

Regionstyrelsen

Yttrande över betänkandet Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63)**Regionledningskontorets förslag till beslut**

Regionrådsberedningen föreslår att regionstyrelsen beslutar följande.

Regiondirektörens tjänsteutlåtande utgör Region Stockholms yttrande över betänkandet Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63).

Sammanfattning

Region Stockholm har beretts möjlighet att lämna yttrande över betänkande från Cybersäkerhetsberedningens ”Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem” (SOU 2021:63).

För att göra användningen av ett informationssystem i säkerhetskänslig verksamhet säkrare, och därmed stärka skyddet för Sveriges säkerhet, föreslår utredningen överföring av säkerhetsskyddsförordningens bestämmelser om förberedande åtgärder inför driftsättning av informationssystem till säkerhetsskyddslagen med tillkommande reglering. Åtgärder som föreslås berör driftsättning och väsentlig förändring av informationssystem i säkerhetskänslig verksamhet, bl.a. krav på godkännande, särskild säkerhetsskyddsbedömning och lämplighetsprövning, liksom utvidgad samrådsskyldighet. Samrådsmyndigheterna (Säkerhetspolisen och Försvarsmakten) föreslås ges möjligheter att besluta åtgärdsföreägganden och att förbjuda en ur säkerhetsskyddssynpunkt olämplig driftsättning eller förändring av informationssystem.

Region Stockholm tillstyrker betänkandets förslag till författningsändringar.

Bakgrund

Europeiska unionen (EU) har antagit ett antal strategier, policys och förordningar för att stärka cybersäkerheten i unionen och medlemsstaterna.¹ Det huvudsakliga

¹ Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av

syftet med förordningen är att uppnå en hög nivå i fråga om cybersäkerhet, cyberresiliens och förtroende inom unionen och säkerställa en väl fungerande inre marknad.²

Utredningen överlämnade sitt delbetänkande Kompletterande bestämmelser till EU:s cybersäkerhetsakt (SOU 2020:25). Riksdagen har fattat beslut om att lagen med kompletterande bestämmelser till EU:s cybersäkerhetsakt ska träda i kraft den 28 juni 2021.³ I lagen finns kompletterande nationella bestämmelser om bl.a. nationell myndighet för cybersäkerhetscertifiering, tillsyn, sanktioner och förfarandet vid cybersäkerhetscertifiering.

Utredningens uppdrag är avgränsat till att överväga om det finns anledning att införa en nationell särskilt anpassad certifieringsordning för IKT-produkter, -tjänster och -processer i nätverks- och informationssystem⁴ i säkerhetskänslig verksamhet och/eller krav på godkännande av en myndighet innan sådana IKT-produkter, -tjänster och -processer i nätverks- och informationssystem får driftsättas. Utredningen konstaterar att enskilda åtgärder av detta slag inte ensamt utgör varken tillräckliga åtgärder för att möta generella krav på informations- och cybersäkerhet eller ens möta kraven på säkerhet i nätverks- och informationssystem i säkerhetskänslig verksamhet, då även övriga förutsättningar för en fullgod informations- och cybersäkerhet måste föreligga.

För att göra användningen av ett informationssystem i säkerhetskänslig verksamhet säkrare, och därmed stärka skyddet för Sveriges säkerhet, föreslår utredningen ändringar i säkerhetsskyddslagen, bl.a. överföring av bestämmelser från säkerhetsskyddsförordningen till säkerhetsskyddslagen, samt utvidgad samrådsskyldighet och möjligheter att besluta åtgärdsföreläggande och förbud mot driftsättning av informationssystem i säkerhetskänslig verksamhet.

Föreslagna ändringar innebär bl.a. följande åtgärder.

informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) trädde i kraft den 27 juni 2019.

² Åtgärder som bl.a. rör försvar och nationell säkerhet faller utanför EU:s kompetens (art. 4.2 EU-fördraget).

³ Lag (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt.

