Rigmor Söderberg

Från: Christina Siwring <christina.siwring@regeringskansliet.se>
Skickat: den 8 oktober 2024 14:48
Till: registrator@svk.se; support@arelion.com; bolagsverket@bolagsverket.se; registrator@bra.se; registrator@chalmers.se; domstolsverket@dom.se; info@drivkraftsverige.se; registrator; info@enerigiforetagen.se; info@energigas.se; registrator; kommunstyrelse@enkoping.se; kommun@falkenberg.se; kontaktcenter@falun.se; info@finansbolagen.se; press@bankid.com; finansinspektionen; flenskommun@flen.se; fortv; registrator; fra@fra.se; registrator; exp-hkv; undom; huvudkontoret; daniel.aldstam@globalconnect.se; regiongotland@gotland.se; kommunstyrelsen@gavle.se; stadsledningskontoret@stadshuset.goteborg.se; info@ikem.se; registrator; registrator vss; imy; kommunstyrelse@jonkoping.se; kommun@kalix.se; kommun@kalmar.se; info@karlskoga.se; karlskrona.kommun@karlskrona.se; karlstadskommun@karlstad.se; registrator; kemi; registrator; konkurrensverket; hk; registrator; registrator; info@lrf.se; info@lantmannen.com; kommun@leksand.se; kommunen@lillaedet.se; linkopingskommun@linkoping.se; info@li.se; henrik.ekelund@svenskhandel.se; livsmedelsverket; lfv@lfv.se; Luleå kommun; info@lif.se; registrator; blekinge@lansstyrelsen.se; dalarna@lansstyrelsen.se; gotland@lansstyrelsen.se; gavleborg@lansstyrelsen.se; halland@lansstyrelsen.se; jamtland@lansstyrelsen.se; jonkoping@lansstyrelsen.se; kalmar@lansstyrelsen.se; kronoberg@lansstyrelsen.se; Norrbotten@lansstyrelsen.se; skane@lansstyrelsen.se; stockholm@lansstyrelsen.se; sodermanland@lansstyrelsen.se; uppsala@lansstyrelsen.se; vasterbotten@lansstyrelsen.se; vasternorrland@lansstyrelsen.se; vastmanland@lansstyrelsen.se; vastragotaland@lansstyrelsen.se; orebro@lansstyrelsen.se; ostergotland@lansstyrelsen.se; kommunstyrelsen@malmo.se; registrator@digg.se; registrator; registrator; registrator@mtfa.se; registrator; kommunstyrelsen@nynashamn.se; prv; registrator; registrator kansli; pts; Regelrådet; regionen@rjl.se; regionnorrbotten@norrbotten.se; region@skane.se; registrator.rlk@regionstockholm.se; post@regionsormland.se; region@regionostergotland.se; Justitieombudsmannen; reception.awl@ri.se; rymdstyrelsen; info@salem.se; support@scrive.com; sjofartsverket@sjofartsverket.se; registrator; socialstyrelsen; info@sparbankerna.se; registrator; registrator; jordbruksverket; registrator@statenssc.se; registrator; kund@svoa.se; kommunstyrelsen@stockholm.se; registrator; registrator; kommun@strangnas.se; sundsvalls.kommun@sundsvall.se; info@svenskhandel.se; info@swedishbankers.se; info@sscspace.com; kansliet@stadsnatsforeningen.se; remisser@svensktnaringsliv.se; svensktvatten@svensktvatten.se; info@transportforetagen.se; info@skr.se; info@swedavia.se; kommun@saffle.se; info@soff.se; sakint; sakerhetspolisen@sakerhetspolisen.se; almega@almega.se; info@teknikforetagen.se; tillvaxtverket; registrator; exp@pliktverket.se; trafikverket; kontakt; trelleborgs.kommun@trelleborg.se; tullverket; umea.kommun@umea.se; registrator; vinnova; registrator; kommunstyrelsen@vasteras.se; kommunstyrelsen@vaxjo.se; kundcenter@ostersund.se; kommunen@osthammar.se; kontakt@bya.se; forvaltningsrattenilinkoping; registrator; forvaltningsratteniumea; registratur; info@svenskdagligvaruhandel.se; kammarrattenijonkoping; info@lo.se; kansliet@sjf.se; info@flygplatser.se; info@tu.se; smhi; info@advokatsamfundet.se; kansli@saco.se; info; info@transportforetagen.se; info@industriarbetsgivarna.se; varmland@lansstyrelsen.se
Kopia: Fö Registrator; betankande@elanders.com; FÖ Remisspublicering; Malin Liljeskog
Ämne: Remiss - betänkandet Motståndskraft i samhällsviktiga tjänster (SOU 2024:64). Svar senast 13/1 2025.
Bifogade filer: Remissmissiv CER 241008 VR tillg anp NY.pdf; SOU 2024_64 (003) 241008 VR tillg anp.pdf

Uppföljningsflagga: Följ upp
Flagga: Har meddelandeflagga

Kategorier: Rigmor
AppServerName: p360_prod
ArchiveStatusCode: 3
DocumentID: RR 2024-245:01
DocumentIsArchived: -1

Hej,

Bifogar remiss samt SOU 2024:64 betänkandet Motståndskraft i samhällsviktiga tjänster.

Med vänlig hälsning

Christina Siwring
Kanslisekreterare
Försvarsdepartementet
Rättssekretariatet
103 33 Stockholm
Tfn 08-405 21 55
Mobil 070-654 1476
christina.siwring@regeringskansliet.se
www.regeringen.se

Regeringskansliet

Regeringskansliet

Remiss

2024-10-08
Fö2024/01550

Försvarsdepartementet
Rättssekretariatet

Remiss av betänkandet Motståndskraft i samhällsviktiga tjänster (SOU 2024:64)

Remissinstanser

1. Affärsverket svenska kraftnät
2. Arbetsgivarverket
3. Arelion Sweden AB
4. Bevakningsbranschens Yrkes- och Arbetsmiljönämnd (BYA)
5. Bolagsverket
6. Brottsförebyggande rådet
7. Chalmers tekniska högskola AB
8. Domstolsverket
9. Drivkraft Sverige
10. E-hälsomyndigheten
11. Energiföretagen Sverige
12. Energigas Sverige
13. Energimarknadsinspektionen
14. Enköpings kommun
15. Falkenbergs kommun
16. Falu kommun
17. Finansbolagens Förening
18. Finansiell ID-Teknik BID AB
19. Finansinspektionen

Telefonväxel: 08-405 10 00
Fax: 08-723 11 89
Webb: www.regeringen.se

Postadress: 103 33 Stockholm
Besöksadress: Jakobsgatan 9
E-post: fo.registrator@regeringskansliet.se

20. Flens kommun
21. Fortifikationsverket
22. Försvarets materielverk
23. Försvarets radioanstalt
24. Försvarshögskolan
25. Försvarsmakten
26. Försvarsunderrättelsedomstolen
27. Försäkringskassan
28. Förvaltningsrätten i Linköping
29. Förvaltningsrätten i Umeå
30. GlobalConnect AB
31. Gotlands kommun
32. Gävle kommun
33. Göteborgs kommun
34. IKEM Innovations- och kemiindustrierna i Sverige
35. Industriarbetsgivarna i Sverige Service AB
36. Inspektionen för strategiska produkter
37. Inspektionen för vård och omsorg
38. Integritetsskyddsmyndigheten
39. Jönköpings kommun
40. Kalix kommun
41. Kalmar kommun
42. Kammarkollegiet
43. Kammarrätten i Jönköping
44. Karlskoga kommun
45. Karlskrona kommun
46. Karlstads kommun
47. Karolinska institutet
48. Kemikalieinspektionen
49. Kommerskollegium

50. Konkurrensverket
51. Kriminalvården
52. Kungl. Tekniska högskolan
53. Kustbevakningen
54. Landsorganisationen i Sverige (LO)
55. Lantbrukarnas riksförbund
56. Lantmännen
57. Leksands kommun
58. Lilla Edets kommun
59. Linköpings kommun
60. Livsmedelsföretagen
61. Livsmedelsgrossisterna
62. Livsmedelsverket
63. Luftfartsverket
64. Luleå kommun
65. Läkemedelsindustriföreningen
66. Läkemedelsverket
67. Länsstyrelsen i Blekinge län
68. Länsstyrelsen i Dalarnas län
69. Länsstyrelsen i Gotlands län
70. Länsstyrelsen i Gävleborgs län
71. Länsstyrelsen i Hallands län
72. Länsstyrelsen i Jämtlands län
73. Länsstyrelsen i Jönköpings län
74. Länsstyrelsen i Kalmar län
75. Länsstyrelsen i Kronobergs län
76. Länsstyrelsen i Norrbottens län
77. Länsstyrelsen i Skåne län
78. Länsstyrelsen i Stockholms län
79. Länsstyrelsen i Södermanlands län

80. Länsstyrelsen i Uppsala län
81. Länsstyrelsen i Värmlands län
82. Länsstyrelsen i Västerbottens län
83. Länsstyrelsen i Västernorrlands län
84. Länsstyrelsen i Västmanlands län
85. Länsstyrelsen i Västra Götalands län
86. Länsstyrelsen i Örebro län
87. Länsstyrelsen i Östergötlands län
88. Malmö kommun
89. Myndigheten för digital förvaltning
90. Myndigheten för psykologiskt försvar
91. Myndigheten för samhällsskydd och beredskap
92. Myndigheten för totalförsvarsanalys
93. Naturvårdsverket
94. Netnod AB
95. Nynäshamns kommun
96. On Tower Sweden AB/Cellnex Sverige
97. Patent- och registreringsverket
98. Pensionsmyndigheten
99. Polismyndigheten
100. Post- och telestyrelsen
101. Regelrådet
102. Region Jönköpings län
103. Region Norrbotten
104. Region Skåne
105. Region Stockholm
106. Region Sörmland
107. Region Östergötland
108. Riksdagens ombudsmän
109. RISE Research Institutes of Sweden AB

110. Rymdstyrelsen
111. Salems kommun
112. Scrive AB
113. Sjöfartsverket
114. Skatteverket
115. Socialstyrelsen
116. Sparbankernas Riksförbund
117. Statens energimyndighet
118. Statens inspektion för försvarsunderrättelseverksamheten
119. Statens jordbruksverk
120. Statens servicecenter
121. Statskontoret
122. Stockholm Vatten och Avfall AB
123. Stockholms kommun
124. Stockholms universitet
125. Strålsäkerhetsmyndigheten
126. Strängnäs kommun
127. Sundsvalls kommun
128. Svensk Dagligvaruhandel
129. Svensk Handel
130. Svenska Bankföreningen
131. Svenska Journalistförbundet
132. Svenska Regionala Flygplatser AB
133. Svenska rymdaktiebolaget (SSC)
134. Svenska stadsnätsföreningen
135. Svenska Tidningsutgivareföreningen (TU)
136. Svenskt Näringsliv
137. Svenskt Vatten
138. Sveriges advokatsamfund
139. Sveriges akademikers centralorganisation (Saco)

140. Sveriges Hamnar
141. Sveriges Kommuner och Regioner
142. Sveriges meteorologiska och hydrologiska institut (SMHI)
143. Swedavia AB
144. Säffle kommun
145. Säkerhets- och försvarsföretagen
146. Säkerhets- och integritetsskyddsnämnden
147. Säkerhetspolisen
148. TechSverige
149. Teknikföretagen
150. Tillväxtverket
151. Tjänstemännens centralorganisation (TCO)
152. Totalförsvarets forskningsinstitut
153. Totalförsvarets plikt- och prövningsverk
154. Trafikverket
155. Transportföretagen
156. Transportstyrelsen
157. Trelleborgs kommun
158. Tullverket
159. Umeå kommun
160. Uppsala universitet
161. Verket för innovationssystem (Vinnova)
162. Vetenskapsrådet
163. Västerås kommun
164. Växjö kommun
165. Östersunds kommun
166. Östhammars kommun

Remissvaren ska ha kommit in till Försvarsdepartementet **senast den 13 januari 2025**. Svaren bör lämnas per e-post till

fo.remissvar@regeringskansliet.se och med kopia till alfred.pucek@regeringskansliet.se. Ange diarienummer Fö2024/01550 och remissinstansens namn i ämnesraden på e-postmeddelandet.

