhetsutövaren ska kunna återhämta sig från incidenter,
> 5. säkerställa en ändamålsenlig hantering av personalsäkerhet, inbegripet åtgärder enligt 4–7 §§, och

Som förklaring till den i förhållande till remissförslaget annorlunda formuleringen av punkt 6 vill Lagrådet påpeka att i artikel 13.1 och 13.1 f) anges att medlemsstaterna ska säkerställa att kritiska entiteter vidtar åtgärder för att säkerställa sin motståndskraft, inbegripet åtgärder som är nödvändiga för att öka medvetenheten om de aktuella åtgärderna hos berörd personal, med vederbörlig hänsyn till utbildningskurser, informationsmaterial och övningar. I remissförslaget har detta översatts med ”öka kunskapen och medvetenheten om åtgärderna för motståndskraft hos berörd personal”. Som Lagrådet uppfattar direktivet ska det emellertid krävas mera än medvetenhet och kunskap hos personalen om åtgärderna för motståndskraft. I själva verket torde personalens förmåga att delta i åtgärderna för motståndskraft vara en avgörande förutsättning för att syftet med lagen ska uppnås. Då räcker det knappast att personalen känner till eller är medveten om vad som krävs i sammanhanget.

3 kap. 4 §

I paragrafen finns regler som innebär att en verksamhetsutövare ska analysera vilka befattningshavare hos denne som ska omfattas av en sådan bakgrundskontroll som det föreskrivs om i 3 kap. 5 §.

En fråga med anledning av paragrafens krav på bakgrundskontroller av personal är vad som ska gälla för verksamhetsutövaren själv när denne inte är en juridisk person. Situationen torde vara ovanlig, men bör kunna förekomma. Lagtexten hindrar i och för sig inte att en fysisk verksamhetsutövare kontrolleras, men det är svårt att se hur det ska gå till i praktiken. Saken bör behandlas i författningskommentaren.

3 kap. 5 §

I paragrafen föreskrivs att en verksamhetsutövare ska säkerställa att en person som deltar i eller ska delta i verksamheten har genomgått en bakgrundskontroll om befattningsanalysen enligt 3 kap. 4 § har lett fram till att han eller hon omfattas av ett sådant krav. En bakgrundskontroll består i att den person som ska kontrolleras ska styrka sin identitet och genomgå en registerkontroll enligt 3 kap. 6 §.

Frågan är emellertid vad verksamhetsutövaren är skyldig att göra om någon anställd som ska kontrolleras vägrar att genomgå kontrollen eller om kontrollen utfaller på sådant sätt, att personen måste omplaceras eller möjligen sägas upp eller avskedas. Problematiken behandlas endast kortfattat i författningskommentaren. Det sägs där att verksamhetsutövaren fall av detta slag behöver vidta åtgärder, vilket kan inbegripa arbetsrättsliga sådana.

Lagrådet ser det som en brist att det i remissförslaget inte finns någon bestämmelse som direkt adresserar vilka krav och möjligheter som ska finnas att vidta arbetsrättsliga åtgärder med stöd av lagen. Det som

lagförslaget innehåller är endast olika regler för hur personalkontrollen ska gå till, men alltså ingen reglering av vad resultatet av kontrollen ska få för följd om det är negativt i fråga om en anställd befattningshavare. Åtminstone bör frågan om hur det arbetsrättsliga regelverket förhåller sig till lagförslaget redas ut på ett mera heltäckande sätt än som har skett i remissen.

3 kap. 6 §

I paragrafen föreskrivs en skyldighet för den som ska genomgå en bakgrundskontroll att visa upp ett utdrag ur belastningsregistret.

Lagrådet föreslår att lagtexten utformas så här:

> En person som avses i 5 § ska på begäran av verksamhetsutövaren visa upp ett utdrag ur det register som förs enligt lagen (1998:620) om belastningsregister. Utdraget får inte vara äldre än sex månader.

3 kap. 8 §

Enligt paragrafen ska en verksamhetsutövare utse en kontaktpunkt för tillsynsmyndigheten. Detta framstår i vart fall inte omedelbart som en åtgärd för motståndskraft, vilket är den rubrik som paragrafen står under. En paragrafrubrik före 3 kap. 8 § av lydelsen **Kontaktpunkt** bör övervägas.

3 kap. 9 §

Paragrafen gäller skyldighet att rapportera incidenter.

Lagtextens första stycket kan hellre skrivas så här:

> En verksamhetsutövare ska till den myndighet som regeringen bestämmer anmäla sådana incidenter som har medfört eller hade kunnat medföra en betydande störning i verksamhetsutövarens tillhandahållande av en samhällsviktig tjänst.

