Regeringen

Dir. 2023:30

Kommittédirektiv

Genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft

Beslut vid regeringssammanträde den 23 februari 2023

Sammanfattning

Europaparlamentet och rådet har nyligen antagit två nya EU-direktiv: direktivet om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2-direktivet) och direktivet om kritiska entiteters motståndskraft (CER-direktivet). En särskild utredare ska föreslå de anpassningar av svensk rätt som är nödvändiga för att NIS2-direktivet och CER-direktivet ska kunna genomföras.

Utredaren ska bl.a.

- föreslå hur identifieringen av och krav på entiteter som omfattas av NIS2-direktivet respektive CER-direktivet ska regleras,
- föreslå hur rollfördelningen mellan svenska myndigheter ska se ut med avseende på de olika uppgifter och ansvarsområden som föreskrivs i NIS2-direktivet och CER-direktivet,
- analysera hur den nya regleringen ska fungera vid sidan av säkerhetsskyddsregleringen och föreslå de ändringar som behövs för att uppnå en mer sammanhållen systematik mellan regelverken,
- ta ställning till om det behövs ett starkare och mer omfattande sekretesskydd för uppgifter som kan komma att behandlas enligt direktiven, och
- lämna förslag till nödvändiga författningsändringar.

Uppdraget ska redovisas senast den 23 februari 2024.

Uppdraget att föreslå hur NIS2-direktivet ska genomföras

NIS-direktivet ställer krav på säkerhet i nätverk och informationssystem

Digitaliseringen innebär att en allt större andel av samhällets aktiviteter i olika grad är beroende av nätverk och informationssystem. Den digitala utvecklingen medför stora möjligheter som bl.a. bättre tjänster och ökad effektivitet, men också risker. Därför är informations- och cybersäkerhet i dag en fråga som angår hela samhället. Särskilt höga säkerhetskrav ska ställas när det gäller samhällsviktig verksamhet som, för att upprätthålla nödvändiga samhällsfunktioner, måste fungera under alla förhållanden.

Utmaningarna inom informations- och cybersäkerhetsområdet delas med andra länder. De strategiska lösningarna måste därför utvecklas genom internationell samverkan. De senaste årens utveckling har till stor del drivits av EU-rätten, i synnerhet genom Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet), som antogs den 6 juli 2016.

Syftet med NIS-direktivet var att förbättra den inre marknadens funktion genom att fastställa åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom unionen. Direktivet gäller för leverantörer av samhällsviktiga tjänster inom sju särskilt utpekade sektorer: energi, transporter, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur. Vidare omfattas leverantörer av vissa digitala tjänster.

Enligt direktivet ställs krav på att leverantörerna ska vidta säkerhetsåtgärder för att hantera risker och incidenter i nätverk och informationssystem som de är beroende av för att kunna tillhandahålla tjänsterna. Leverantörerna ska också rapportera incidenter som har en betydande eller avsevärd påverkan på kontinuiteten i tjänsterna. Medlemsstaterna ska utse behöriga myndigheter med ansvar för att övervaka tillämpningen av direktivet på nationell nivå. I direktivet fastställs även en ram för samarbete både på nationell nivå och mellan medlemsstaterna, vilket ska ske bl.a. genom en särskilt inrättad samarbetsgrupp.

Direktivet har genomförts i svensk rätt genom lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174), även kallad NIS-lagen, och förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster. Därutöver har främst Myndigheten för samhällsskydd och beredskap (MSB) meddelat föreskrifter.

Kraven skärps genom det nya NIS2-direktivet

EU har nyligen antagit det så kallade NIS2-direktivet, som ersätter det tidigare NIS-direktivet. Syftet med det nya direktivet är att minska fragmenteringen av den inre marknaden genom att föreskriva minimiregler för ett samordnat regelverk. Tillämpningsområdet för regleringen utvidgas till att omfatta aktörer inom fler sektorer än det tidigare NIS-direktivet. De tillkommande sektorerna är avloppsvatten, 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 och forskning.

Vidare skärps kraven på aktörer genom minimikrav för åtgärder som ska tillämpas för att hantera risker kopplade till säkerheten i respektive aktörs nätverk och informationssystem. Dessutom införs mer precisa rapporteringskrav. I syfte att harmonisera sanktionssystemen i medlemsstaterna innehåller NIS2-direktivet även detaljerade bestämmelser om ingripanden och sanktioner.

En annan nyhet i NIS2-direktivet är införandet av ett system för sakkunnigbedömningar (peer reviews) som ska kunna utföras av cybersäkerhetsexperter utsedda av andra medlemsstater. Deltagandet i sakkunnigbedömningarna är emellertid frivilligt för medlemsstaterna och metodiken för dessa, liksom organisatoriska aspekter, ska etableras av samarbetsgruppen efter det att direktivet har trätt i kraft. Det finns därmed inte skäl att inom ramen för detta uppdrag analysera hur ett eventuellt svenskt deltagande vid sakkunnigbedömningar bör utformas.

Medlemsstaterna ska ha genomfört direktivet senast 21 månader efter dess ikraftträdande.

Vilka aktörer ska omfattas av regleringen?

Enligt NIS-direktivet har medlemsstaterna ansvaret för att fastställa vilka aktörer som uppfyller kriterierna för att klassificeras som leverantörer av samhällsviktiga tjänster. I NIS2-direktivet fastslås i stället ett enhetligt kriterium för vilka aktörer (i direktivet benämnda entiteter) som enligt huvudregeln ska omfattas av direktivets tillämpningsområde. Kriteriet innebär att alla entiteter som är av en viss storlek och av en typ som pekas ut i direktivet omfattas. Även mindre entiteter omfattas av direktivet om de uppfyller vissa specifika kriterier som tar sikte på om entiteten har en nyckelroll för samhället, ekonomin eller en viss sektor som omfattas av direktivet.