Med hänsyn till den korta fristen för direktivets genomförande är utrymmet för anstånd ytterst begränsat.

Svaret bör lämnas i två versioner: den ena i ett bearbetningsbart format (t.ex. Word), den andra i ett format (t.ex. pdf) som följer tillgänglighetskraven enligt lagen (2018:1937) om tillgänglighet till digital offentlig service. Remissinstansens namn ska anges i namnet på respektive dokument.

Remissvaren kommer att publiceras på regeringens webbplats.

I remissen ligger att regeringen vill ha synpunkter på förslagen eller materialet i betänkandet. Om remissen är begränsad till en viss del av betänkandet, anges detta inom parentes efter remissinstansens namn i remisslistan. En sådan begränsning hindrar givetvis inte att remissinstansen lämnar synpunkter också på övriga delar.

Myndigheter under regeringen är skyldiga att svara på remissen. En myndighet avgör dock på eget ansvar om den har några synpunkter att redovisa i ett svar. Om myndigheten inte har några synpunkter, räcker det att svaret ger besked om detta.

För **andra remissinstanser** innebär remissen en inbjudan att lämna synpunkter.

Betänkandet kan laddas ned från Regeringskansliets webbplats www.regeringen.se.

Remissinstanserna kan utan kostnad beställa tryckta exemplar av betänkandet via ett beställningsformulär hos Elanders Sverige AB.

Råd om hur remissyttranden utformas finns i Statsrådsberedningens promemoria Svara på remiss (SB PM 2021:1). Den kan laddas ned från Regeringskansliets webbplats www.regeringen.se.

Charlotta Fröcklin
Ämnesråd

Kopia till

Elanders Sverige AB, e-postadress: betankande@elanders.com

Till statsrådet Carl-Oskar Bohlin

Regeringen beslutade den 23 februari 2023 att tillkalla en särskild utredare med uppgift att föreslå de anpassningar av svensk rätt som är nödvändiga för att EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2-direktivet) och EU:s direktiv om kritiska entiteters motståndskraft (CER-direktivet) ska kunna genomföras. Uppdraget skulle redovisas ett år senare.

Som särskild utredare förordnades dagen efter juristen Annette Norman.

Anställda som sekreterare i utredningen har varit strategen Andreas Häll från den 27 februari 2023, hovrättsassessorn Nina Nordengren mellan den 15 mars och 30 juni 2023 och därefter som huvudsekreterare, samt seniore analytikern Love de Besche från den 1 september 2023.

Som sakkunniga förordnades den 14 april 2023 rättssakkunniga Lisa Wilander, Försvarsdepartementet, departementssekreteraren Tommy Forsell, Försvarsdepartementet, rättssakkunniga Mathilda Klang, Justitiedepartementet, kanslirådet Anna Stenberg, Finansdepartementet, numera kanslirådet Shafagh Elhami, Finansdepartementet och departementssekreteraren Marina Fransson, Landsbygds- och infrastrukturdepartementet. Shafagh Elhami entledigades den 6 september 2023 och ersattes samma dag av departementssekreteraren Agata Uhlhorn, Finansdepartementet.

Som experter förordnades den 14 april 2023 verksamhetsstrategen Helena Andersson, Myndigheten för samhällsskydd och beredskap (MSB), seniore it- och informationssäkerhetsspecialisten Magnus Bergström, Integritetsskyddsmyndigheten (IMY), handläggaren Martin Carlsson, Statens energimyndighet, professorn Mads Dam, Kungliga Tekniska högskolan (KTH), NIS-informationssäkerhetsinspektören Kristin Eriksson, Transportstyrelsen, seniore juristen Sebastian Fichtel, Finansinspektionen, ingenjören Anders Franzén, Post- och telestyrel-

sen (PTS), beredskapshandläggaren Per Gustavsson, Livsmedelsverket, it-säkerhetschefen Lars Hjelm, Försäkringskassan, förbundsjuristen Magnus Ljung, Sveriges Kommuner och Regioner (SKR), juristen Emmelie Pettersén Uggla, Socialstyrelsen, gruppchefen Karin Stoffel, Polismyndigheten och verksjuristen Robert Tolonen Scherman, Säkerhetspolisen. Den 28 april 2023 förordnades handläggaren Linda Avad, Försvarsmakten och verksjuristen Fredrik Qvist, Bolagsverket som experter. Linda Avad entledigades den 18 september och analytikern Erik Hansen, Försvarsmakten, förordnades som expert samma dag. Mathilda Klang entledigades den 16 februari 2024. Tommy Forsell, Karin Stoffel och Lars Hjelm entledigades den 5 mars 2024 och kanslirådet Jessika Bohr, Försvarsdepartementet, förordnades som sakkunnig samma dag. Mads Dam entledigades den 15 mars 2024. Erik Hansen entledigades den 11 april 2024 och försvarsjuristen Sara Westerlund, Försvarsmakten, förordnades som expert samma dag.

Som ledamöter i en till utredningen knuten referensgrupp förordnades fr.o.m. den 14 april 2023 seniora juristen Sarah Berwick, Svenskt vatten, avdelningschefen Johan Billow, Försvarets materielverk (FMV), enhetschefen Cem Göcgören, Affärsverket svenska kraftnät, ansvarige för säkerhet och beredskap Emma Johansson, Energiföretagen, handläggaren inom rymdlägesbild Kristina Pålsson, Rymdstyrelsen, näringspolitiske experten Fredrik Sand, TechSverige, näringspolitiske experten Patrik Sandgren, Teknikföretagen, beredskapshandläggaren Fredrik Toreheim, Naturvårdsverket och juristen Åsa Wiklund Fredström, Kemikalieinspektionen. Fredrik Toreheim entledigades den 21 september 2023 och säkerhetsspecialisten Line Zandén förordnades att ingå i referensgruppen samma dag. Cem Göcgören entledigades den 23 oktober 2023 och säkerhetsskyddsspecialisten Elin Devonport Wretman, Affärsverket svenska kraftnät, förordnades att ingå i referensgruppen samma dag. Fredrik Sand entledigades den 22 januari 2024 från uppdraget att ingå i referensgruppen och förordnades att vara expert i utredningen samma dag. Sarah Berwick samt Line Zandén entledigades den 7 maj 2024 och dricksvattenexperten Birger Wallsten, Svenskt vatten, samt handläggaren Pontus Cronholm, Naturvårdsverket, förordnades att ingå i referensgruppen samma dag.

Förordnandet för experterna är personligt. Likväl hänvisar utredningen till expertens myndighet eller motsvarande när det gäller redovisade synpunkter. Experterna och de sakkunniga har i allt väsentligt

ställt sig bakom utredningens överväganden och förslag. De särskilda ståndpunkter som enskilda experter och sakkunniga kan ha haft i olika frågor har berörts i texterna eller som möjliga alternativa bedömningar.

Genom tilläggsdirektiv den 11 januari 2024 förlängdes utredningstiden för den del av uppdraget som avser anpassningar med anledning av CER-direktivet (dir. 2024:3).

Utredningen överlämnade delbetänkandet *Nya regler om cybersäkerhet* (SOU 2024:18) i mars 2024. Härmed överlämnar utredningen slutbetänkandet *Motståndskraft i samhällsviktiga tjänster* (SOU 2024:64).

Utredningens uppdrag är därmed slutfört.

Stockholm i september 2024

Annette Norman

/Andreas Häll
Love de Besche

Innehåll

Bilagor

Sammanfattning

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, finansmarknadsinfrastruktur, 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.

[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.

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 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.

[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).

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 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

[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.

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 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 inne-

bär att sanktionsavgiften för enskilda kritiska verksamhetsutövare ska bestämmas till lägst 5 000 kronor och högst till det högsta av:

1. 2 procent av den kritiska verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. 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.

Summary

CER Directive

On 14 December 2022, the European Parliament and the Council of the European Union adopted the Directive on the resilience of critical entities (CER Directive)[1]. The aim of the Directive is to strengthen entities' resilience and ability to provide essential services in the internal market.

According to the Directive, by 17 July 2026 each Member State must identify operators that offer essential services in the energy, transport, banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, public administration, space and production, processing and food distribution sectors. By 17 January 2026, each Member State must carry out a national risk assessment and adopt a strategy for enhancing the resilience of critical entities.

The Directive requires critical entities to carry out a risk assessment and take measures aimed at enhancing resilience, including background checks, and to report incidents. An entity must carry out the risk assessment within nine months of being notified that it has been identified as a critical entity. The required resilience measures should be applied 10 months after the critical entity has been notified of its identification as a critical entity. The Directive also contains provisions on critical entities of particular European significance.

It also contains provisions on supervision and penalties, and a framework for cooperation between Member States.

The Directive establishes harmonised minimum rules, which means that Swedish legislation could impose more extensive obligations.

[1] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

By 17 October 2024, the Member States must adopt and publish the provisions that are necessary for compliance with the Directive. The provisions will apply from 18 October 2024.

From 18 October 2024, the Directive will replace Council Directive 2008/114/EC on the identification and designation of European critical infrastructure and assessment of the need to improve the protection of that infrastructure. References to the repealed Directive will be construed as references to the new Directive.

The Inquiry's remit

In this final report, the Inquiry outlines its proposals on incorporating the CER Directive into Swedish law and proposals on amending the public access to information and confidentiality provisions, the Protective Security Act and the proposed cybersecurity act. In its interim report *New rules on cybersecurity* (SOU 2024:18), the Inquiry outlined proposals on incorporating the Directive on measures for a high common level of cybersecurity across the Union (NIS 2)[2].

The Inquiry has been tasked with proposing amendments to Swedish law that are necessary for implementation of the CER Directive. This includes proposing how the identification of and requirements placed on entities covered by the Directive should be regulated and how the roles as regards the various tasks and areas of responsibility prescribed under the CER Directive should be divided between Swedish government agencies.

The Inquiry's remit also includes considering whether the provisions of the Public Access to Information and Secrecy Act (2009:400) provide adequate protection for personal data that may be processed in accordance with the NIS 2 and CER Directives, and proposing any amendments that are necessary for a more cohesive system between the Protective Security Act, the proposed cybersecurity act and the proposed act on resilience of critical entities, particularly with respect to supervisory authorities' powers and the size of financial penalties.

[2] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

The Inquiry should also consider issues that are common to the NIS 2 and CER Directives to the extent that they are relevant for implementation of the CER Directive.

The Inquiry's proposals

Act on resilience of critical entities

The Inquiry proposes that the CER Directive be incorporated through a new act on resilience of critical entities. The Inquiry does not propose any obligations beyond those set out in the Directive.

Who is covered by the regulations on resilience of critical entities?

The regulatory framework will apply to private and public entities that provide an essential service identified in the Annex to the Directive. The Directive also requires that the entity has been identified as critical by a supervisory authority. Only certain limited parts of the regulatory framework apply to critical entities within the banking, financial market infrastructure and digital infrastructure sectors.

The proposal includes certain exemptions from the act's scope of application. The act shall not apply to matters covered by the proposed cybersecurity act, nor would it apply if there are provisions in other legislation on requirements concerning risk assessment, resilience measures, background checks and incident reporting, provided that the requirements have at least the equivalent effect. The act would likewise not apply to the Government, the Government Offices, missions abroad, government commissions, committees and inquiries, Parliamentary Ombudsmen, Sveriges Riksbank, the Riksdag Administration or the Courts of Sweden.

Moreover, the act would not apply to government agencies that primarily carry out law enforcement or security-sensitive activities. For other entities, Chapters 3–6 of the act would apply to parts of the essential service that are security-sensitive. This means that those entities are subject to the provisions on identification under Chapter 2 of the proposed act.

Identification of critical entities

The supervisory authorities should, by independent decision, identify critical entities within their supervisory areas. For an entity to be identified as critical in accordance with the Directive, three criteria must be fulfilled. First, the entity must provide one or multiple critical services within a sector identified in the Annex to the Directive; second, the entity must have critical infrastructure located in Sweden; and third, an incident would have a significant disruptive effect on the provision of the essential service. The Swedish Civil Contingencies Agency will issue regulations on when a disruptive effect is considered significant.