4 kap. 2 §

I paragrafen regleras uppdraget för en tillsynsmyndighet. Enligt tredje punkten ska en tillsynsmyndighet inom ramen för sin tillsyn medverka till att rådgivande uppdrag genomförs i enlighet med artikel 18 i CER-direktivet. I den angivna artikeln sägs, i punkt 1, att kommissionen, på begäran att den medlemsstat som har identifierat en kritisk entitet av särskild europeisk betydelse som en kritisk entitet enligt artikel 6.1, ska anordna ett rådgivande uppdrag för att bedöma de åtgärder som den kritiska entiteten har infört för att uppfylla sina skyldigheter avseende motståndskraft. Varje rådgivande uppdrag ska bestå av experter från den medlemsstat där den kritiska entiteten av särskild europeisk betydelse är belägen, experter från de medlemsstater till eller i vilka den samhällsviktiga tjänsten tillhandahålls och företrädare för kommissionen. Det rådgivande uppdraget kan därmed sägas vara en sorts expertgrupp med en särskild uppgift.

Lagrådet föreslår följande lagtext.

En tillsynsmyndighet ska
1. utöva tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs,
2. utöva tillsyn över att sådana rättsakter följs som har antagits med stöd av artikel 13.6 i CER-direktivet och
3. inom ramen för sin tillsyn, om förutsättningarna för det är uppfyllda, medverka till att ett sådant rådgivande uppdrag som avses i artikel 18 i CER-direktivet anordnas av kommissionen och att det rådgivande uppdraget därefter genomförs i enlighet med direktivet.

4 kap. 3 §

I paragrafen föreskrivs att den som står under tillsyn, på begäran av en tillsynsmyndighet, ska tillhandahålla de uppgifter eller handlingar som behövs för tillsynen.

Rubriken omedelbart före paragrafen – och de tre därefter följande paragraferna – är **Tillsynsmyndigheternas befogenheter**. Det kan diskuteras om rubriken träffar rätt; enligt paragrafen är det ju den som står under tillsyn som åläggs en skyldighet, låt vara att den ska uppfyllas på en tillsynsmyndighets begäran. Bättre hade varit att som rubrik skriva endast **Tillsynen** eller **Innehållet i tillsynen**, alternativt **Utövandet av tillsynen**. Eftersom rubriktexten stämmer överens med motsvarande rubrik i cybersäkerhetslagen låter Lagrådet emellertid saken bero med denna anmärkning.

5 kap.

Kapitlet handlar om vilka ingripanden som får användas mot den som inte uppfyller sina skyldigheter enligt lagen.

Enligt direktivet har medlemsstaterna en betydande frihet när det gäller sanktionernas utformning. I artikel 22, som har rubriken **Sanktioner**, står endast att medlemsstaterna ska fastställa regler om sanktioner för överträdelser av de nationella åtgärder som har antagits enligt direktivet och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Det tilläggs att sanktionerna ska vara effektiva, proportionella och avskräckande.

I fråga om förslagen till sanktionsavgifter vill Lagrådet här påminna om det som mera allmänt har anförts om sådana avgifter inledningsvis i detta yttrande.

5 kap. 1 §

I paragrafen finns grundläggande bestämmelser om när och hur en tillsynsmyndighet ska ingripa. Förslaget innebär att det finns tre olika sätt för hur ett ingripande får ske: genom föreläggande, eventuellt förenat med vite, genom sanktionsavgift och genom anmärkning.

I ett tredje stycke anges att tillsynsmyndigheten får avstå från ett ingripande om överträdelsen är ringa eller ursäktlig eller om det annars med hänsyn till omständigheterna vore oskäligt att ingripa.

I 4 kap. cybersäkerhetslagen finns motsvarande bestämmelser om när och hur en tillsynsmyndighet ska ingripa. Dessa är emellertid mera utförliga och det anges fler omständigheter som tillsynsmyndigheten ska beakta vid valet av ingripande, bl.a. verksamhetsutövarens subjektiva förhållande till det åsidosättande som har skett. Lagrådet anser att reglerna i cybersäkerhetslagen bör kunna utgöra förebild för reglerna om ingripande enligt den här lagen.

Det är angeläget att reglerna för sanktionsavgifter utformas så att det för tillsynsmyndigheten – och även för domstolen vid ett överklagande – ges en tydlig vägledning i fråga om hur olika faktorer ska inverka både på i vilka fall som avgift ska beslutas och på hur hög avgiften ska vara i olika situationer. Detta är naturligtvis viktigt också för verksamhetsutövarna, särskilt som det är höga belopp som ska kunna beslutas. (Jfr den straffrättsliga legalitetsprincipen.) Det kan utan vidare konstateras att det som står i tredje stycket i förslaget till 1 § om i vilka fall som tillsynsmyndigheten får avstå från ett ingripande är alltför kortfattat för att kunna utgöra en nöjaktig vägledning vid tillämpningen. Inte heller vad som står i författningskommentaren är tillräckligt i detta hänseende.