En av de nya sektorerna i NIS2-direktivet är offentlig förvaltning. Offentliga aktörer som bedriver verksamhet inom någon av de befintliga sektorerna berörs redan av det nuvarande NIS-regelverket. Inkluderingen av en särskild sektor för offentlig förvaltning innebär dock att offentliga aktörer kommer att omfattas i betydligt högre utsträckning än tidigare. Inom denna sektor är det bara aktörer, som i direktivet benämns offentliga förvaltningsentiteter, på statlig och regional nivå som omfattas. Översatt till svenska förhållanden kan direktivet tolkas så att statliga myndigheter och regioner omfattas, men inte kommuner. Medlemsstaterna är dock fria att bestämma att även de senare ska omfattas. Eftersom direktivets bestämmelser gäller för regioner finns det skäl för att regelverket ska gälla även för kommuner. I samma riktning talar den omständigheten att viss kommunal verksamhet under alla förhållanden kommer att omfattas, när verksamheten bedrivs inom någon av de övriga sektorerna. Det är dock viktigt att också belysa skäl som kan tala mot en full inkludering av kommunerna. Vid denna bedömning ska utredaren beakta bl.a. de eventuellt ökade kostnaderna för staten som en inkludering kan medföra. Utredaren ska mot denna bakgrund överväga om kommuner bör omfattas av den nya regleringen.

Forskning är en annan ny sektor i NIS2-direktivet. I sektorn innefattas forskningsorganisationer, vilka i NIS2-direktivet definieras som en entitet vars främsta mål är att bedriva tillämpad forskning eller experimentell utveckling i syfte att utnyttja resultaten av denna forskning i kommersiellt syfte, men som inte inbegriper utbildningsinstitutioner. Det är emellertid frivilligt för medlemsstaterna att föreskriva att NIS2-direktivet ska tillämpas på utbildningsinstitutioner, särskilt om de utför kritisk forskningsverksamhet. Utredaren ska mot denna bakgrund överväga om

universitet och högskolor, eller ett urval av dessa, bör omfattas av den nya regleringen. Utredaren ska i sina överväganden rörande universitet och högskolor ta hänsyn till principer som säkerställer akademisk frihet, institutionell autonomi och forskningsintegritet samt excellens och öppenhet inom högre utbildning och forskning.

Entiteter som omfattas av direktivets tillämpningsområde ska klassificeras antingen som väsentliga eller som viktiga entiteter, utifrån deras betydelse för den sektor de verkar inom eller den tjänst de tillhandahåller, liksom utifrån deras storlek. Medlemsstaterna ska upprätta en förteckning över väsentliga och viktiga entiteter och regelbundet uppdatera den. För att möjliggöra upprättandet av förteckningen ska entiteterna vara skyldiga att lämna vissa uppgifter till de behöriga myndigheterna. Medlemsstaterna får även inrätta ett system som bygger på att entiteterna själva registrerar sig. De behöriga myndigheterna ska därefter med viss regelbundenhet underrätta kommissionen om bl.a. antalet registrerade entiteter inom olika kategorier.

Mot denna bakgrund behöver det analyseras hur direktivets bestämmelser om registrering av väsentliga och viktiga entiteter ska genomföras i svensk rätt. Dagens reglering bygger på att det är verksamhetsutövaren som är ansvarig för att avgöra om denne omfattas av regelverket och i så fall anmäla sig till tillsynsmyndigheten. Det bör vara utgångspunkten även för genomförandet av det nya direktivet.

Utredaren ska därför

- ta ställning till om kommuner ska omfattas av regleringen,
- överväga om universitet och högskolor, eller ett urval av dessa, ska omfattas av den nya regleringen,
- föreslå ett system för hur entiteter som omfattas av regleringen ska identifieras och registreras, och
- lämna förslag till nödvändiga författningsändringar.

Hur ska rollfördelningen mellan svenska myndigheter se ut?

I likhet med vad som gäller enligt NIS-direktivet ska medlemsstaterna enligt NIS2-direktivet utse en eller flera behöriga myndigheter och en nationell gemensam kontaktpunkt. De behöriga myndigheterna ska utöva tillsyn och övervaka tillämpningen av direktivet på nationell nivå. Den nationella gemensamma kontaktpunkten ska utgöra en sambandsfunktion som

säkerställer gränsöverskridande samarbete mellan medlemsstatens myndigheter och relevanta myndigheter i andra medlemsstater och ett sektorsövergripande samarbete med andra nationella behöriga myndigheter i medlemsstaten. Liksom NIS-direktivet föreskriver NIS2-direktivet att det ska finnas en eller flera enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter) som bl.a. ska ansvara för hanteringen av incidenter. I NIS2-direktivet åläggs dessa ytterligare uppgifter.

NIS2-direktivet innehåller dessutom nya regler om ramverk för storskaliga cybersäkerhetsincidenter och cyberkriser. Varje medlemsstat ska enligt direktivet utse en eller flera behöriga myndigheter med ansvar för hanteringen av sådana incidenter och kriser (cyberkrishanteringsmyndighet).

Vidare ställer NIS2-direktivet större krav på såväl strategiskt som operativt samarbete mellan medlemsstaterna. Det befintliga samarbetet inom samarbetsgruppen förstärks. Det gör även det operativa samarbetet, bl.a. genom att det så kallade CSIRT-nätverket – där företrädare för de nationella CSIRT-enheterna deltar – tilldelas fler arbetsuppgifter.

I NIS2-direktivet regleras även nya forum för samarbete mellan medlemsstaterna. Ett sådant forum är det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe), som ska verka stödjande vid samordning och hantering av storskaliga incidenter och cyberkriser. Nätverket ska bestå av företrädare för medlemsstaternas cyberkrishanteringsmyndigheter. Det finns redan i dag på frivillig basis, med MSB som svensk representant, men får i NIS2 en tydlig rättslig grund.

Vid genomförandet av NIS2-direktivet bör systemet för tillsyn utgå från den struktur som finns enligt dagens regelverk. Utöver de ändringar som är nödvändiga med anledning av NIS2-direktivets utökade krav kan det emellertid finnas skäl till ändringar för att åstadkomma en mer effektiv tillsyn. Utredaren ska därför göra en utvärdering av den tillsyn som har bedrivits enligt den nuvarande NIS-regleringen sedan dess införande. Enligt den nu gällande NIS-lagen finns det för varje sektor och för de digitala tjänster som omfattas av lagen en utpekad tillsynsmyndighet som ska ansvara för att övervaka att regelverket följs. De nuvarande tillsynsmyndigheterna är Statens energimyndighet, Transportstyrelsen, Finansinspektionen, Inspektionen för vård och omsorg, Livsmedelsverket och Post- och telestyrelsen.