When identifying critical entities, supervisory authorities should observe the national risk assessment and the strategy for critical entities' resilience.

The supervisory authorities should keep a list of critical entities within their supervisory areas, and the Swedish Civil Contingencies Agency should keep a list of all critical entities.

Critical entities of particular European significance

Critical entities that provide an essential service to or in at least six Member States must notify their supervisory authority of this. Those critical entities will take part in the Commission's consultations. On the basis of consultations, the Commission will establish whether the critical entities are of particular European significance.

The Commission will notify the Swedish Civil Contingencies Agency of its decision as to whether a critical entity is of particular European significance, which will communicate this decision to the supervisory authority. The supervisory authority will then notify the critical entity.

The Commission will organise advisory missions to assess the measures critical entities have introduced to fulfil their obligations. An advisory mission can only take place if the Swedish Civil Contingencies Agency gives its consent after consultation with the critical entity and its supervisory authority.

Requirements concerning risk assessment, resilience measures and incident reporting

The Inquiry proposes that the Swedish Civil Contingencies Agency carry out a national risk assessment.

A critical entity must carry out a risk assessment nine months after receiving notification of being identified as a critical entity. The risk assessment must include a report on all relevant risks that could lead to an incident.

The entity must also take technical, security and organisational measures to ensure its resilience. These measures should be taken based on the risk assessment, apply an all-hazards approach and be proportionate to the risk. There should be a resilience plan in place describing measures that have been or will be taken. The supervisory authorities may issue regulations on risk assessment, measures and plans for resilience. The Swedish Civil Contingencies Agency may issue regulations for the public administration sector.

Critical entities must immediately report any incidents that entail or could entail a significant disruption of the provision of the essential service to the Swedish Civil Contingencies Agency. An initial report should be submitted within 24 hours. The Swedish Civil Contingencies Agency may issue regulations on what constitutes a significant disruption and on incident reporting.

The obligations concerning measures and incident reporting will begin to apply ten months after the date on which the entity receives notification that the supervisory authority has identified it as a critical entity.

Critical entities should also appoint a liaison officer who serves as a point of contact for relevant authorities.

Background checks

The aim of a background check is to ensure that only those deemed suitable are employed or in some other way participate in roles where participation can cause more than minor harm to the essential service.

The Inquiry proposes that critical entities carry out an analysis to determine which positions require a background check. The analysis should be documented.

The critical entity should carry out the background check and assess whether the relevant person is suitable. A background check would include verification of the person's identity and a criminal records extract. The Criminal Records Ordinance (1999:1134) stipulates what information is contained in an extract.

Completion of a background check should be documented and a record should be kept for two years.

Supervision

The Inquiry proposes that the supervisory authorities designated under the proposed cybersecurity act should also be the supervisory authorities under the proposed act on resilience of critical entities. A few supervisory authorities have been assigned a new subsector or category of entity. The public administration sector only includes government agencies. The following supervisory authorities are proposed.

Supervisory authority	Sector
Swedish Energy Agency	Energy
Swedish Transport Agency	Transport
Swedish Financial Supervisory Authority	Banking Financial market infrastructure
Health and Social Care Inspectorate	Healthcare providers[3] in the healthcare sector
Swedish Medical Products Agency	The healthcare sector, except for healthcare providers
Swedish Food Agency	Wastewater Drinking water Production, processing and distribution of food
Swedish Post and Telecom Authority	Digital infrastructure Space
The Norrbotten, Skåne, Stockholm and Västra Götaland county administrative boards	Public administration

[3] According to the definition in Article 3(g) of Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare.

Supervisory authorities should carry out supervision to ensure compliance with the proposed act and regulations issued in connection with it.

Critical entities should provide supervisory authorities with the information necessary for supervision and for the national risk assessment. Supervisory authorities should also have the right to access areas, premises and other spaces to the extent necessary for supervision. Exceptions should be made for classified information and access to organisations where security-sensitive activities are conducted.

The Swedish Civil Contingencies Agency should lead a cooperation forum composed of the supervisory authorities so as to facilitate coordination and achieve efficient and equal supervision.

Within the scope of supervision, the supervisory authority should also implement advisory missions organised by the Commission with respect to critical entities of particular European significance.

The supervisory authorities should also provide material for the national risk assessment.

Single point of contact

The Swedish Civil Contingencies Agency should be the single point of contact. This single point of contact must have a liaison function to ensure cross-border cooperation with the single points of contact of other Member States and the European Commission.

Enforcement measures and penalties

The Inquiry proposes that interventions be possible in the form of injunctions, financial penalties and reprimands issued by the supervisory authorities. The supervisory authority should intervene if an entity has disregarded its obligation to report that it provides a service to at least six Member States, carry out a risk assessment, adopt measures and plans for resilience, appoint a liaison officer, report incidents, carry out a position analysis, perform a background check or retain certain information.

The Inquiry proposes that the levels of financial penalties should be the same as for critical entities under the proposed cybersecurity

act. This means that financial penalties for individual critical entities should be set at no less than SEK 5 000 and no more than whichever is higher of:

1. 2 per cent of the critical entity's entire global turnover of the preceding fiscal year, or
2. EUR 10 000 000.

For public critical entities, the fee should be set at no less than SEK 5 000 and no more than SEK 10 000 000.

When determining the size of the financial penalty, particular consideration should be given to the damage or risk of damage that arose as a result of the infringement, whether the critical entity previously committed any infringement and the costs the entity avoided due to the infringement.

If the supervisory authority did not find grounds for intervention through an injunction or financial penalty, it should issue a reprimand. In certain cases, the supervisory authority should be able to refrain from intervening.

Cybersecurity act

An entity identified as critical under the act on resilience of critical entities should, regardless of size, be covered by the proposed cybersecurity act if its activities are identified in Annex 1 or 2 of the NIS 2 Directive and the entity is established in Sweden.

Secrecy and confidentiality

For the Swedish Civil Contingencies Agency and the supervisory authorities to be able to exchange information originating from other Member States and EU institutions that is subject to secrecy in accordance with Chapter 15, Section 1a of the Public Access to Information and Secrecy Act (2009:400), the Inquiry proposes introducing a new provision that overrides secrecy to Chapter 15.

The Inquiry further proposes strengthening secrecy protection by introducing a new secrecy provision to Chapter 18 of the Public Access to Information and Secrecy Act that would pertain to information in incident reporting under the proposed cybersecurity act

and the act on resilience of critical entities, and to information concerning measures taken in response to such incidents. It is proposed that a reverse requirement of damage apply to the provision (i.e. that there be a presumption that secrecy applies), and that the right to report and disclose information be limited. It is additionally proposed that chronological registers of incidents kept by reporting authorities, supervisory authorities and the Swedish Civil Contingencies Agency be subject to secrecy.

The Inquiry proposes introducing a provision on a duty of confidentiality concerning information arising in connection with background checks. An equivalent provision is being introduced to Chapter 35 of the Public Access to Information and Secrecy Act.

The secrecy protection concerning information handled by the supervisory authorities needs to be supplemented as regards information concerning private business or operating conditions. The Inquiry therefore proposes introducing a provision to the Annex to the Public Access to Information and Secrecy Ordinance (2009:641) concerning information in activities consisting in supervision and investigation in accordance with the act on resilience of private entities.

Financial penalties in accordance with the Protective Security Act, etc.

The Inquiry proposes increasing the size of financial penalties for private entities under the Protective Security Act (2018:585). This would mean that financial penalties would be set at no less than SEK 25 000 and no more than whichever is higher of SEK 120 000 000 or 2 per cent of the entity's entire global turnover of the preceding fiscal year. The Inquiry does not propose any amendments to the Protective Security Act as regards supervisory authorities' powers.

The Inquiry has found that interventions by means of filing for a ban on exercising management functions and issuing reprimands should not be introduced to the Protective Security Act.

If a critical entity indicates that its essential service is in any part security-sensitive, the supervisory authority should be notified in accordance with the Protective Security Act. The supervisory authority should notify the supervisory authority under the proposed act on resilience of critical entities whether the critical entity has reported that it carries out security-sensitive activities.

Impact

The Inquiry's proposals would have a financial impact for the supervisory authorities, the Swedish Civil Contingencies Agency, the Swedish Police Authority and critical entities.

The Inquiry proposes that:

- the supervisory authorities receive additional funding for 2025 and 2026. The Inquiry proposes that costs for ongoing supervision should be calculated once the critical entities have been identified;
- the Swedish Civil Contingencies Agency should receive additional funding for 2025 and 2026. Costs for support in case of incidents should be established once the critical entities have been identified;
- the Swedish Police Authority's running costs for processing of criminal record extracts should be calculated once the identification of critical entities has been carried out and those entities have carried out the prescribed position analysis.

The Inquiry proposes that costs for public entities should be funded within the existing budgetary framework. As regards costs for private entities, the Inquiry proposes that there may be grounds to consider whether there is a need to introduce state aid once the number of critical entities has been identified and the risk assessments carried out.

Entry into force

The Inquiry proposes that the act on resilience of critical entities and the associated ordinance enter into force on 1 August 2025.

The proposals for the Public Access to Information and Secrecy Act and Public Access to Information and Secrecy Ordinance concerning the proposed cybersecurity act should enter into force on 1 January 2025.

The remaining proposals should enter into force on 1 August 2025.

1 Författningsförslag

1.1 Förslag till lag om motståndskraft hos kritiska verksamhetsutövare

Härigenom förskrivs 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] 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).

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.

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.

1.2 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

[1] Senaste lydelse 2019:431.

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 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.

---

[2] Senaste lydelse 2022:735.

1.3 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.

Nuvarande lydelse	*Föreslagen lydelse*
	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.
	För uppgift i en allmän handling gäller sekretessen i högst fyrtio år.

Nuvarande lydelse	*Föreslagen lydelse*
	18 kap.
	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 rumsavlyss-

[1] Senast lydelse 2024:477.

ning 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 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,

[2] Senaste lydelse 2024:328.

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.

1.4 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 verksamhets-

[1] Senaste lydelse 2021:952.

utövare 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.

1.5 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.*

Nuvarande lydelse	*Föreslagen lydelse*
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.

1.6 Förslag till förordning om motståndskraft hos kritiska verksamhetsutövare

Härigenom föreskrivs följande.

Inledande bestämmelser

1 § Denna förordning kompletterar lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare.

Uttryck i förordningen

2 § Uttryck som används i förordningen har samma innebörd som i lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare.

Undantag

Krav i andra författningar

3 § I bilagan till denna förordning anges de lagar och krav och andra författningar som innehåller krav på riskbedömning, åtgärder för motståndskraft, bakgrundskontroller och incidentrapportering med verkan som sammantaget motsvarar skyldigheterna enligt lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare.

Brottsbekämpning eller Sveriges säkerhet

4 § Fortifikationsverket, Försvarets materielverk, Försvarets radioanstalt, Försvarsmakten, Försvarsunderrättelsedomstolen, Statens inspektion för försvarsunderrättelseverksamheten, Säkerhetspolisen, Totalförsvarets forskningsinstitut och Totalförsvarets plikt- och prövningsverk bedriver säkerhetskänslig verksamhet till övervägande del.

5 § Brottsförebyggande rådet, Brottsoffermyndigheten, Ekobrottsmyndigheten, Kriminalvården, Polismyndigheten, Rättsmedicinalverket, Säkerhetspolisen och Åklagarmyndigheten bedriver brottsbekämpning till övervägande del.

Nationell riskbedömning

6 § Myndigheten för samhällsskydd och beredskap ska göra en nationell riskbedömning.

Den nationella riskbedömningen ska delges tillsynsmyndigheterna och de kritiska verksamhetsutövarna i relevanta delar.

7 § Myndigheten för samhällsskydd och beredskap ska lämna relevant information till kommissionen om de typer av risker som har identifierats i den nationella riskbedömningen, per sektor och undersektor enligt bilagan till CER-direktivet inom tre månader från det att riskbedömningen har upprättats eller uppdaterats.