I cybersäkerhetslagen finns det en regel om att tillsynsmyndigheten får avstå från ingripande om någon annan tillsynsmyndighet har vidtagit åtgärder mot verksamhetsutövaren med anledning av överträdelsen och dessa åtgärder bedöms som tillräckliga. En motsvarande regel i den här lagen framstår som motiverad.

Med hänsyn till att förslaget i dessa delar behöver omarbetas i betydande utsträckning avstår Lagrådet från att lämna förslag till utformningen av det som ska motsvara den här paragrafen.

5 kap. 2 §

I paragrafen finns bestämmelser avseende förelägganden från en tillsynsmyndighet.

Den enda justering av den föreslagna lagtexten som behövs är att ordet ”kritisk” tas bort. Ett undantag som tar höjd för passivitetsrätten, dvs. rätten för var och en att inte behöva yppa något som kan belasta personen själv, bör dock övervägas. Ett sådant skulle i ett nytt tredje stycke kunna utformas i linje med följande.

Ett föreläggande får inte förenas med vite om det finns anledning att anta att den som ska föreläggas har begått en gärning som är straffbelagd eller kan leda till sanktionsavgift, och föreläggandet avser utredning av en fråga som har samband med gärningen. Förbudet mot att förena ett föreläggande med vite gäller också om den som ska föreläggas är en juridisk person och det finns anledning att anta att en ställföreträdare för den juridiska personen har begått gärningen.

5 kap. 3 §

I paragrafen föreskrivs att en tillsynsmyndighet får besluta att ta ut en sanktionsavgift av en kritisk verksamhetsutövare till följd av en överträdelse av de skyldigheter som avses i 5 kap. 1 § första stycket.

Den enda justeringen av lagtexten som behövs är att ordet ”kritisk” tas bort.

I författningskommentaren sägs att det inte är obligatoriskt att ta ut en sanktionsavgift när en överträdelse har konstaterats, utan att tillsynsmyndigheten avgör om en avgift ska tas ut i det enskilda fallet. Lagrådet får hänvisa till det som redan har sagts avseende sanktionsavgifter tidigare i detta yttrande. Fastän det finns mer än ett exempel i gällande rätt på en lagstiftning av detta slag är det Lagrådets uppfattning att en så löst hållen bestämmelse som här föreslås svarar dåligt mot intresset av rättssäkerhet. Åtminstone bör det i författningskommentaren utvecklas vilka bedömningsgrunder som tillsynsmyndigheten – och i förlängningen domstolen – ska tillämpa vid sitt beslutsfattande.

5 kap. 4 §

I paragrafen anges inom vilket spann som sanktionsavgiften ska bestämmas. För enskilda verksamhetsutövare rör det sig om lägst 5 000 kronor och om maximalt det högsta av 2 procent av den kritiska verksamhetsutövarens totala globala årsomsättning under närmast föregående räkenskapsår och ett belopp i kronor motsvarande 10 000 000 euro. För en offentlig verksamhetsutövare är minimum detsamma och maxbeloppet 10 000 000 kronor.

Som Lagrådet i det föregående har konstaterat innehåller inte CER-direktivet några precisa bestämmelser angående hur sanktionerna ska utformas. Det är därmed inte givet t.ex. att Euro-kursen ska ha betydelse för hur hög avgiften kan bli. En sådan lösning har emellertid valts i cybersäkerhetslagen. Lagrådet motsätter sig inte den valda lösningen.

En fråga är vad som punkten 1 menas med närmast föregående räkenskapsår. Detta är något som bör anges i lagtexten. Jfr här 5 kap. 7 § där en tidsfrist räknas från det att överträdelsen ägde rum. Jfr också det förslag som Lagrådet i det följande lämnar i fråga om förslaget till ändring i säkerhetsskyddslagen.

5 kap. 5 §

Paragrafen innehåller bestämmelser om vad som särskilt ska beaktas när sanktionsavgiftens storlek bestäms. Det som anges är (1) den skada eller risk för skada som har uppstått till följd av överträdelsen, (2) om den kritiska verksamhetsutövaren tidigare har gjort sig skyldig till en överträdelse och (3) den ekonomiska fördel som överträdelsen har inneburit för verksamhetsutövaren.

Lagrådet sätter frågetecken för hur regeln är konstruerad. Att ange vad som särskilt ska beaktas vid bedömningen när det inte finns någon grundbestämmelse om vilka omständigheter som det mera allmänt ska tas hänsyn till framstår som ologiskt. Det naturliga är i stället att lagstiftaren i en generellt hållen bestämmelse anger vad som ska beaktas och sedan i denna eller i en därefter kommande paragraf talar om vilka bedömningsgrunder som är särskilt viktiga.