Som konstaterats innebär NIS2-direktivet att fler sektorer kommer att omfattas av regelverket än vad som är fallet i dag. Det behöver därför utses tillsynsmyndigheter för de tillkommande sektorerna. Inom vissa av dessa finns redan myndigheter med tillsynsuppgifter inom informationssäkerhet. Exempelvis utövar Post- och telestyrelsen tillsyn enligt säkerhetsskyddslagen (2018:585) över enskilda verksamhetsutövare inom området posttjänster. I dessa fall är det naturligt att myndigheten utses till tillsynsmyndighet för den aktuella sektorn även enligt NIS2-regelverket. I andra fall behöver utredaren överväga vilken myndighet som ska anförtros tillsynsansvaret för sektorn. I enlighet med vad som anges nedan bör tillsynsmyndigheterna enligt CER-direktivet som utgångspunkt vara desamma som tillsynsmyndigheterna enligt NIS2-direktivet. Även detta behöver beaktas av utredaren.

MSB har i dag en bred roll kopplat till NIS-regleringen som bl.a. innefattar ett samordningsansvar för tillsynen. Myndigheten leder bl.a. ett samarbetsforum där samtliga tillsynsmyndigheter och Socialstyrelsen ingår. Därutöver är MSB nationell gemensam kontaktpunkt och företräder Sverige i den strategiska samarbetsgruppen. MSB har även rollen som Sveriges CSIRT-enhet och deltar därmed också i CSIRT-nätverket. Denna ansvarsfördelning är ändamålsenlig och utgångspunkten för utredarens uppdrag bör därför vara att MSB ska fullgöra motsvarande uppgifter enligt det nya NIS2-regelverket. Mot bakgrund av de närliggande uppgifter som MSB har i dag och den kompetens som finns inom myndigheten bör MSB även utses till cyberkrishanteringsmyndighet. Det innebär att MSB även fortsättningsvis bör företräda Sverige i det nya europeiska kontaktnätverket för cyberkriser. Det behöver analyseras om och i vilken utsträckning som MSB:s nuvarande mandat behöver förändras för att myndigheten ska kunna fullgöra dessa uppgifter.

NIS2-direktivet anger vidare att medlemsstaterna är skyldiga att anta en nationell strategi för cybersäkerhet. Som en del av strategin ska medlemsstaterna särskilt anta riktlinjer på en rad områden. Dessutom ska medlemsstaterna anta en nationell plan för hanteringen av storskaliga cybersäkerhetsincidenter och kriser där mål och villkor för hanteringen av storskaliga cybersäkerhetsincidenter och kriser fastställs. Utformningen av den nationella strategin och den nationella planen bör emellertid inte omfattas av utredarens uppdrag utan bör i stället hanteras i särskild ordning.

Utredaren ska därför

- utvärdera den tillsyn som har bedrivits enligt NIS-lagen sedan dess införande,
- föreslå vilka myndigheter som ska utöva tillsyn över de tillkommande sektorerna i NIS2-direktivet,
- analysera vilka ändringar av den befintliga tillsynsstrukturen som i övrigt behövs,
- analysera vilka ändringar som behövs för att MSB i enlighet med NIS2-direktivets krav ska kunna utöva uppdraget som nationell gemensam kontaktpunkt, CSIRT-enhet och cyberkrishanteringsmyndighet samt deltagare i de samarbetsnätverk som direktivet lägger grund för, och
- lämna förslag till nödvändiga författningsändringar.

Vilka krav ska ställas på aktörerna?

NIS2-direktivet skärper kraven på väsentliga och viktiga entiteter vad gäller riskhanteringsåtgärder, i nuvarande lagstiftning benämnda som säkerhetsåtgärder, och rapporteringsskyldigheter. Medlemsstaterna ska säkerställa att entiteterna vidtar tekniska, operationella och organisatoriska åtgärder för att hantera risker för säkerheten i nätverks- och informationssystem. Åtgärderna ska vara proportionella, med beaktande av bl.a. entitetens storlek, sannolikheten för att incidenter inträffar och den påverkan de skulle ha. Direktivet fastställer vissa minimikrav på åtgärder som entiteterna ska vidta. Kraven omfattar bl.a. rutiner för riskanalys och säkerhet i informationssystem, incidenthantering samt rutiner för kryptografi och, om det är lämpligt, kryptering. Åtgärderna ska även innefatta säkerhet i leveranskedjor.

Direktivet ålägger även medlemsstaterna att säkerställa att entiteterna rapporterar incidenter som har en betydande inverkan på tillhandahållandet av deras tjänster till CSIRT-enheten eller nationella behöriga myndigheter. Rapportering ska ske vid olika tillfällen efter att en incident har inträffat och en slutlig rapport med mer detaljerad information ska avges inom en månad från det att den första incidentrapporten lämnades.

Enligt nuvarande ordning ska incidenter rapporteras till CSIRT-enheten, det vill säga MSB. Mot bakgrund av den roll som MSB i egenskap av

CSIRT-enhet har när det gäller hantering av incidenter bör detta vara utgångspunkten även vid genomförandet av NIS2-direktivet.

Medlemsstaterna får enligt direktivet bestämma att entiteter som ett led i riskhanteringen ska använda särskilda certifierade produkter i nätverks- och informationssystem. Utredaren ska analysera hur ändamålsenlighet och proportionalitet i sådana föreskrifter kan beaktas samt hur de ska meddelas. I det sammanhanget behöver det beaktas att kommissionen har getts befogenhet att genom delegerade akter föreskriva att vissa kategorier av entiteter ska vara skyldiga att använda vissa certifierade produkter.

Utredaren ska därför

- analysera hur direktivets krav på riskhanteringsåtgärder och incidentrapportering ska genomföras i svensk rätt, och
- lämna förslag till nödvändiga författningsändringar.

Vilka befogenheter ska tillsynsmyndigheterna ha?

I likhet med det tidigare direktivet förutsätts det att tillsynsmyndigheterna har tillräckliga verktyg för att se till att regelverket följs. NIS2-direktivet uppställer även detaljerade krav på vissa befogenheter som tillsynsmyndigheterna ska ha och på sanktioner som ska kunna tillgripas. Kraven skiljer sig åt mellan väsentliga respektive viktiga entiteter. Vid tillsynen av väsentliga entiteter ska tillsynsmyndigheterna ha större befogenheter och tillsynen ska vara såväl proaktiv som reaktiv. För viktiga entiteter ska tillsynen vara reaktiv och mindre omfattande.