Identifiering av kritiska verksamhetsutövare

Betydande störande effekt

8 § Vid bedömningen av när en störande effekt enligt 2 kap. 2 § första stycket 3 lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare är betydande ska följande kriterier beaktas.

a) Antalet användare som är beroende av den samhällsviktiga tjänst som den berörda verksamhetsutövaren tillhandahåller,

b) den grad till vilken andra sektorer och undersektorer som anges i bilagan till CER-direktivet 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) verksamhetsutövarens 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, och

f) verksamhetsutövarens betydelse för upprätthållandet av en tillräcklig nivå på den samhällsviktiga tjänsten, med beaktande av tillgången till alternativa sätt för att tillhandahålla den samhällsviktiga tjänsten.

9 § Myndigheten för samhällsskydd och beredskap får, efter att ha gett tillsynsmyndigheterna tillfälle att yttra sig, meddela ytterligare föreskrifter om när en störande effekt enligt 2 kap. 2 § första stycket 3 lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare är betydande.

Förteckning över kritiska verksamhetsutövare

10 § Myndigheten för samhällsskydd och beredskap ska upprätta en samlad förteckning över samtliga kritiska verksamhetsutövare. Av förteckningen ska framgå antalet kritiska verksamhetsutövare som har identifierats för varje sektor, undersektor som anges i bilagan till CER-direktivet samt antalet kritiska verksamhetsutövare för varje samhällsviktig tjänst.

Förteckningen ska uppdateras vid behov men minst var fjärde år.

11 § Myndigheten för samhällsskydd och beredskap ska lämna en förteckning över samhällsviktiga tjänster och om det finns ytterligare samhällsviktiga tjänster jämfört med den förteckning över samhällsviktiga tjänster som anges i kommissionens delegerade förordning, det antal kritiska verksamhetsutövare som har identifierats för varje sektor och undersektor som anges i bilagan till CER-direktivet och för varje samhällsviktig tjänst samt vilka föreskrivna tröskelvärden enligt 9 § som har tillämpats till kommissionen.

Informationen ska lämnas utan dröjsmål och därefter när det är nödvändigt men minst vart fjärde år.

Kritiska verksamhetsutövare av särskild europeisk betydelse

12 § Myndigheten för samhällsskydd och beredskap ska underrätta kommissionen om vilka kritiska verksamhetsutövare som tillhandahåller samhällsviktiga tjänster till eller i minst sex medlemsstater, vilka samhällsviktiga tjänster som erbjuds samt till eller i vilka medlemsstater den kritiska verksamhetsutövaren tillhandahåller sådana tjänster.

Samråd

13 § Myndigheten för samhällsskydd och beredskap ska delta i kommissionens samråd enligt artikel 17.2 i CER-direktivet och informera kommissionen om tjänsten som omfattas av samrådet bedöms vara en samhällsviktig tjänst. Bedömningen ska göras i samråd med berörd tillsynsmyndighet.

14 § Myndigheten för samhällsskydd och beredskap ska ta emot kommissionens underrättelse om att en kritisk verksamhetsutövare är att betrakta som kritisk verksamhetsutövare av särskild europeisk betydelse och vidarebefordra underrättelsen till berörd tillsynsmyndighet.

Rådgivande uppdrag

15 § Myndigheten för samhällsskydd och beredskap får begära att kommissionen anordnar ett rådgivande uppdrag. En sådan begäran ska ske på initiativ av den kritiska verksamhetsutövaren eller dennas tillsynsmyndighet.

16 § Ett rådgivande uppdrag som anordnas på initiativ av kommissionen eller en annan medlemsstat får genomföras först efter samtycke av Myndigheten för samhällsskydd och beredskap. Myndigheten för samhällsskydd och beredskap ska samråda med den kritiska verksamhetsutövaren av särskild europeisk betydelse och dennas tillsynsmyndighet innan ett samtycke lämnas.

17 § Ett rådgivande uppdrag som anordnas för en kritisk verksamhetsutövare som inte är av särskild europeisk betydelse får anordnas endast om verksamhetsutövaren har lämnat samtycke.

18 § Myndigheten för samhällsskydd och beredskap ska lämna förslag på experter till sådana rådgivande uppdrag som kommissionen anordnar samt utfärda säkerhetsgodkännande enligt 6 kap. 7 § lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare för experter som ska delta i ett rådgivande uppdrag.

19 § Myndigheten för samhällsskydd och beredskap ska, om begäran enligt artikel 18.3 är motiverad, tillhandahålla kommissionen den information som inhämtats enligt 3 kap. 5 § lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare.

20 § Myndigheten för samhällsskydd och beredskap ska lämna information till kommissionen och de medlemsstater till eller i vilka den samhällsviktiga tjänsten tillhandahålls om vilka åtgärder som vidtagits i enlighet med kommissionens yttrande enlig artikel 18.4 tredje stycket CER-direktivet.

Riskbedömning och åtgärder för motståndskraft

21 § Tillsynsmyndigheten får inom sitt tillsynsområde meddela föreskrifter om riskbedömning enligt 4 kap. 1 § lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare. Myndigheten för samhällsskydd och beredskap ska ges tillfälle att yttra sig.

För sektorn offentlig förvaltning får Myndigheten för samhällsskydd och beredskap meddela föreskrifter om riskbedömning enligt 4 kap. 1 § lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare.

22 § Tillsynsmyndigheten får inom sitt tillsynsområde meddela föreskrifter om åtgärder och planer för motståndskraft enligt 4 kap. 2 § lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare. Myndigheten för samhällsskydd och beredskap ska ges tillfälle att yttra sig.

För sektorn offentlig förvaltning får Myndigheten för samhällsskydd och beredskap meddela föreskrifter om åtgärder och planer för motståndskraft enligt 4 kap. 2 § lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare.

Incidentrapportering

23 § Incidentrapportering enligt 5 kap. 1 § lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare ska göras till Myndigheten för samhällsskydd och beredskap.

24 § Vid bedömningen om en incident medför en betydande störning ska särskilt följande beaktas:

1. Antal och andel användare som berörs av störningen.
2. Störningens varaktighet.
3. Det geografiska område som påverkas av störningen och om området är geografiskt isolerat.

25 § Myndigheten för samhällsskydd och beredskap får meddela föreskrifter om vad som utgör en betydande störning och om incidentrapportering enligt 5 kap. 1 § lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare. Tillsynsmyndigheterna ska ges tillfälle att yttra sig.

26 § En incidentrapport ska innehålla information som är nödvändig för att förstå incidentens art, orsak och möjliga konsekvenser.

27 § Myndigheten för samhällsskydd och beredskap ska ge den kritiska verksamhetsutövaren eventuell information som skulle kunna hjälpa den kritiska verksamhetsutövaren att reagera ändamålsenligt på incidenten.

Myndigheten för samhällsskydd och beredskap ska tillgängliggöra informationen i incidentrapporter utan dröjsmål för tillsynsmyndigheten.

Myndigheten för samhällsskydd och beredskap får i samband med en incident informera allmänheten.

28 § Myndigheten för samhällsskydd och beredskap ska informera gemensamma kontaktpunkter i andra medlemsstater om en incident har eller kan ha betydande påverkan på kritiska verksamhetsutövare och kontinuiteten i tillhandahållandet av samhällsviktiga tjänster i den medlemsstaten.

Om en incident har eller kan ha betydande påverkan på kontinuiteten i tillhandahållandet av samhällsviktiga tjänster i minst sex medlemsstater ska Myndigheten för samhällsskydd och beredskap anmäla incidenten till kommissionen.

Tillsyn

Tillsynsmyndigheter

29 § Följande myndigheter ska vara tillsynsmyndighet enligt lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare och denna förordning för angivna tillsynsområden.

Tillsynsmyndighet	Sektor
Statens energimyndighet	Energi
Transportstyrelsen	Transport
Finansinspektionen	Bankverksamhet Finansmarknadsinfrastruktur
Inspektionen för vård och omsorg	Vårdgivare[1] 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

[1] 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.

30 § Länsstyrelsen i Norrbottens län ska vara tillsynsmyndighet för verksamhetsutövare som har sitt säte i Västernorrlands, Jämtlands, Västerbottens eller Norrbottens län samt Länsstyrelsen i Västra Götaland.

31 § Länsstyrelsen i Skåne län ska vara tillsynsmyndighet för verksamhetsutövare som har sitt säte i Kronobergs, Blekinge, Kalmar eller Skåne län samt Länsstyrelsen i Stockholms län.

32 § Länsstyrelsen i Stockholms län ska vara tillsynsmyndighet för verksamhetsutövare som har sitt säte i Stockholms, Uppsala, Södermanlands, Västmanlands, Värmlands, Gotlands, Örebro, Dalarnas eller Gävleborgs län samt Länsstyrelsen i Norrbottens län.

33 § Länsstyrelsen i Västra Götalands län ska vara tillsynsmyndighet för verksamhetsutövare som har sitt säte i Hallands, Jönköpings, Västra Götalands eller Östergötlands län samt Länsstyrelsen i Skåne län.

Tillsynsmyndighetens uppgifter

34 § Tillsynsmyndigheterna ska, för sina respektive tillsynsområden

1. upprätta en förteckning över kritiska verksamhetsutövare. Av förteckningen ska framgå identiteten på den kritiska verksamhetsutövaren, antalet kritiska verksamhetsutövare som har identifierats för varje sektor, undersektor som anges i bilagan till CER-direktivet samt antalet kritiska verksamhetsutövare för varje samhällsviktig tjänst,
2. utan dröjsmål lämna förteckningen enligt punkt 1 till Myndigheten för samhällsskydd,
3. utan dröjsmål lämna uppgifter till Myndigheten för samhällsskydd och beredskap om vilka kritiska verksamhetsutövare som uppgett att den tillhandahåller samhällsviktiga tjänster till eller i minst sex medlemsstater, vilka samhällsviktiga tjänster som erbjuds samt till eller i vilka medlemsstater den kritiska verksamhetsutövaren tillhandahåller sådana tjänster,
4. underrätta den kritiska verksamhetsutövaren om att denna är att betrakta som kritisk verksamhetsutövare av särskild europeisk

betydelse och lämna information om vilka skyldigheter som följer av att vara en kritisk verksamhetsutövare av särskild europeisk betydelse,

5. lämna uppgifter till Myndigheten för samhällsskydd och beredskap om tillsynsåtgärder, inbegripet bedömningar av efterlevnad eller beslut om förelägganden och sanktioner enligt 7 kap. 2 § och 8 kap. lagen om motståndskraft hos kritiska verksamhetsutövare som tillsynsmyndigheten vidtagit avseende kritiska verksamhetsutövare av särskild europeisk betydelse,

6. lämna uppgifter till Myndigheten för samhällsskydd och beredskap om vilka åtgärder den kritiska verksamhetsutövaren av särskild europeisk betydelse har vidtagit enligt kommissionens yttrande enligt artikel 18.4 tredje stycket CER-direktivet, och

7. underrätta den eller de andra tillsynsmyndigheter som utövar tillsyn över den kritiska verksamhetsutövaren enligt lagen (2025:000) om cybersäkerhet om besluten enligt 2 kap. 1 § och 5 § lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare. Om den kritiska verksamhetsutövaren är verksam inom sektorerna bankverksamhet, finansmarknadsinfrastruktur eller digital infrastruktur ska underrättelsen även innehålla uppgift om att verksamhetsutövaren inte är skyldig att vidta sådana åtgärder som följer av 3–6 kap. i lagen om motståndskraft hos kritiska verksamhetsutövare.

Begäran om information

35 § När en tillsynsmyndighet begär information enligt 7 kap. 3 § lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare ska tillsynsmyndigheten ange syftet med begäran och precisera vilken information som krävs.

Samarbetsforum för effektiv och likvärdig tillsyn

36 § Myndigheten för samhällsskydd och beredskap ska leda ett samarbetsforum där tillsynsmyndigheterna ingår. Syftet med forumet ska vara att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn.

Gemensam kontaktpunkt

37 § Myndigheten för samhällsskydd och beredskap ska vara gemensam kontaktpunkt.