Förordning (2021:555) med kompletterande bestämmelser till EU:s cybersäkerhetsakt

⁴ För nätverks- och informationssystem som används i eller har betydelse för säkerhetskänslig verksamhet finns i dag särskilda krav i säkerhetsskydds-förordningen (2018:658). Bestämmelserna innehåller även krav på samråd med Säkerhetspolisen eller Försvarsmakten i de fall informationssystemen kan komma att behandla säkerhetsskyddsklassificerade uppgifter av visst slag och informationssystem där obehörig åtkomst till systemen kan medföra en skada för Sveriges säkerhet som inte är obetydlig.

- Säkerhetsskyddsförordningens bestämmelser om förberedande åtgärder inför driftsättning av informationssystem ska överföras till säkerhetsskyddslagen.
- Befintligt krav på verksamhetsutövare att göra en särskild säkerhetsskyddsbedömning utvidgas till att även omfatta planerade väsentliga förändringar av informationssystem som kan ha betydelse för säkerhetskänslig verksamhet.
- Verksamhetsutövare ska pröva lämpligheten av en planerad driftsättning eller väsentlig förändring av informationssystem som har betydelse för säkerhetskänslig verksamhet. Om lämplighetsprövningen leder till bedömningen att det planerade förfarandet är olämpligt från säkerhetsskyddssynpunkt ska det inte inledas.
- Lämplighetsprövningen ska, liksom den särskilda säkerhetsskyddsbedömningen, dokumenteras.
- I fall verksamhetsutövarens lämplighetsprövning leder till bedömningen att det planerade förfarandet inte är olämpligt från säkerhetsskyddssynpunkt ska verksamhetsutövaren – om övriga rekvisit för samråd är uppfyllda – samråda med ansvarig tillsynsmyndighet (Säkerhetspolisen).
- Verksamhetsutövares skyldighet att, inför driftsättning eller väsentlig förändring av vissa informationssystem, samråda med Säkerhetspolisen eller Försvarsmakten ska inte begränsas till att ske i form av en skriftlig process.
- Säkerhetspolisen och Försvarsmakten ska, i egenskap av samrådsmyndigheter enligt säkerhetsskyddslagen, få inleda samråd och inom ramen för ett samråd besluta åtgärdsföreläggande mot verksamhetsutövaren att vidta en säkerhetsskyddsåtgärd i berört informationssystem.
- Samrådsmyndigheterna ska även få möjlighet att förbjuda en ur säkerhetsskyddssynpunkt olämplig driftsättning eller förändring åsidosätter samrådsmyndighetens eller agerar i strid med meddelat förbud.
- Tillsynsmyndigheterna får en ny undersökningsbefogenhet genom möjligheten att, vid äventyr av vite, få tillgång till verksamhetsutövares informationssystem.

Utredningen föreslår att regeringen ger Försvarets materielverk (FMV) i uppdrag att, i samråd och samverkan med främst de myndigheter som ingår i det nationella cybersäkerhetscentret, utveckla formerna för hur gemensamt framtagna hot-, sårbarhets- och riskbedömningar samt skyddsprofiler kan tas fram till stöd för kravställning på IKT-produkter, -tjänster och -processer som ska användas i nätverks- och informationssystem i säkerhetskänslig verksamhet.

Lagändringarna föreslås träda i kraft 2022-07-01.

Fastighets- och servicenämnden, Trafiknämnden, Karolinska universitetssjukhuset och Stockholms läns sjukvårdsområde (SLSO) har beretts möjlighet att lämna synpunkter på betänkandet.

Karolinska universitetssjukhuset har i yttrande 2021-10-21 avstått från att lämna specifika synpunkter.

SLSO har i beslut 2021-10-20, § 9, påtalat att förslagen för SLSO:s del bedöms vara av begränsad betydelse. Bedömningen är att de förslag som utredningen presenterar är bra och skulle innebära en trygghet och säkerhet i arbetet med att driftsätta ett system som är av betydelse för Sveriges säkerhet.

Fastighets- och servicenämnden har genom tjänstemannayttrande på delegation från nämnden 2021-10-28 ställt sig positiva till utredningens förslag, men menar också att konsekvenserna för regioner inte är tillräckligt utredda. Förvaltningen ser en risk för administrativa kostnader och ökade ledtider. Förvaltningen lyfter även behovet av begreppsförtydliganden och vägledningar, och betonar vikten av beställarkompetens och expertis i framtida upphandlingar.