Direktivet föreskriver flera åtgärder som saknar direkt motsvarighet i svensk rätt. När det gäller väsentliga entiteter kräver direktivet bl.a. att det ska finnas möjlighet – om andra åtgärder visar sig vara ineffektiva – att tillfälligt upphäva en certifiering eller auktorisation för entitetens verksamhet och att tillfälligt förbjuda personer i entitetens ledning från att utöva ledningsfunktioner. Utredaren behöver analysera hur den nationella regleringen av sådana åtgärder ska förhålla sig till relevant reglering på andra områden, t.ex. associationsrättsliga regler eller sektorsspecifika regler som innehåller krav på certifiering eller auktorisation för viss verksamhet.

Det är enligt direktivet upp till medlemsstaterna att avgöra om bestämmelser om straffansvar ska införas för överträdelser av den nationella regleringen.

Vid genomförandet av NIS-direktivet gjordes bedömningen att överträdelser inte skulle vara straffsanktionerade (prop. 2017/18:205 s. 64 f.). Det saknas skäl att frångå den bedömningen. Inriktningen ska alltså vara att sanktioner för överträdelser av den nya regleringen ska vara av administrativt slag.

Utredaren ska därför

- analysera vilka befogenheter i fråga om tillsyn och sanktioner som tillsynsmyndigheterna enligt NIS2-direktivet bör ha, och
- lämna förslag till nödvändiga författningsändringar.

Uppdraget att föreslå hur CER-direktivet ska genomföras

CER-direktivet ställer krav på motståndskraft i samhällsviktig verksamhet

Säkerheten för samhällsviktig verksamhet, inbegripet kritisk infrastruktur, är en i högsta grad aktuell fråga. Motståndskraften hos sådan verksamhet är central för att förebygga, motstå och hantera situationer som riskerar att innebära allvarliga störningar av viktiga samhällsfunktioner. Arbetet med att stärka motståndskraften behöver ske på alla nivåer i samhället, och även på unionsnivå.

Inom EU har det under en längre tid pågått arbete med frågor kopplade till skydd av kritisk infrastruktur. Den unionsrättsliga regleringen har dock främst skett sektorsvis och endast tagit sikte på vissa aspekter av motståndskraft hos aktörer inom de sektorerna. Bland annat finns det regler som tar sikte på skyddet för europeisk kritisk infrastruktur inom energi- respektive transportsektorn i 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. Vid utvärderingen av detta direktiv har det konstaterats att skyddsåtgärder som tar sikte på enskilda tillgångar inte är tillräckliga för att förhindra alla störningar från att uppstå. I stället har det bedömts att ansatsen bör ändras i riktning mot att säkerställa motståndskraften hos de aktörer som bedriver samhällsviktig verksamhet.

EU har nyligen antagit det så kallade CER-direktivet, vilket ersätter rådets direktiv 2008/114/EG. Enligt CER-direktivet ska medlemsstaterna identifiera aktörer (så kallade kritiska entiteter) som tillhandahåller 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.

Direktivet ålägger de kritiska entiteterna skyldigheter att bl.a. vidta åtgärder för att stärka sin motståndskraft och att rapportera incidenter. Det innehåller också bestämmelser om tillsyn och sanktioner. Vidare fastställs i direktivet en ram för samarbete mellan medlemsstaterna.

Medlemsstaterna ska ha genomfört direktivet senast 21 månader efter dess ikraftträdande.

Hur ska rollfördelningen mellan svenska myndigheter se ut?

Direktivet ålägger medlemsstaterna att utse en nationell gemensam kontaktpunkt för samarbetet med andra medlemsstater och en eller flera behöriga myndigheter som ska ansvara för direktivets tillämpning på nationell nivå. Frågan vilka befogenheter de behöriga myndigheterna ska ha för att kunna utöva en effektiv tillsyn och beivra överträdelser behandlas i ett särskilt avsnitt nedan.

För att säkerställa samstämmighet mellan de två direktiven föreskrivs det i dessa att entiteter som har identifieras som kritiska entiteter enligt CER även ska anses vara väsentliga entiteter enligt NIS2. I direktiven anges vidare att de behöriga myndigheterna enligt respektive direktiv ska utbyta information med varandra om hot och incidenter samt om åtgärder som myndigheterna vidtar. Mot denna bakgrund är en naturlig utgångspunkt att samma myndighet som utövar tillsyn över en viss entitet enligt NIS2-direktivet även utövar tillsyn över entiteten enligt CER-direktivet. På så vis kan det säkerställas att tillsynen enligt de två direktiven utövas på ett effektivt och samordnat sätt.

MSB har en bred kompetens kopplad till skyddet för samhällsviktig verksamhet och kritisk infrastruktur. Myndigheten fullgör också rollen som nationell gemensam kontaktpunkt för det arbete som i dag bedrivs inom ramen för direktiv 2008/114/EG. Av dessa skäl, och för att säkerställa samstämmighet med NIS2-regleringen, bör MSB utses till nationell gemensam kontaktpunkt även enligt CER-direktivet.

MSB har i dag en samordnande roll mellan tillsynsmyndigheterna enligt NIS-regelverket. För att säkerställa att NIS2-direktivet och CER-direktivet genomförs och tillämpas på ett effektivt och koordinerat sätt bör MSB ha en motsvarade roll enligt båda regelverken. För att få en samlad bild av genomförandet och tillämpningen behöver MSB få del av relevant information från de övriga behöriga myndigheterna. MSB bör även ha en samordnande roll i fråga om den riskbedömning som de behöriga myndigheterna är skyldiga att göra.

Medlemsstaterna ska enligt CER-direktivet även anta en nationell strategi för kritiska entiteters motståndskraft. Frågan om hur en sådan strategi ska utformas bör emellertid inte omfattas av utredarens uppdrag utan i stället hanteras i särskild ordning, i likhet med den nationella strategin för cybersäkerhet som medlemsstaterna ska anta enligt NIS2-direktivet.

Utredaren ska därför

- föreslå ett system för tillsyn som uppfyller CER-direktivets krav och som är samordnat med det system som föreslås för NIS2,
- föreslå vilka myndigheter som ska utses till tillsynsmyndigheter,
- ta ställning till hur MSB:s roll som nationell gemensam kontaktpunkt ska utformas och regleras, och
- lämna förslag till nödvändiga författningsändringar.