Gemensamma kontaktpunktens uppgifter

38 § Den gemensamma kontaktpunkten ska ha en sambandsfunktion för att säkerställa gränsöverskridande samarbete med gemensamma kontaktpunkter i andra medlemsstater och kommissionen.

39 § Den gemensamma kontaktpunkten ska senast den 17 juli 2028 och därefter vartannat år lämna den rapport som avses i artikel 9.3 i CER-direktivet.

40 § Den gemensamma kontaktpunkten ska i samverkan med tillsynsmyndigheten delta i de samråd som avses i artikel 11 i CER-direktivet.

Övrigt

41 § Myndigheten för samhällsskydd och beredskap och tillsynsmyndigheterna ska lämna stöd till Sveriges deltagande i den samarbetsgrupp som inrättats enligt artikel 19 i CER-direktivet.

Denna förordning träder i kraft den 1 augusti 2025.

Bilaga

1.7 Förslag till förordning om ändring i förordningen (1999:1134) om belastningsregister

Härigenom föreskrivs i fråga om förordningen (1999:1134) om belastningsregister att 22 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
22 §[1]	
Ett registerutdrag enligt 9 § andra stycket 1 lagen (1998:620) om belastningsregister ska endast innehålla uppgifter om domar, beslut eller *strafföreläggande* där	Ett registerutdrag enligt 9 § andra stycket 1 *och 7* lagen (1998:620) om belastningsregister ska endast innehålla uppgifter om domar, beslut eller *strafföreläggande* där
1. någon annan påföljd än böter har dömts ut,	1. någon annan påföljd än böter har dömts ut,
2. dagsböter har dömts ut för brott mot 3 kap. 5 §, 4 kap. 4 och 5 §§, 8, 9 och 14 kap. samt 17 kap. 1, 2 och 4 §§ brottsbalken eller lagen (2014:307) om straff för penningtvättsbrott, eller	2. dagsböter har dömts ut för brott mot 3 kap. 5 §, 4 kap. 4 och 5 §§, 8, 9 och 14 kap. samt 17 kap. 1, 2 och 4 §§ brottsbalken eller lagen (2014:307) om straff för penningtvättsbrott, eller
3. böter har dömts ut för brott som avses i 6 kap. 8 och 10 §§ samt 16 kap. 11 § brottsbalken, narkotikastrafflagen (1968:64), lagen (1991:1969) om förbud mot vissa dopningsmedel, vapenlagen (1996:67), vapenförordningen (1996:70) och äldre vapenlagstiftning.	3. böter har dömts ut för brott som avses i 6 kap. 8 och 10 §§ samt 16 kap. 11 § brottsbalken, narkotikastrafflagen (1968:64), lagen (1991:1969) om förbud mot vissa dopningsmedel, vapenlagen (1996:67), vapenförordningen (1996:70) och äldre vapenlagstiftning.

Om påföljden även avser något annat brott än de som anges i första stycket 2 och 3, ska också uppgifter om det brottet lämnas ut.

Ett registerutdrag enligt 9 § andra stycket 2 lagen om belastningsregister som den enskilde begär med hänvisning till bestämmelser i skollagen (2010:800) ska endast innehålla uppgifter om domar, beslut eller strafföreläggande där påföljd har dömts ut

[1] Senaste lydelse 2017:526.

eller åtalsunderlåtelse meddelats för brott mot 3 kap. 1, 2 och 6 §§, 4 kap. 1 §, 6 kap., 8 kap. 6 § och 16 kap. 10 a § brottsbalken. Om påföljden eller åtalsunderlåtelsen även avser något annat brott, ska också uppgifter om det brottet lämnas ut.

Ett registerutdrag enligt 9 § andra stycket 4 lagen om belastningsregister som den enskilde begär med hänvisning till bestämmelser i lagen (2007:171) om registerkontroll av personal vid vissa boenden som tar emot barn ska endast innehålla uppgifter om domar, beslut eller strafföreläggande där påföljd har dömts ut eller åtalsunderlåtelse meddelats för brott mot 3 kap. 1, 2, 5 och 6 §§, 4 kap. 1–2 och 4–5 §§, 6 kap., 8 kap. 5 och 6 §§, 16 kap. 8, 9 och 10 a §§ brottsbalken, narkotikastrafflagen, lagen om förbud mot vissa dopningsmedel, lagen (1999:42) om förbud mot vissa hälsofarliga varor, 6 § lagen (2000:1225) om straff för smuggling och 11 kap. 4 § alkohollagen (2010:1622) samt medverkan och försök till sådana brott. I fråga om brott som avses i 6 kap. brottsbalken, narkotikastrafflagen och lagen om förbud mot vissa dopningsmedel ska utdraget också innehålla uppgifter om domar, beslut och strafföreläggande där påföljd har dömts ut eller åtalsunderlåtelse meddelats för förberedelse, stämpling och underlåtenhet att avslöja brott. Om påföljden eller åtalsunderlåtelsen även avser något annat brott, ska också uppgifter om det brottet lämnas ut.

Ett registerutdrag enligt 9 § andra stycket 5 lagen om belastningsregister som den enskilde begär med hänvisning till bestämmelser i lagen (2010:479) om registerkontroll av personal som utför vissa insatser åt barn med funktionshinder ska endast innehålla uppgifter om domar, beslut eller strafföreläggande där påföljd har dömts ut eller åtalsunderlåtelse meddelats för brott mot 3 kap. 1, 2 och 6 §§, 4 kap. 1 §, 6 kap., 8 kap. 6 § och 16 kap. 10 a § brottsbalken. Om påföljden eller åtalsunderlåtelsen även avser något annat brott, ska också uppgifter om det brottet lämnas ut.

Ett registerutdrag enligt 9 § andra stycket 6 lagen om belastningsregister som den enskilde begär med hänvisning till bestämmelser i lagen (2013:852) om registerkontroll av personer som ska arbeta med barn ska endast innehålla uppgifter om domar, beslut eller strafföreläggande där påföljd har dömts ut eller åtalsunderlåtelse meddelats för brott mot 3 kap. 1, 2 och 6 §§, 4 kap. 1 §, 6 kap., 8 kap. 6 § och 16 kap. 10 a § brottsbalken. Om påföljden eller åtalsunder-

låtelsen även avser något annat brott, ska också uppgifter om det brottet lämnas ut.

Denna förordning träder i kraft den 1 augusti 2025.

1.8 Förslag till förordning om ändring i förordningen (2007:1119) med instruktion för Affärsverket svenska kraftnät

Härigenom föreskrivs i fråga om förordningen (2007:1119) med instruktion för Affärsverket svenska kraftnät att 3 § ska följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

3 §[1]

Svenska kraftnät ska också

1. bygga ut ett transmissionsnät för el i Sverige och förbindelser med elnät i andra länder baserat på samhällsekonomiska lönsamhetsbedömningar,

2. svara för tillsyn i frågor om driftsäkerhet hos det nationella elsystemet enligt ellagen (1997:857) och förordningen (2023:241) om det nationella elsystemet,

3. främja konkurrensen på elmarknaden,

4. främja forskning, utveckling och demonstration av ny teknik av betydelse för verksamheten,

5. bedriva tjänsteexport inom sitt verksamhetsområde,

6. främja dammsäkerheten i landet,

7. bygga ut, installera och förvalta ledningar för elektronisk kommunikation, främst på transmissionsnätet, samt upplåta nätkapacitet i dessa,

8. bevaka tillgången på höglastkapacitet i det svenska elsystemet och löpande förmedla information om effekttillgång till marknadens aktörer samt övervaka och utföra bedömningar av resurstillräckligheten i enlighet med artikel 20.1 i Europaparlamentets och rådets förordning (EU) 2019/943 av den 5 juni 2019 om den inre marknaden för el,

9. inom sitt verksamhetsområde se till att möjligheterna att bygga ut fossilfri elproduktion och nya användningsområden för el tas tillvara i omställningen av elsystemet,

[1] Senaste lydelse 2023:577.

10. inom sitt område inkassera kapacitetsavgifter och betalningar i enlighet med artikel 49 i förordning (EU) 2019/943,

11. även i övrigt inom sitt verksamhetsområde fullgöra uppgifter som följer av förordning (EU) 2019/943,

12. se till att de regelverk och rutiner som affärsverket disponerar över är kostnadseffektiva och enkla för medborgare och företag,

13. vartannat år genomföra och, efter att ha hört Statens energimyndighet, till Myndigheten för samhällsskydd och beredskap redovisa ett identifieringsarbete av potentiella europeiska kritiska infrastrukturer inom undersektorn el enligt 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,

14. senast den 31 maj varje år i en särskild rapport till regeringen redovisa

a) hur kraftbalansen under den senaste vintern har upprätthållits,

b) en prognos för kraftbalansen under den kommande vintern, där även omgivande länders exportmöjligheter beaktas för att inkludera en bedömning av hur mycket import Sverige kan räkna med vid topplasttimmen,

c) en bedömning av förutsättningarna för att långsiktigt upprätthålla kraftbalansen, där även omgivande länders exportmöjligheter beaktas för att

13. senast den 31 maj varje år i en särskild rapport till regeringen redovisa

a) hur kraftbalansen under den senaste vintern har upprätthållits,

b) en prognos för kraftbalansen under den kommande vintern, där även omgivande länders exportmöjligheter beaktas för att inkludera en bedömning av hur mycket import Sverige kan räkna med vid topplasttimmen,

c) en bedömning av förutsättningarna för att långsiktigt upprätthålla kraftbalansen, där även omgivande länders exportmöjligheter beaktas för att

inkludera en bedömning av hur mycket import Sverige kan räkna med vid topplasttimmen, och	inkludera en bedömning av hur mycket import Sverige kan räkna med vid topplasttimmen, och
d) vilka informationsinsatser som har riktats till aktörerna på elmarknaden i fråga om kraftbalansen,	d) vilka informationsinsatser som har riktats till aktörerna på elmarknaden i fråga om kraftbalansen,
15. vartannat år med början 2023 upprätta en tioårig investeringsplan och lämna in planen till Energimarknadsinspektionen,	*14*. vartannat år med början 2023 upprätta en tioårig investeringsplan och lämna in planen till Energimarknadsinspektionen,
16. inom sitt verksamhetsområde verka för att de energipolitiska mål som riksdagen har godkänt uppnås, och	*15*. inom sitt verksamhetsområde verka för att de energipolitiska mål som riksdagen har godkänt uppnås, och
17. vid tillämpningen av förordning (EU) 2019/941 av den 5 juni 2019 om riskberedskap inom elsektorn och om upphävande av direktiv 2005/89/EG	*16*. vid tillämpningen av förordning (EU) 2019/941 av den 5 juni 2019 om riskberedskap inom elsektorn och om upphävande av direktiv 2005/89/EG
a) ta fram underlag enligt artiklarna 7, 10, 14 och 17 i förordningen, och	a) ta fram underlag enligt artiklarna 7, 10, 14 och 17 i förordningen, och
b) särskilt samverka med Statens energimyndighet när denna fullgör sina uppgifter i egenskap av behörig myndighet enligt förordningen, i syfte att säkerställa ett effektivt utarbetande och korrekt genomförande av riskberedskapsplaner och att underlätta förebyggande och utvärdering av elkriser och informationsutbyte om sådana.	b) särskilt samverka med Statens energimyndighet när denna fullgör sina uppgifter i egenskap av behörig myndighet enligt förordningen, i syfte att säkerställa ett effektivt utarbetande och korrekt genomförande av riskberedskapsplaner och att underlätta förebyggande och utvärdering av elkriser och informationsutbyte om sådana.

Denna förordning träder i kraft den 1 augusti 2025.

1.9 Förslag till förordning om ändring i förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap

Härigenom föreskrivs att 17 a § förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap ska upphöra gälla vid utgången av juli 2025.

Nuvarande lydelse	*Föreslagen lydelse*
17 a §[1]	
Myndigheten ska vara Sveriges kontaktpunkt för skydd av europeisk kritisk infrastruktur enligt artikel 10.1 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.	