Trafiknämnden har vid remisstidens utgång inte inkommit med yttranden.

Region Stockholms yttrande

Regionledningskontoret är positiva till utredningens förslag och tillstyrker betänkandets förslag till författningsändringar.

Med den tilltagande digitaliseringen och globaliseringen skapas nya former för kommunikation och informationslagring i snabb takt, och med det nya hot och risker mot offentliga och privata aktörer. Region Stockholm noterar den av utredningen framförda bedömningen att den föreslagna regleringen i viss mån påverkar den kommunala självstyrelsen, och tillstyrker utredningens bedömning att författningsändringarna är nödvändiga för att skydda de mest skyddsvärda verksamheterna i samhället.

Ekonomiska konsekvenser

Regionstyrelsens beslut innebär inga ekonomiska konsekvenser.

De ekonomiska konsekvenserna av utredningens förslag bedöms troligen vara begränsade och bör ställas mot det stärkta skydd som föreslagna

författningsändringar medför för de mest skyddsvärda verksamheterna i Sverige.

Carina Lundberg Uudelepp
Regiondirektör

Susanne Bayard
IT-direktör

Beslutsunderlag

1. Sammanfattning av SOU 2021:63, Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem
2. Karolinska universitetssjukhuset yttrande den 21 oktober 2021
3. Stockholms läns sjukvårdsområdes yttrande den 20 oktober 2021
4. Fastighets- och servicenämndens yttrande den 28 oktober 2021

Beslutsexpediering

1. Karolinska universitetssjukhuset
2. Stockholms läns sjukvårdsområde
3. Fastighets- och servicenämnden

Regionstyrelsen

PROTOKOLL
2021-12-14

RS 2021-0043

§ 231**Yttrande över betänkandet Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63)**

RS 2021-0750

Ärendebeskrivning

Region Stockholm har beretts möjlighet att lämna yttrande över betänkande från Cybersäkerhetsberedningens "Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem" (SOU 2021:63).

Beslutsunderlag

Regiondirektörens tjänsteutlåtande

Sammanfattning av SOU 2021:63, Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem

Karolinska universitetssjukhuset yttrande den 21 oktober 2021

Stockholms läns sjukvårdsområdes yttrande den 20 oktober 2021

Fastighets- och servicenämndens yttrande den 28 oktober 2021

Yrkanden

1:e vice ordförande Gustav Hemming (C) yrkar bifall till regionrådsberedningens förslag i skrivelse den 1 december.

Beslut

Regionstyrelsen beslutar följande.

Regiondirektörens tjänsteutlåtande utgör Region Stockholms yttrande över betänkandet Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63).

V-ledamöterna deltar ej i beslutet.

Särskilt uttalande

S-ledamöterna anmäler särskilt uttalande (bilaga).

Expedieras till

Akten



Ordförande



Justerare

Exp. datum

Sign.

Regionstyrelsen

SÄRSKILT UTTALANDE
2021-12-14Ärende 10
RS 2021-0750**Yttrande över betänkandet Sveriges säkerhet - behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63)**

Socialdemokraterna delar regionledningskontorets synpunkter på betänkandet, och håller med om att cybersäkerhet och skydd för informationssystem är en väldigt viktig fråga för regionen och alla dess verksamheter.

Men även regionen i sig har ett ansvar att skydda information och data. Vi oroar oss över högerstyrets naiva inställning till främmande makts investeringar i den svenska välfärden och infrastrukturen, och vad det kan innebära för region Stockholms säkerhet.

Vi lyfte i vårt budgetförslag för 2022 särskilt vikten av en brandvägg mot auktoritära regimer, speciellt kopplat till områden som rör vårddata och personlig integritet.

Därutöver har vi inför upphandlingar av samhällsviktig kollektivtrafik lyft frågan om främmande makts medverkan i de processerna och hur man agerar för att säkerhetsklassad information inte ska hamna i fel händer.