Hur ska identifieringen av de kritiska entiteterna gå till?

Medlemsstaterna är skyldiga att identifiera kritiska entiteter inom de sektorer och undersektorer som omfattas av direktivet och upprätta en förteckning över dessa. För att en aktör ska anses vara en kritisk entitet ska tre kriterier vara uppfyllda: för det första att aktören tillhandahåller en eller flera samhällsviktiga tjänster, för det andra att aktören verkar på medlemsstatens territorium och har sin kritiska infrastruktur belägen där, för det tredje att en incident skulle medföra en betydande störning vid tillhandahållandet av tjänsten eller tjänsterna. För det fall en kritisk entitet tillhandahåller samma eller liknande samhällsviktiga tjänster i sex eller fler medlemsstater ska kommissionen ha möjlighet att fastställa att denna ska betraktas som en så kallad kritisk entitet av särskild europeisk betydelse. För sådana entiteter gäller särskilda bestämmelser enligt direktivet.

En icke uttömmande förteckning över tjänster som ska anses samhällsviktiga kommer att fastställas av kommissionen genom en delegerad akt. Det kan inte uteslutas att det kan finnas behov av att låta den nationella regleringen omfatta aktörer som tillhandahåller även andra samhällsviktiga tjänster än de som kommissionen pekar ut. Utredaren behöver därför ta ställning till hur regler för att peka ut samhällsviktiga tjänster ska utformas. Det måste även analyseras hur direktivets kriterier för vad som utgör en betydande störning ska tillämpas i en svensk kontext och hur eventuella tröskelvärden ska fastställas. Enligt den nuvarande nationella NIS-regleringen får MSB, efter att ha gett tillsynsmyndigheterna och Socialstyrelsen tillfälle att yttra sig, meddela föreskrifter dels om vilka tjänster som är samhällsviktiga tjänster, dels om vad som avses med en betydande störning. En motsvarande ordning skulle kunna vara lämplig för genomförandet av CER-direktivet. Det behöver även övervägas vem som ska ansvara för identifieringen av de kritiska entiteterna, hur identifieringsförfarandet ska gå till och hur förteckningen över de kritiska entiteterna ska upprättas och uppdateras.

Vidare måste utredaren analysera om särskilda nationella bestämmelser behövs i fråga om identifieringen och anmälan till kommissionen av kritiska entiteter av särskild europeisk betydelse.

Utredaren ska därför

- föreslå hur kritiska entiteter ska identifieras samt hur en förteckning över dessa kan upprättas och uppdateras i enlighet med direktivets krav, och
- lämna förslag till nödvändiga författningsändringar.

Vilka krav ska ställas på de kritiska entiteterna?

Medlemsstaterna ska enligt CER-direktivet säkerställa att kritiska entiteter utför en riskbedömning som omfattar alla relevanta risker som skulle kunna leda till incidenter. Vidare ska medlemsstaterna se till att de kritiska entiteterna vidtar lämpliga och proportionella åtgärder för att säkerställa sin motståndskraft. Åtgärderna ska grundas på den riskbedömning som den kritiska entiteten själv har utfört men även på relevant information från medlemsstaternas riskbedömning som har delats med entiteten. Direktivet uppställer även vissa minimikrav på åtgärder som ska vidtas. Kommissionen kommer vid en senare tidpunkt att komplettera dessa minimikrav med icke-bindande riktlinjer och med tekniska specifikationer. Utredaren ska mot

denna bakgrund analysera hur reglerna om de kritiska entiteternas riskbedömning ska utformas och vid behov kunna kompletteras. Vid den analysen ska utredaren även överväga hur CER-direktivets krav på riskbedömningar förhåller sig till liknande krav i annan reglering.

Vidare innehåller direktivet krav på att kritiska entiteter ska rapportera incidenter som medför eller skulle kunna medföra en betydande störning vid tillhandahållandet av samhällsviktiga tjänster. Parametrar som ska beaktas vid bedömningen av en störnings betydelse är antalet användare som påverkas av störningen, störningens varaktighet och det geografiska område som påverkas av störningen. Hur den närmare bedömningen ska gå till regleras emellertid inte i direktivet och är därför en fråga som utredaren behöver analysera.

Incidenter ska enligt CER-direktivet rapporteras till den behöriga myndigheten. För det fall en medlemsstat har utsett flera behöriga myndigheter måste det anses vara upp till medlemsstaten att avgöra till vilken eller vilka av dessa som rapporteringen ska ske. Vid genomförandet av NIS-direktivet gjordes, som framgått ovan, bedömningen att incidenter skulle rapporteras till MSB i myndighetens egenskap av CSIRT-enhet. Motsvarande fråga behöver analyseras i fråga om CER-direktivet. Utredaren behöver således ta ställning till vilken eller vilka myndigheter som incidenter ska rapporteras till.

Utredaren ska därför

- analysera hur direktivets krav på riskbedömning, åtgärder för motståndskraft och incidentrapportering för kritiska entiteter ska genomföras i svensk rätt,
- lämna förslag till nödvändiga författningsändringar.

Hur ska systemet för bakgrundskontroller utformas?

Medlemsstaterna ska enligt CER-direktivet anta regler som ger kritiska entiteter rätt att i vissa fall begära bakgrundskontroller. Bakgrundskontroller ska kunna begäras avseende bl.a. personer som innehar en känslig roll i den kritiska entiteten, som har tillträde till entitetens lokaler eller tillgång till dess informationssystem eller som är aktuella för en anställning som innefattar en sådan roll, sådant tillträde eller sådan tillgång. En bakgrundskontroll ska bekräfta personens identitet och ska även innefatta uppgifter från

belastningsregistret. Utredaren behöver analysera hur direktivets krav på bakgrundskontroller ska genomföras i svensk rätt. Det behöver särskilt övervägas hur ett system för belastningsregisterkontroll ska utformas.

Utgångspunkten för utredarens överväganden ska vara att de kritiska entiteterna på ett effektivt sätt ska kunna få kännedom om eventuella uppgifter om brott som kan vara av betydelse för deltagande i verksamheten. Samtidigt måste det beaktas att de uppgifter som finns i belastningsregistret är av integritetskänsligt slag. Systemet för belastningsregisterkontroll bör utformas på ett sätt som innebär att integritetsintrånget för den enskilde inte blir större än nödvändigt.