Denna förordning träder i kraft den 1 augusti 2025.

[1] Senaste lydelse 2009:611.

1.10 Förslag till förordning om ändring i offentlighets- och sekretessförordningen (2009:641)

Härigenom föreskrivs i fråga om offentlighets- och sekretessförordningen (2009:641)

dels att 3 § ska följande lydelse,

dels att bilagan till offentlighets- och sekretessförordningen (2009:641) ska ha följande lydelse.

3 §[1] Följande myndigheter ska i den utsträckning som framgår nedan inte tillämpa 5 kap. 2 § andra stycket offentlighets- och sekretesslagen (2009:400)

Myndighet	Register
Myndigheten för samhällsskydd och beredskap, tillsynsmyndighet och myndighet som rapporterar incidenter enligt lagen (2025:000) om cybersäkerhet och lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare.	*Diarium över incidentrapporter enligt lagen (2025:000) om cybersäkerhet och lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare.*

Bilaga[2]

Verksamheten består i	Särskilda begränsningar i sekretessen
173. *tillsyn och utredning enligt lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare.*	*Gäller ej beslut i ärenden*

[1] Senaste lydelse 2023:637.
[2] Senaste lydelse 2024:77.

Denna förordning träder i kraft den 1 januari 2025 i fråga om lagen (2025:000) om cybersäkerhet och i övrigt den 1 augusti 2025.

1.11 Förslag till förordning om ändring i förordningen (2010:185) med instruktion för Trafikverket

Härigenom föreskrivs i fråga om förordningen (2010:185) med instruktion för Trafikverket att 4 § ska följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

4 §[1]

Trafikverket ska

1. årligen till regeringen redovisa produktiviteten för drift-, underhålls- och byggåtgärder inom det egna ansvarsområdet,

2. årligen följa upp och till regeringen redovisa genomförda åtgärder i den nationella planen för transportinfrastruktur samt i länsplaner för regional transportinfrastruktur i de delar verket ansvarar för genomförandet,

3. årligen bistå Trafikanalys i dess uppgift att till regeringen redovisa en uppföljning av de transportpolitiska målen,

4. årligen till regeringen rapportera kostnad per identifierad avgiftsbelagd passage som nyckeltal för vägavgiftssystem,

5. bistå Trafikanalys när det gäller användningen av databaser och analysverktyg,

6. när det gäller det transeuropeiska transportnätet TEN-T och Fonden för ett sammanlänkat Europa (FSE)

a) ansvara för Sveriges del i förvaltningen av det tekniska informationssystemet för det transeuropeiska transportnätet (TENtec),

b) sprida information om möjligheterna att söka bidrag till projekt,

c) bistå regeringen i beredning, kvalitetssäkring och samordning av bidragsansökningar,

d) följa upp genomförandet av de projekt som har beviljats bidrag, granska projektens års- och slutrapporter samt pröva frågor om att godkänna rapporterna för projekt där Trafikverket inte självt är stödmottagare,

e) bistå regeringen i arbetet gällande de europeiska korridorer som anges i Europaparlamentets och rådets förordning (EU) nr 1315/2013 av den 11 december 2013 om unionens riktlinjer för

[1] Senaste lydelse 2023:46.

utbyggnad av det transeuropeiska transportnätet och om upphävande av beslut nr 661/2010/EU,

7. årligen rapportera hur kraven på försäkringar för ett fartyg och dess drift och utbildningsplatser ombord enligt förordningen (2001:770) om sjöfartsstöd uppfyllts,	7. årligen rapportera hur kraven på försäkringar för ett fartyg och dess drift och utbildningsplatser ombord enligt förordningen (2001:770) om sjöfartsstöd uppfyllts, *och*
8. vartannat år genomföra och till Myndigheten för samhällsskydd och beredskap redovisa ett identifieringsarbete av potentiella europeiska kritiska infrastrukturer inom transportsektorn enligt 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, i den ursprungliga lydelsen, och	
9. i syfte att bedöma behov av underhåll och investeringar i järnvägsnätet samt behov av finansiering av sådana åtgärder upprätta och föra register över de järnvägsanläggningar Trafikverket förvaltar.	*8*. i syfte att bedöma behov av underhåll och investeringar i järnvägsnätet samt behov av finansiering av sådana åtgärder upprätta och föra register över de järnvägsanläggningar Trafikverket förvaltar.

Denna förordning träder i kraft 1 augusti 2025.

1.12 Förslag till förordning om ändring i förordningen (2014:520) med instruktion för Statens energimyndighet

Härigenom föreskrivs i fråga om förordningen (2014:520) med instruktion för Statens energimyndighet att 3 § ska följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
3 §[1]	
Statens energimyndighet ska	
1. ha ett samlat ansvar för information och för att ta fram underlag i enlighet med Europaparlamentets och rådets direktiv (EU) 2018/2001 av den 11 december 2018 om främjande av användningen av energi från förnybara energikällor och göra de beräkningar som medlemsstaterna är skyldiga att göra enligt artiklarna 7 och 23–27 och enligt bilagorna till samma direktiv,	
2. vara behörig myndighet enligt 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,	
3. till Myndigheten för samhällsskydd och beredskap vartannat år redovisa ett identifieringsarbete av potentiella europeiska kritiska infrastrukturer inom undersektorerna olja och gas enligt 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,	
4. vidta åtgärder för att förstärka, utveckla och följa upp insatserna inom ramen för Europaparlamentets och rådets förordning (EU) 2017/1369 av den	*3.* vidta åtgärder för att förstärka, utveckla och följa upp insatserna inom ramen för Europaparlamentets och rådets förordning (EU) 2017/1369 av den

[1] Senaste lydelse 2024:528.

4 juli 2017 om fastställande av en ram för energimärkning och om upphävande av direktiv 2010/30/EU och inom ramen för genomförandet av Europaparlamentets och rådets direktiv 2009/125/EG av den 21 oktober 2009 om upprättande av en ram för att fastställa krav på ekodesign för energirelaterade produkter,

5. fullgöra Sveriges uppgiftsskyldighet enligt kapitel V i avtalet om ett internationellt energiprogram (IEP) som undertecknades i Paris den 18 november 1974 (SÖ 1975:50) och de uppgifter för krisåtgärder som följer av avtalet,

6. fullgöra de uppgifter som följer av rådets direktiv 2009/119/EG av den 14 september 2009 om skyldighet för medlemsstaterna att inneha minimilager av råolja och/eller petroleumprodukter,

7. bevaka att Europaparlamentets och rådets förordning (EG) nr 106/2008 av den 15 januari 2008 om ett gemenskapsprogram för energieffektivitetsmärkning av kontorsutrustning följs,

8. ansvara för genomförandeåtgärder enligt artikel 4.4 i Europaparlamentets och rådets direktiv 2006/32/EG av den 5 april 2006 om effektiv slutanvändning av energi och om

4 juli 2017 om fastställande av en ram för energimärkning och om upphävande av direktiv 2010/30/EU och inom ramen för genomförandet av Europaparlamentets och rådets direktiv 2009/125/EG av den 21 oktober 2009 om upprättande av en ram för att fastställa krav på ekodesign för energirelaterade produkter,

4. fullgöra Sveriges uppgiftsskyldighet enligt kapitel V i avtalet om ett internationellt energiprogram (IEP) som undertecknades i Paris den 18 november 1974 (SÖ 1975:50) och de uppgifter för krisåtgärder som följer av avtalet,

5. fullgöra de uppgifter som följer av rådets direktiv 2009/119/EG av den 14 september 2009 om skyldighet för medlemsstaterna att inneha minimilager av råolja och/eller petroleumprodukter,

6. bevaka att Europaparlamentets och rådets förordning (EG) nr 106/2008 av den 15 januari 2008 om ett gemenskapsprogram för energieffektivitetsmärkning av kontorsutrustning följs,

7. ansvara för genomförandeåtgärder enligt artikel 4.4 i Europaparlamentets och rådets direktiv 2006/32/EG av den 5 april 2006 om effektiv slutanvändning av energi och om

energitjänster och om upphävande av rådets direktiv 93/76/EEG,

9. främja och bevaka utvecklingen på marknaderna för energitjänster och energieffektiva produkter samt uppmärksamma behov av åtgärder för att undanröja hinder som hämmar utvecklingen på dessa marknader i enlighet med vad som anges i artikel 18 i Europaparlamentets och rådets direktiv 2012/27/EU av den 25 oktober 2012 om energieffektivitet, om ändring av direktiven 2009/125/EG och 2010/30/EU och om upphävande av direktiven 2004/8/EG och 2006/32/EG,

10. ansvara för årlig uppföljning av kumulativ energibesparing i enlighet med riktlinjer i regeringens plan för genomförande av artikel 7 i Europaparlamentets och rådets direktiv 2012/27/EU,

11. se till att informationen om tillgängliga energieffektivitetsmekanismer och de finansiella och rättsliga ramarna tydligt redovisas och sprids till alla berörda marknadsaktörer i enlighet med vad som anges i Europaparlamentets och rådets direktiv 2012/27/EU,

12. uppmuntra tillhandahållandet av information till banker och andra finansinstitut om möjligheter att delta i finansieringen av åtgärder för att förbättra energieffektiviteten i enlighet

energitjänster och om upphävande av rådets direktiv 93/76/EEG,

8. främja och bevaka utvecklingen på marknaderna för energitjänster och energieffektiva produkter samt uppmärksamma behov av åtgärder för att undanröja hinder som hämmar utvecklingen på dessa marknader i enlighet med vad som anges i artikel 18 i Europaparlamentets och rådets direktiv 2012/27/EU av den 25 oktober 2012 om energieffektivitet, om ändring av direktiven 2009/125/EG och 2010/30/EU och om upphävande av direktiven 2004/8/EG och 2006/32/EG,

9. ansvara för årlig uppföljning av kumulativ energibesparing i enlighet med riktlinjer i regeringens plan för genomförande av artikel 7 i Europaparlamentets och rådets direktiv 2012/27/EU,

10. se till att informationen om tillgängliga energieffektivitetsmekanismer och de finansiella och rättsliga ramarna tydligt redovisas och sprids till alla berörda marknadsaktörer i enlighet med vad som anges i Europaparlamentets och rådets direktiv 2012/27/EU,

11. uppmuntra tillhandahållandet av information till banker och andra finansinstitut om möjligheter att delta i finansieringen av åtgärder för att förbättra energieffektiviteten i enlighet

med vad som anges i Europaparlamentets och rådets direktiv 2012/27/EU,

13. i enlighet med vad som anges i Europaparlamentets och rådets direktiv 2012/27/EU, tillsammans med berörda aktörer, däribland lokala och regionala myndigheter, främja initiativ för att informera, medvetandegöra och utbilda medborgarna om fördelarna med och de praktiska detaljerna kring åtgärder för att förbättra energieffektiviteten,

14. som tillsynsmyndighet för ursprungsgarantier för el vara medlem i Association of Issuing Bodies (AIB) för Sveriges räkning,

15. vara marknadskontrollmyndighet och utöva marknadskontroll enligt Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011 över att produkter överensstämmer med kraven i

a) Europaparlamentets och rådets förordning (EU) 2017/1369 av den 4 juli 2017 om fastställande av en ram för energimärkning och om upphävande av direktiv 2010/30/EU,

med vad som anges i Europaparlamentets och rådets direktiv 2012/27/EU,

12. i enlighet med vad som anges i Europaparlamentets och rådets direktiv 2012/27/EU, tillsammans med berörda aktörer, däribland lokala och regionala myndigheter, främja initiativ för att informera, medvetandegöra och utbilda medborgarna om fördelarna med och de praktiska detaljerna kring åtgärder för att förbättra energieffektiviteten,

13. som tillsynsmyndighet för ursprungsgarantier för el vara medlem i Association of Issuing Bodies (AIB) för Sveriges räkning,