En annan kritik som Lagrådet vill rikta mot förslaget i den här delen tar sikte på utformningen av punkt 1, där det som framgått sägs att särskild hänsyn ska tas till den skada eller risk för skada som har uppstått till följd av överträdelsen. Det ska jämföras med vad som sägs i 1 kap. 1 § om syftet med lagen, som ju är att stärka motståndskraften hos verksamhetsutövare som omfattas av lagen. Det borde därmed snarare vara nivån på bristerna i åtgärderna för motståndskraft som skulle spela särskild roll vid avgörandet av sanktionsavgiftens storlek än omfattningen av en inträffad skada eller vilken risk för skada som har uppstått. Hur stor skadan i ett enskilt fall blir, eller hur stor risken för skada bedöms vara, kan inte sällan ha mera med slumpen att göra än vara avhängigt nivån på den försummelse – om det nu har rört sig om en försummelse – som har bidragit till skadan eller skaderisken.

Också det som sägs i punkten 2, dvs. att särskild hänsyn ska tas till om verksamhetsutövaren tidigare har gjort sig skyldig till en överträdelse, måste diskuteras. Uttrycket ”gjort sig skyldig till” innefattar att verksamhetsutövaren har ådragit sig någon form av skuld. Men samtidigt sägs i författningskommentaren till 5 kap. 3 §, som Lagrådet läser det, att verksamhetsutövarens större eller mindre skuld inte har någon betydelse när en sanktionsavgift ska beslutas. Skrivningarna går därmed inte ihop.

Beträffande det som anges i punkten 3, att särskild hänsyn ska tas till den ekonomiska fördel som överträdelsen har inneburit för verksamhetsutövaren, kan väl bara påpekas att det är långt ifrån givet att ett åsidosättande av något åliggande enligt lagen leder till en ekonomisk fördel för verksamhetsutövaren.

Slutsatsen kan inte bli någon annan än att paragrafens utformning måste övervägas på nytt.

6 kap. 1 §

Eftersom det inte är endast tillsynsmyndighetens beslut som får överklagas bör lagtexten i första stycket skrivas så här:

> Beslut enligt denna lag får överklagas till allmän förvaltningsdomstol.
> När ett beslut överklagas är beslutande myndighet motpart i domstolen.

<u>Förslaget till lag om ändring i lagen om belastningsregister</u>

9 §

Den tillagda lagtexten i första stycket bör lyda:

9. enligt bestämmelser i lagen (2026:000) om motståndskraft i samhällsviktiga tjänster.

Förslaget till lag om ändring i offentlighets- och sekretesslagen

15 kap. 3 d §

Det blir egendomligt att riksdagen i lag indirekt anger att det är Myndigheten för civilt försvar som ska utses som gemensam kontaktpunkt enligt 1 kap. 8 § i den föreslagna lagen om motståndskraft (hos kritiska verksamhetsutövare) när det i den lagen inte sägs något annat än att det är den myndighet som regeringen bestämmer som ska vara kontaktpunkt. Paragrafen bör skrivas utan att myndigheten anges.

Lagrådet föreslår följande lagtext i första stycket.

Sekretessen enligt 1 a § hindrar inte att den myndighet som med stöd av 1 kap. 8 § lagen (2026:000) om motståndskraft i samhällsviktiga tjänster har utsetts som gemensam kontaktpunkt lämnar en uppgift till en tillsynsmyndighet enligt samma lag, om uppgiften behövs för att tillsynsmyndigheten ska kunna fullgöra sitt uppdrag.

18 kap. 8 b §

Namnet på den nya lagen behöver justeras för att överensstämma med Lagrådets förslag.

Förslaget till lag om ändring i cybersäkerhetslagen

1 kap. 8 a §

Med hänsyn till de justeringar av lagtexten i den nya lagen om motståndskraft i samhällsviktiga tjänster som Lagrådet föreslår bör lagtexten ges den här lydelsen:

Lagen gäller också för en verksamhetsutövare som omfattas av lagen (2026:000) om motståndskraft i samhällsviktiga tjänster.

Övriga lagförslag

Lagrådet lämnar förslagen utan erinran.

Försvarsdepartementet

Utdrag ur protokoll vid regeringssammanträde den 9 juli 2026

Närvarande: statsrådet Jonson, ordförande, och statsråden Forssmed, Forssell, Slottner, Liljestrand, Bohlin, Carlson, Rosencrantz, Dousa

Föredragande: statsrådet Bohlin

Regeringen beslutar proposition En ny lag för ökad motståndskraft hos kritiska verksamhetsutövare