Utredaren behöver bl.a. ta ställning till vem som ska ha rätt att begära ut uppgifterna från Polismyndigheten. Systemet ska emellertid inte bygga på att den kritiska entiteten själv begär ut uppgifterna. Även om det i belastningsregisterregleringen finns exempel på situationer där enskilda har getts rätt att begära uppgifter om andra enskilda kan en sådan lösning inte anses vara lämplig i detta fall.

Utredaren ska därför

- föreslå hur ett system med bakgrundskontroller ska utformas, och
- lämna förslag till nödvändiga författningsändringar.

Vilka befogenheter ska tillsynsmyndigheterna ha?

I likhet med NIS2-direktivet förutsätter CER-direktivet att tillsynsmyndigheterna har tillräckliga verktyg för att se till att regelverket följs. Myndigheterna ska enligt direktivet ha rätt att utföra inspektioner av såväl kritisk infrastruktur som de kritiska entiteternas riskhanteringsåtgärder. Tillsynsmyndigheterna ska också ha befogenhet att utföra säkerhetsrevision eller att begära att de kritiska entiteterna genomgår sådan. Vidare ska myndigheterna kunna begära att de kritiska entiteterna lämnar information som är nödvändig för att utvärdera entiteternas riskhanteringsåtgärder och dokumentation gällande genomförandet av dessa åtgärder. Tillsynsmyndigheterna ska även ha befogenhet att kräva att kritiska entiteter som inte fullgör sina skyldigheter vidtar rättelse. Dessutom ska medlemsstaterna anta regler om effektiva, proportionella och avskräckande sanktioner för överträdelser av direktivets bestämmelser.

I jämförelse med NIS2-direktivet lämnar CER-direktivet förhållandevis stort bedömningsutrymme för medlemsstaterna vad gäller den närmare utformningen av tillsynsmyndigheternas verktyg. Som konstaterats ovan kommer emellertid samtliga entiteter som omfattas av CER-direktivet även att omfattas av NIS2-direktivet. Vidare bör tillsynsmyndigheterna vara desamma för båda direktiven. Det behöver inte nödvändigtvis betyda att det är lämpligt att samtliga verktyg för tillsynsmyndigheterna som föreskrivs i NIS2-direktivet ska kunna tillämpas även i fråga om kritiska entiteter enligt CER-direktivet eller att sanktionsavgifterna måste ha samma storlek. Utgångspunkten för utredarens överväganden ska dock vara att tillsynen enligt båda direktiven ska kunna utövas på ett samordnat och effektivt sätt. Det ska också eftersträvas att de ingripanden och sanktioner som kan bli aktuella enligt respektive direktiv framstår som proportionerliga i förhållande till varandra och lever upp till enskildas behov av förutsebarhet.

Utredaren ska därför

- analysera vilka befogenheter i fråga om tillsyn och sanktioner som tillsynsmyndigheterna enligt CER-direktivet bör ha, och
- lämna förslag till nödvändiga författningsändringar.

Gemensamma frågor för NIS2-direktivet och CER-direktivet

Förhållandet till säkerhetsskyddsregleringen

Säkerhetsskyddslagen är den lag som reglerar skyddsåtgärder för de mest skyddsvärda verksamheterna i samhället. 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. Med säkerhetsskydd avses skydd av säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter. Säkerhetsskyddslagstiftningens huvudsyfte är alltså att skydda verksamheter som har betydelse för Sveriges säkerhet ur ett nationellt perspektiv mot i första hand antagonistiska angrepp.

Av artikel 4.2 i fördraget om Europeiska unionen följer att den nationella säkerheten ska vara varje medlemsstats eget ansvar. I NIS2-direktivet och CER-direktivet betonas också att direktiven inte påverkar medlemsstaternas ansvar för att skydda nationell säkerhet. Offentliga förvaltningsentiteter som

bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning är i sin helhet undantagna från direktivens tillämpningsområde. När det gäller andra aktörer har medlemsstaterna möjlighet att besluta att särskilda entiteter med verksamhet på de aktuella områdena ska vara undantagna från skyldigheter enligt direktivet.

Reglerna om undantag för särskilda entiteter i NIS2-direktivet innebär sammanfattningsvis följande. Om entiteten endast delvis bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning får medlemsstaten besluta att entiteten ska undantas från direktivets krav på riskhanteringsåtgärder och incidentrapportering, när det gäller den delen av verksamheten. Motsvarande gäller med avseende på sådana tjänster som en entitet tillhandahåller uteslutande till offentliga förvaltningsentiteter på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning. Om en entitet bedriver verksamhet eller tillhandahåller tjänster uteslutande på dessa områden, får entiteten undantas även från reglerna om registrering. På motsvarande sätt får medlemsstaterna enligt CER-direktivet besluta att flertalet av det direktivets bestämmelser inte ska vara tillämpliga på särskilda kritiska entiteter som bedriver verksamhet inom de aktuella områdena.

Direktivens bestämmelser om undantag för särskilda entiteter saknar motsvarighet i svensk rätt. Undantaget för säkerhetskänslig verksamhet i NIS-lagen är i stället konstruerat på det sättet att lagen inte gäller för verksamhet som omfattas av säkerhetsskyddslagen. Regleringen bygger på att en leverantör av samhällsviktiga eller digitala tjänster som bedriver säkerhetskänslig verksamhet själv ska bedöma vilka delar av verksamheten som omfattas av säkerhetsskyddslagen respektive NIS-lagen. En sådan lösning framstår emellertid inte som förenlig med hur möjligheten till undantag för verksamhet som rör nationell säkerhet har formulerats i NIS2-direktivet och CER-direktivet. Det behöver därför analyseras hur direktivens möjlighet att undanta specifika aktörer ska genomföras i svensk rätt.