14. vara marknadskontrollmyndighet och utöva marknadskontroll enligt Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011 över att produkter överensstämmer med kraven i

a) Europaparlamentets och rådets förordning (EU) 2017/1369 av den 4 juli 2017 om fastställande av en ram för energimärkning och om upphävande av direktiv 2010/30/EU,

b) direktiv 92/42/EEG av den 21 maj 1992 om effektivitetskrav för nya värmepannor som eldas med flytande eller gasformigt bränsle, och

c) Europaparlamentets och rådets förordning (EU) 2020/740 av den 25 maj 2020 om märkning av däck med avseende på drivmedelseffektivitet och andra parametrar, om ändring av förordning (EU) 2017/1369 samt om upphävande av förordning (EG) nr 1222/2009,

16. vara behörig myndighet enligt Europaparlamentets och rådets förordning (EU) 2019/941 av den 5 juni 2019 om riskberedskap inom elsektorn och om upphävande av direktiv 2005/89/EG,

17. vid tillämpningen av förordning (EU) 2019/941

a) särskilt samverka med Affärsverket svenska kraftnät i syfte att säkerställa att riskberedskapsplaner utarbetas effektivt och genomförs korrekt samt att underlätta förebyggande och utvärdering av elkriser och informationsutbyte om sådana, och

b) beakta de underlag som Affärsverket svenska kraftnät tar fram enligt förordningen,

18. vara nationellt centrum för frågor om infångning och lagring av koldioxid,

b) direktiv 92/42/EEG av den 21 maj 1992 om effektivitetskrav för nya värmepannor som eldas med flytande eller gasformigt bränsle, och

c) Europaparlamentets och rådets förordning (EU) 2020/740 av den 25 maj 2020 om märkning av däck med avseende på drivmedelseffektivitet och andra parametrar, om ändring av förordning (EU) 2017/1369 samt om upphävande av förordning (EG) nr 1222/2009,

15. vara behörig myndighet enligt Europaparlamentets och rådets förordning (EU) 2019/941 av den 5 juni 2019 om riskberedskap inom elsektorn och om upphävande av direktiv 2005/89/EG,

16. vid tillämpningen av förordning (EU) 2019/941

a) särskilt samverka med Affärsverket svenska kraftnät i syfte att säkerställa att riskberedskapsplaner utarbetas effektivt och genomförs korrekt samt att underlätta förebyggande och utvärdering av elkriser och informationsutbyte om sådana, och

b) beakta de underlag som Affärsverket svenska kraftnät tar fram enligt förordningen,

17. vara nationellt centrum för frågor om infångning och lagring av koldioxid,

19. fullgöra de åtaganden som följer av Sveriges deltagande i de projektbaserade mekanismerna i Kyotoprotokollet till Förenta nationernas ramkonvention om klimatförändringar, i enlighet med de modaliteter och procedurer som specificeras i beslut 3/CMP.1 av partskonferensen till Kyotoprotokollet, och

20. vara behörig myndighet enligt kommissionens delegerade förordning (EU) 2024/1366 av den 11 mars 2024 om komplettering av Europaparlamentets och rådets förordning (EU) 2019/943 genom inrättandet av en nätföreskrift om sektorsspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden.

18. fullgöra de åtaganden som följer av Sveriges deltagande i de projektbaserade mekanismerna i Kyotoprotokollet till Förenta nationernas ramkonvention om klimatförändringar, i enlighet med de modaliteter och procedurer som specificeras i beslut 3/CMP.1 av partskonferensen till Kyotoprotokollet, och

19. vara behörig myndighet enligt kommissionens delegerade förordning (EU) 2024/1366 av den 11 mars 2024 om komplettering av Europaparlamentets och rådets förordning (EU) 2019/943 genom inrättandet av en nätföreskrift om sektorsspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden.

Bestämmelser om en marknadskontrollmyndighets befogenhet att besluta om åtgärder enligt förordning (EU) 2019/1020 finns i lagen (2018:550) med kompletterande bestämmelser till EU:s energimärkningsförordning, plan- och bygglagen (2010:900) respektive lagen (2018:551) med kompletterande bestämmelser till EU:s däckmärkningsförordning.

Denna förordning träder i kraft den 1 augusti 2025.

2 Utredningens uppdrag och arbete

I detta kapitel ska utredningens uppdrag och arbete beskrivas. Under 2.1 analyseras uppdraget, i 2.2 redovisas arbetet och 2.3 beskriver betänkandets disposition.

2.1 Analys av regeringens direktiv

2.1.1 Bakgrund

Europaparlamentet och rådet antog den 14 december 2022 två nya EU-direktiv: NIS2-direktivet[1] och CER-direktivet.[2] Regeringen beslutade i februari 2023 att utredningen skulle föreslå de anpassningar av svensk rätt som är nödvändiga för att genomföra de två direktiven. Utredningstiden bestämdes till ett år, se bilaga 1. Genom tilläggsdirektiv i januari 2024 bestämde regeringen att utredningstiden låg fast för de delar av uppdraget som avsåg att föreslå hur NIS2-direktivet skulle införlivas och utredningen överlämnade i mars 2024 delbetänkandet ”Nya regler om cybersäkerhet”.[3] I tilläggsdirektivet förlängde regeringen vidare tiden för den delen av uppdraget som avsåg CER-direktivet samt några andra frågor. Det uppdraget skulle slutredovisas den 16 september 2024, se bilaga 2.

I detta slutbetänkande analyseras CER-direktivet och utredningen lämnar förslag på hur det ska införlivas i svensk rätt. Direktivet finns

[1] 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).
[2] 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.
[3] SOU 2024:18.

i bilaga 3. Det som vidare återstår för utredningen är enligt regeringens tilläggsdirektiv

1. gemensamma frågor för NIS2- och CER-direktiven i den mån dessa är hänförliga till genomförandet av CER-direktivet eller i övrigt syftar till att uppnå en sammanhängande reglering,
2. 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
3. ta ställning till om bestämmelserna i offentlighets- och sekretesslagen (2009:400), OSL, innebär ett tillräckligt skydd för sådana uppgifter som kan komma att behandlas enligt direktiven.

2.1.2 Utredningens övergripande utgångspunkter

Utredningen hade i sitt delbetänkande några övergripande utgångspunkter som även kommer att gälla för detta betänkande.

Båda EU-direktiven är så kallade minimidirektiv, varför medlemsstaterna får anta mer långtgående bestämmelser. Det betyder att utredningen skulle kunna lämna förslag om att exempelvis fler sektorer än vad som följer av direktiven skulle kunna omfattas av en reglering. Utgångspunkten enligt regeringen ska dock vara att förslagen utformas så att regelbördan och administrationen minimeras för berörda verksamhetsutövare. Om utredningen lämnar mer långtgående förslag ska utredningen motivera varför det är nödvändigt och göra en analys om förslagen är samhällsekonomiskt effektiva och hur svenska företags konkurrenskraft skulle påverkas. En slutsats bör vara att tidsramen för uppdraget i hög grad utgör hinder för sådana förslag. Detsamma bör gälla för utredningens möjlighet enligt regeringens direktiv att ta sig an närliggande frågor.

Den andra utgångspunkten som även kommer att gälla för CER är att direktivet inte ska införlivas direktivnära utan att förslagen ska utformas utifrån den systematik och terminologi som används i svensk rätt. Det betyder att ett normalt språkbruk ska eftersträvas. En följd blir att utredningen även i den lag som ska införliva kraven

i CER-direktivet kommer att exempelvis ersätta begreppet entitet med verksamhetsutövare.

Vidare kommer CER-direktivets krav på motsvarande sätt som NIS2-direktivet att regleras i en särskild lag med tillhörande förordning. Därutöver kommer att krävas följdändringar med anledning av att direktiv 2008/114/EG upphävs.

2.1.3 CER-direktivet

CER-direktivet ställer krav på motståndskraft i samhällsviktiga tjänster. Enligt CER-direktivet ska medlemsstaterna identifiera verksamhetsutövare som erbjuder samhällsviktiga tjänster inom sektorerna energi, transport, bankverksamhet, finansmarknadsstruktur, hälso- och sjukvård, dricksvatten, avloppsvatten, digital infrastruktur, offentlig förvaltning, rymden samt produktion, bearbetning och distribution av livsmedel. De utpekade sektorerna i CER-direktivet pekas även ut av NIS2-direktivet, men NIS2 innehåller även områden som inte återfinns i CER-direktivet som till exempel post- och budtjänster, avfallshantering och forskning. För de utpekade verksamhetsutövarna ska det gälla särskilda skyldigheter. De ska vidta åtgärder för att stärka sin motståndskraft och rapportera incidenter. CER-direktivet innehåller också bestämmelser om tillsyn och sanktioner och en ram för samarbete mellan medlemsstaterna. En slutsats är att CER-direktivets krav påminner om det första NIS-direktivet som genomfördes genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, NIS-lagen. Som följer av den lagens första paragraf omfattar den lagen samhällsviktiga tjänster inom sektorerna energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten, digital infrastruktur och digitala tjänster.

Medlemsländerna ska senast den 17 oktober 2024 anta de nationella bestämmelser som krävs för att följa direktiven.

Identifiering av kritiska verksamhetsutövare

Medlemsländerna är skyldiga att identifiera de kritiska verksamhetsutövarna inom de utpekade sektorerna samt att upprätta en förteckning. Flera kriterier ska vara uppfyllda för att identifiering ska kunna ske. Verksamhetsutövaren ska tillhandahålla en eller flera samhällsviktiga tjänster och ha sin kritiska infrastruktur belägen i medlemsstaten. Vidare skulle en incident medföra betydande störande effekt. Verksamhetsutövare som tillhandahåller samma eller liknande samhällsviktiga tjänster i minst sex medlemsstater har särskild europeisk betydelse och ska omfattas av särskilda bestämmelser.

Det anförda betyder att utredningen behöver klarlägga hur regler för att peka ut samhällsviktiga tjänster ska utformas. Kommissionen har visserligen i en delegerad akt fastställt en icke uttömmande förteckning över tjänster som ska anses samhällsviktiga,[4] men enligt regeringen kan det inte uteslutas att det kan finnas behov av andra samhällsviktiga tjänster i en nationell reglering. Vidare behöver analyseras hur direktivets kriterier för vad som utgör en betydande störande effekt ska tillämpas nationellt. Enligt regeringens direktiv skulle det kunna vara lämpligt att överväga en motsvarande lösning som enligt nuvarande NIS-reglering. Den innebär att MSB, efter att tillsynsmyndigheterna och Socialstyrelsen getts tillfälle att yttra sig, får meddela föreskrifter om vilka tjänster som är samhällsviktiga och vad som avses med betydande störning. Utredningen behöver även överväga vem som ansvarar för identifieringen, hur förfarandet ska gå till, hur en förteckning kan upprättas och uppdateras och om det krävs särskilda nationella bestämmelser om identifiering och anmälan av kritiska verksamhetsutövare.

Krav på kritiska verksamhetsutövare

Kritiska verksamhetsutövare ska enligt direktivet utföra en riskbedömning och vidta lämpliga och proportionella åtgärder för att säkerställa sin motståndskraft. Åtgärderna ska grundas på riskbedömning av verksamhetsutövaren och medlemsstaten. Direktivet uppställer också vissa minimikrav, som kommer att kompletteras med icke-

[4] Kommissionens delegerade förordning (EU) 2623/2450 av den 25 juli 2023 om komplettering av Europaparlamentets och rådets direktiv (EU) 2022/2557 genom upprättande av en förteckning över samhällsviktiga tjänster.

bindande riktlinjer och tekniska specifikationer. Utredningen ska mot denna bakgrund analysera hur reglerna om riskbedömning ska utformas och kunna kompletteras vid behov. Det ingår att analysera hur krav om riskbedömning förhåller till annan lagstiftning om liknande krav.

Vidare ska kritiska verksamhetsutövare rapportera incidenter som medför eller skulle kunna medföra en betydande störning för samhällsviktiga tjänster. Utredningen behöver analysera hur bedömningen ska gå till och till vilken myndighet rapportering ska ske.