I detta sammanhang framstår det som naturligt att utgå från den befintliga tillsynsstrukturen inom säkerhetsskyddsregleringen. Denna innebär att tillsynsansvaret är fördelat på Försvarsmakten, Säkerhetspolisen och vissa andra utpekade myndigheter som ansvarar för tillsynen av verksamhetsutövare inom olika sektorer. Tillsynsmyndigheterna ska genom

systematisk kartläggning identifiera vilka verksamhetsutövare och andra tillsynsobjekt som finns inom myndigheternas respektive tillsynsområden. Myndigheterna ska ha en aktuell förteckning över sina tillsynsobjekt. Det framstår därför som en effektiv ordning att dessa myndigheter ges rätt att besluta om undantag från skyldigheter enligt direktiven för sådana aktörer som står under deras tillsyn enligt säkerhetsskyddslagen. Utredaren får emellertid föreslå även andra lösningar om det finns skäl för det. Inriktningen för förslagen ska vara att säkerhetskänslig verksamhet undantas från den nya regleringen i den utsträckning som är möjlig.

Vidare framgår det av både NIS2-direktivet och CER-direktivet att det inte finns någon skyldighet att tillhandahålla information vars utlämnande strider mot väsentliga intressen i fråga om medlemsstaternas nationella säkerhet, allmänna säkerhet eller försvar. I skälen i direktivens ingresser anges det att nationella regler till skydd för säkerhetsskyddsklassificerade uppgifter bör beaktas i detta sammanhang.

För att säkerställa att säkerhetsskyddsklassificerade uppgifter inte lämnas ut är det inte tillräckligt att särskilda entiteter som bedriver säkerhetskänslig verksamhet helt eller delvis kan undantas från direktivens krav på bl.a. incidentrapportering. Exempelvis behöver det även säkerställas att uppgifter som rör säkerhetskänslig verksamhet inte registreras i den europeiska sårbarhetsdatabas som enligt NIS2-direktivet ska upprättas av Enisa eller lämnas ut i samband med sådana rådgivande uppdrag för kritiska entiteter av särskild europeisk betydelse som regleras i CER-direktivet. Det behöver därför införas regler som direkt undantar säkerhetsskyddsklassificerade uppgifter från såväl rapporteringskraven som från annan uppgiftslämning som regleras i direktiven.

Det anförda innebär att delar av en entitets verksamhet kan komma att omfattas av NIS2-direktivets eller CER-direktivets tillämpningsområde samtidigt som andra delar av verksamheten undantas och i stället omfattas av säkerhetsskyddslagen. Det behöver mot denna bakgrund analyseras hur säkerhetsskyddslagens systematik och terminologi i praktiken ska fungera vid sidan om den nya regleringen. Utredaren får föreslå ändringar i säkerhetsskyddsregleringen som behövs för att uppnå en sammanhållen systematik mellan regelverken.

I detta sammanhang finns det särskilt anledning att uppmärksamma tillsynsmyndigheternas befogenheter och bestämmelserna om sanktioner. Tillsynsmyndigheternas befogenheter enligt säkerhetsskyddsregleringen är i flera avseenden mindre långtgående än motsvarande befogenheter som regleras i NIS2-direktivet. Detta skulle i vissa fall kunna få till följd 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 NIS2-direktivet eller CER-direktivet. Eftersom säkerhetsskyddsregleringen gäller för de mest skyddsvärda verksamheterna i samhället är en sådan ordning inte önskvärd. Utredaren ska därför särskilt analysera vilka ändringar i säkerhetsskyddsregleringen som behövs i detta avseende.

Utredaren ska därför

- föreslå ett system för hur aktörer som bedriver säkerhetskänslig verksamhet ska undantas, med avseende på den verksamheten, från NIS2-direktivets och CER-direktivets krav på bl.a. incidentrapportering,
- föreslå hur säkerhetsskyddsklassificerade uppgifter ska undantas från rapporteringsplikten och andra former av uppgiftslämning som regleras i direktiven,
- analysera hur den nya regleringen ska fungera vid sidan av säkerhetsskyddsregleringen och föreslå ändringar som behövs för att uppnå en mer sammanhållen systematik mellan regelverken, särskilt vad gäller tillsynsmyndigheternas befogenheter och sanktionsavgifternas storlek, och
- lämna förslag till nödvändiga författningsändringar.

Förhållandet till annan unionsrättslig och nationell reglering

Både NIS2-direktivet och CER-direktivet innehåller bestämmelser om förhållandet till sektorsspecifika unionsrättsakter. Exempelvis följer det av CER-direktivet att berörda bestämmelser i det direktivet inte ska vara tillämpliga om det i en sektorsspecifik unionsrättsakt ställs åtminstone likvärdiga krav på att kritiska entiteter ska vidta åtgärder för att stärka sin motståndskraft. Ett liknande undantag finns i NIS2-direktivet. En sektorsspecifik unionsrättsakt som pekas ut särskilt i båda direktiven är 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). I CER-direktivet framhålls även att behörig myndighet för sektorerna bankverksamhet och finansmarknadsinfrastruktur i princip ska vara den behöriga myndigheten enligt Dora-förordningen. Utredaren behöver beakta dessa bestämmelser och relevanta sektorsspecifika unionsrättsakter när det gäller vilka krav som ska ställas på entiteterna, hur rollfördelningen mellan svenska myndigheter ska se ut och vilka befogenheter tillsynsmyndigheterna ska ha.

Av föregående avsnitt följer att utredaren ska analysera hur den nya regleringen ska fungera vid sidan av säkerhetsskyddsregleringen, i syfte att uppnå en mer sammanhållen systematik mellan regelverken. Utredaren behöver i sitt arbete beakta även annan relevant reglering. Utredaren ska särskilt överväga hur förslagen kan utformas på ett sätt som innebär att samordningsvinster i entiteternas säkerhetsarbete kan uppnås. Vidare ska utredaren analysera hur den terminologi som används i direktiven vid genomförandet kan anpassas till vedertagna begrepp i nationell reglering, såsom den nuvarande NIS-lagen och förordningen (2022:524) om statliga myndigheters beredskap.

Såväl NIS2-direktivet som CER-direktivet är så kallade minimidirektiv. Medlemsstaterna är oförhindrade att anta bestämmelser som säkerställer en högre cybersäkerhetsnivå eller en högre nivå av motståndskraft än vad som krävs enligt direktiven. Utredaren har därmed möjlighet att lämna förslag som exempelvis omfattar även andra sektorer och typer av entiteter än de som pekas ut i EU-direktiven, om det bedöms lämpligt för att uppnå en bättre sammanhållen reglering för samhällsviktig verksamhet. Utgångspunkten för utredarens arbete ska dock vara att förslagen utformas så att regelbördan och administrationen för berörda entiteter minimeras. Om förslag lämnas som går utöver EU-direktivens krav, ska utredaren särskilt motivera varför dessa är nödvändiga för att uppnå nationella svenska mål och göra en analys av om förslagen är samhällsekonomiskt effektiva och hur förslagen påverkar svenska företags konkurrenskraft. Vid utformningen av förslagen ska utredaren genomgående beakta vikten av kostnadseffektivitet.

Utredaren får även ta upp andra närliggande frågor i samband med de frågeställningar som ska utredas och lägga fram de förslag som behövs.

Utredaren ska därför

- beakta gränsdragningen mellan NIS2-direktivet och CER-direktivet samt relevanta sektorsspecifika unionsrättsakter vid utformningen av sina förslag,
- analysera hur samordningsvinster kan uppnås i entiteternas säkerhetsarbete enligt NIS2-direktivet, CER-direktivet och andra relevanta regelverk samt även i övrigt överväga hur förslagen kan utformas på ett sätt som är kostnadseffektivt och som inte är oproportionerligt administrativt betungande för berörda entiteter,
- överväga hur de olika kategorierna av aktörer ska benämnas i en kommande svensk lagstiftning och hur EU-direktivens terminologi i övrigt kan anpassas till vedertagna begrepp i relevant nationell reglering, och
- lämna förslag till nödvändiga författningsändringar.

Sekretess och dataskydd

Entiteter enligt såväl NIS2-direktivet som CER-direktivet kommer att vara skyldiga att rapportera incidenter. Incidentrapporterna kommer många gånger att innehålla känslig information, t.ex. om incidentens art, orsak och konsekvenser. Entiteterna kommer även vara skyldiga att till tillsynsmyndigheterna tillhandahålla information som är nödvändig för tillsynen, såsom uppgifter om säkerhets- och bevakningsåtgärder och resultat av genomförda säkerhetsrevisioner.

Såväl NIS2-direktivet som CER-direktivet ställer krav på att konfidentialitet för information som utbyts enligt direktiven bevaras. Det behöver mot denna bakgrund säkerställas att det finns ett tillräckligt skydd för uppgifter som ska rapporteras vid incidenter och tillhandahållas vid tillsyn. Av särskilt intresse i detta sammanhang är bestämmelsen i 18 kap. 8 § offentlighets- och sekretesslagen (2009:400), förkortad OSL, som reglerar sekretess för uppgifter som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärder inom vissa närmare angivna områden. Enligt den bestämmelsen gäller sekretess för en sådan uppgift om det kan antas att syftet med åtgärden motverkas om uppgiften röjs.

I samband med remitteringen av betänkandet Informationssäkerhet för samhällsviktiga och digitala tjänster (SOU 2017:36) ansåg flera remissinstanser att det fanns behov av ett starkare sekretesskydd. Vissa av

remissinstanserna framhöll att en för svag sekretess kan göra att aktörer väljer att inte rapportera incidenter eller att lämna knapphändig information i sina incidentrapporter. Vid genomförandet av NIS-direktivet bedömde regeringen att befintliga bestämmelser om sekretess erbjöd ett tillräckligt skydd (prop. 2017/18:205 s. 81 f.). Frågan behöver emellertid analyseras på nytt med beaktande av NIS2-direktivets och CER-direktivets krav på konfidentialitet. Det behöver bl.a. övervägas om sekretessen enligt 18 kap. 8 § OSL är tillräckligt stark. Särskilt med hänsyn till CER-direktivets tillämpningsområde behöver det även analyseras om de befintliga bestämmelserna i OSL är tillräckligt omfattande och täcker samtliga områden som omfattas av direktivet.

Utredaren behöver även analysera om befintliga bestämmelser i OSL tillgodoser NIS2-direktivets och CER-direktivets krav på utlämnande av uppgifter till andra medlemsstater samt till kommissionen och Europeiska unionens cybersäkerhetsbyrå (Enisa). Detsamma gäller för kraven på skydd av uppgifter som har tagits emot.

Av NIS2-direktivet och CER-direktivet framgår att behandling av personuppgifter ska ske i enlighet med tillämpliga dataskyddsbestämmelser. Utredaren behöver analysera vilken personuppgiftsbehandling som direktiven kommer att ge upphov till och säkerställa att det finns stöd för sådan behandling.

Särskilda överväganden i fråga om såväl sekretess som dataskydd kan behöva göras när det gäller utformningen av systemet för bakgrundskontroller, inbegripet belastningsregisterkontroller, enligt CER-direktivet.

Utredaren ska därför

- ta ställning till om bestämmelserna i OSL innebär ett tillräckligt skydd för sådana uppgifter som kan komma att behandlas enligt direktiven,
- analysera vilken personuppgiftsbehandling som kan bli aktuell vid tillämpningen av direktivens bestämmelser, och
- vid behov lämna förslag till författningsändringar.

Konsekvensbeskrivningar

Utredaren ska bedöma de ekonomiska konsekvenserna av förslagen för det allmänna och för företag eller andra enskilda samt konsekvenserna i övrigt

av förslagen. Utredarens förslag ska utformas så att reglerna blir tydliga och ger så låga administrativa och andra kostnader som möjligt för entiteterna. I detta ingår att bedöma de ekonomiska konsekvenserna av förslagen för de behöriga myndigheterna. Om förslagen kan förväntas leda till kostnadsökningar för det allmänna, ska utredaren föreslå hur dessa ska finansieras. I 14 kap. 3 § regeringsformen anges att en inskränkning av den kommunala självstyrelsen inte bör gå utöver vad som är nödvändigt med hänsyn till ändamålen. Det innebär att en proportionalitetsprövning ska göras under lagstiftningsprocessen. Om något av förslagen i betänkandet påverkar den kommunala självstyrelsen ska därför, utöver dess konsekvenser, också de särskilda avvägningar som lett fram till förslaget särskilt redovisas.

Kontakter och redovisning av uppdraget

Utredaren ska hålla sig informerad om och beakta relevant arbete som pågår inom Regeringskansliet, utredningsväsendet och EU.

Utredaren ska i den utsträckning det är lämpligt ha en dialog med berörda myndigheter och organisationer och företag.

Uppdraget ska redovisas senast den 23 februari 2024.

(Försvarsdepartementet)