Bakgrundskontroller

I Sverige gäller lagen (1998:620) om belastningsregister. Det förs av Polismyndigheten som är personuppgiftsansvarig. Enligt lagen ska uppgifter ur belastningsregistret lämnas ut om det begärs av särskilt utpekade svenska myndigheter som till exempel en åklagarmyndighet för visst syfte. Därutöver får även en myndighet i övrigt, i den utsträckning regeringen för vissa slag av ärenden föreskriver det eller för ett särskilt fall ger tillstånd till det, begära ut uppgifter. Den enskilde får också begära uppgifter om sig själv. Även utländska organ kan begära ut uppgifter. Slutligen finns det vissa särregler för till exempel Advokatsamfundet och enskilda kan i vissa särskilda fall begära uppgifter om andra enskilda.

Kritiska verksamhetsutövare ska enligt direktivet kunna ansöka om bakgrundskontroller för personer som har en känslig roll i verksamheten. En sådan kontroll ska bekräfta identiteten och även innefatta uppgifter från belastningsregistret.

Utredningen behöver föreslå ett system för bakgrundskontroller. Det ska bygga på att kritiska verksamhetsutövare på ett effektivt sätt ska få kännedom om brott, men samtidigt ska integritetsintrånget för den enskilde inte vara större än nödvändigt. Enligt regeringen ska systemet inte bygga på verksamhetsutövaren själv kan begära ut uppgifterna. Med verksamhetsutövare avses enligt utredningens bedömning en nuvarande eller framtida arbetsgivaren, som kan vara en offentlig eller enskild verksamhetsutövare. Det betyder att verksamhetsutövaren kan vara exempelvis en myndighet, men även ett företag.

Myndigheternas ansvarsfördelning

Även enligt detta direktiv ska en gemensam kontaktpunkt för samarbetet med andra myndigheter utses. Vidare ska det finnas en eller flera myndigheter som ska ansvara för direktivets tillämpning på nationell nivå.

Det finns ett krav på samstämmighet mellan de två direktiven. Det anges att verksamhetsutövare som har identifierats som kritiska enligt CER-direktivet även ska anses vara väsentliga enligt NIS2-direktivet och att myndigheterna som ansvar för tillämpningen av respektive direktiv ska utbyta information om hot, incidenter och åtgärder.

Mot den angivna bakgrunden anger regeringen att samma myndighet bör utöva tillsyn över såväl verksamheter enligt NIS2-direktivet som CER-direktivet. MSB är redan nationell kontaktpunkt för det arbete som bedrivs inom ramen för direktiv 2008/114/EG,[5] som alltså ersätts av CER-direktivet. Enligt regeringen bör därför MSB utses till nationell kontaktpunkt även för CER-direktivet. MSB bör även ha en samordnande roll för tillsynsmyndigheterna enligt CER-direktivet på sätt som den redan har för tillsynsmyndigheterna enligt NIS-regelverket. MSB bör också få del av relevant information från tillsynsmyndigheterna och ha en samordnande roll om riskbedömningen. Utredningen ska därför föreslå ett system för tillsyn för CER-direktivet, som är samordnat med NIS2-direktivet. Det betyder att föreslå vilka myndigheter som ska vara tillsynsmyndigheter och föreslå hur MSB:s roll som gemensam nationell kontaktpunkt utformas. I denna del är det självklart att de överväganden om myndighetsstruktur som gjordes för NIS2-direktivet kommer att vara utredningens utgångspunkt.

Myndigheternas befogenheter

Myndigheterna ska ha rätt att utföra inspektioner av kritisk infrastruktur och riskhanteringsåtgärder, ha rätt att besluta om säkerhetsrevision samt kunna kräva information och rättelse. Medlemsstaterna ska anta regler om effektiva, proportionella och avskräckande sanktioner.

[5] 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.

Medlemsstaterna har större valfrihet avseende utformningen av myndigheternas verktyg för CER-direktivet jämfört med NIS2-direktivet. Samtidigt är utgångspunkten att tillsynen enligt båda direktiven ska kunna utövas på ett samordnat och effektivt sätt. Vidare ska ingripanden och sanktionerna enligt direktiven framstå som proportionerliga i förhållande till varandra och vara förutsebara.

2.1.4 Gemensamma frågor för NIS2 och CER

Som framgår ovan under 2.1.1 återstår det för utredningen att klarlägga om det finns gemensamma frågor för NIS2- och CER-direktiven. Det ska noteras att det ska vara frågor som är hänförliga till genomförandet av CER-direktivet eller i övrigt syftar till att uppnå en sammanhängande reglering. Ett exempel som utredningen identifierade vid arbetet med delbetänkandet är som även framgår ovan att det av artiklarna 2.3 och 3.1 f i NIS2-direktivet följer att alla verksamhetsutövare som är kritiska enligt CER-direktivet också är väsentliga enligt NIS2-direktivet. Det ska dock beaktas att utredningen saknar mandat för att genomföra justeringar av tidigare slutsatser om NIS2-direktivet, eftersom det arbetet är avslutat och ett delbetänkande har överlämnats.

2.1.5 Anpassning av säkerhetsskyddslagen

Vidare återstår det för utredningen enligt regeringens tilläggsdirektiv att analysera hur den nya regleringen ska fungera vid sidan om säkerhetsskyddsregleringen och föreslå ändringar som behövs för att uppnå en mer sammanhållen systematik mellan regelverken, särskilt vad gäller tillsynsmyndigheternas befogenheter och sanktioner. Här ska noteras att utredningen redan i delbetänkandet har genomfört en omfattande analys om hur säkerhetsskyddsregleringen ska förhålla sig till cybersäkerhetsregleringen. Utredningen har därför redan klarlagt i vilken utsträckning cybersäkerhetslagen ska vara tillämplig för verksamheter som redan omfattas av säkerhetsskyddslagen (2018:585). Slutsatsen blev att myndigheter som bedriver säkerhetskänslig verksamhet till övervägande del undantas från cybersäkerhetsregleringen. Motsvarande ska gälla för enskilda verksamhetsutövare som enbart bedriver säkerhetskänslig verksamhet. För övriga

offentliga och enskilda verksamhetsutövare som bedriver säkerhetskänslig verksamhet gäller för den säkerhetskänsliga delen enbart kraven om anmälningsskyldighet i cybersäkerhetslagen, medan lagen i dess helhet gäller för den övriga verksamheten.

Utredningen kommer att på samma sätt analysera förhållandet mellan CER-direktivet och säkerhetsskyddsregleringen i detta slutbetänkande.

Därutöver är det dock en kvarstående uppgift för utredningen att anpassa säkerhetsskyddsregleringens bestämmelser om tillsynsbefogenheter och sanktioner efter NIS2-direktivets och CER-direktivets tillsynsbefogenheter och sanktioner. Skälet är att det inte skulle vara önskvärt om säkerhetsskyddsregleringen innehöll mindre ingripande befogenheter och sanktioner än regleringen avseende NIS2-direktivet och CER-direktivet.

2.1.6 Sekretess och dataskydd

Slutligen är också en återstående uppgift för utredningen att ta ställning till om bestämmelserna i offentlighets- och sekretesslagen (2009:400), OSL, innebär ett tillräckligt skydd för sådana uppgifter som kan komma att behandlas enligt direktiven. Såväl NIS2-direktivet som CER-direktivet kräver att verksamhetsutövaren lämnar uppgifter. Direktiven ställer krav på konfidentialitet. Det behöver därför klargöras om de nationella reglerna om sekretess i OSL är tillräckliga. Den frågan lyftes redan av remissinstanserna vid beredningen av NIS-lagen. Regeringen bedömde då att sekretesskyddet var tillräckligt, men frågan behöver på nytt analyseras med hänsyn särskilt till CER-direktivets bestämmelser.

Vidare behöver utredningen analysera vilken personuppgiftsbehandling direktiven ger upphov till och kan särskilt behöva göra överväganden om sekretess och dataskydd avseende utformning av system för bakgrundskontroller.

2.1.7 Konsekvensanalys

En viktig uppgift för utredningen är att göra en konsekvensanalys för förslagen. Det handlar särskilt om ekonomiska konsekvenser för de myndigheter som utredningen föreslår uppgifter för. Vidare kom-

mer offentliga som enskilda verksamhetsutövares kostnader att kunna öka till följd av att nya skyldigheter åläggs dem. Även påverkan på den kommunala självstyrelsen ska analyseras.

Kostnadsökningar för det allmänna ska utredningen föreslå en finansiering för.

Utredningens gav i delbetänkandet Sweco Aktiebolag (Sweco) i uppdrag att ge in ett underlag för att utredningen ska kunna bedöma de ekonomiska konsekvenserna för de myndigheter som kommer att få uppgifter enligt den nya regleringen om NIS2. Som framgår av delbetänkandet hade dock ett flertal av myndigheterna svårigheter att inom den begränsade utredningstiden kunna bedöma sina kostnader för uppgifterna enligt cybersäkerhetsregleringen, varför Swecos underlag inte kunde läggas till grund för någon bedömning i delbetänkandet.

Tiden för att införliva CER-direktivet är än mer begränsat och uppgår till drygt sex månader. Detta talar emot att använda samma metod. Det ska vidare noteras att skillnaden mellan NIS2- och CER-direktiven har bäring på hur konsekvensanalysen ska utformas. För att omfattas av NIS2-direktivet är det tillräckligt att verksamhetsutövaren omfattas av en utpekad sektor i bilagor till direktivet. Det betydde att det tillsynsmyndigheterna behövde göra för att uppskatta sina kostnader för tillsyn enligt NIS2- direktivet var att beräkna antalet verksamhetsutövare som skulle omfattas inom respektive sektor. Som kommer att framgå närmare av kapitel 6 är förutsättningarna för att omfattas av CER mer långtgående. Det krävs dels att verksamhetsutövaren ingår i en utpekad sektor som anges i bilagan till CER-direktivet, dels att verksamhetsutövaren identifierats som kritisk. Det betyder att det är en tvåstegsprocess som kommer att bli tidskrävande. Enligt artikel 6.1 i CER-direktivet ska också medlemsstaterna först den 17 juli 2026 ha identifierat de kritiska verksamhetsutövarna. Det betyder att kostnaderna för tillsyn enligt CER-direktivet aktualiseras först 2027.

2.2 Utredningens uppdrag och arbete

Utredningens arbete har bedrivits på sedvanligt sätt med regelbundna möten med sakkunniga och experter samt med deltagarna i en till utredningen knuten referensgrupp. Utredningen har haft tre

protokollförda möten med expert- och sakkunniggruppen och två med referensgruppen.

Utredningen har också träffat Läkemedelsverket, MSB och Polismyndigheten.

Utredningen har löpande hållit Regeringskansliet informerat om arbetet.

Utredningen har därutöver samverkat med bland annat *Uppdrag att förbättra bakgrundskontroller i kommunerna* (Ju 2024:A). Utredningen har informerat utredningen *Samordning för nationell digital infrastruktur i hälso- och sjukvården* (S 2023:14) om uppdraget.

2.3 Betänkandets disposition

Betänkandet inleds i kapitel 3 med en övergripande beskrivning av CER-direktivet. I kapitel 4 redogörs för sektorerna som följer enligt CER-direktivet och skillnader gentemot motsvarigheterna enligt NIS2-direktivet. Av kapitel 5 följer den föreslagna lagens tillämpningsområde. I kapitel 6 behandlas systemet för identifiering av kritiska verksamhetsutövare och de förteckningar som ska föras. Därefter följer i kapitel 7 en redogörelse för bestämmelserna kring kritiska verksamhetsutövare av särskild europeisk betydelse. I kapitel 8 redogörs för de kritiska verksamhetsutövarnas riskbedömning, åtgärder för motståndskraft och incidentrapportering. I kapitel 9 behandlas bakgrundskontroller. I kapitel 10 och 11 behandlas tillsyn respektive ingripanden och sanktioner. Kapitel 12 behandlar gemensam kontaktpunkt i Sverige och dess uppgifter. I kapitel 13 redogörs för bestämmelser om sekretess kopplat till NIS2- och CER-direktiven. Kapitel 14 innehåller föreslag till ändringar av säkerhetsskyddsregleringen. I kapitel 15 återfinns konsekvensanalysen. Kapitel 16 behandlar frågor kopplade till ikraftträdande. Avslutningsvis återfinns författningskommentaren i kapitel 17.

Det finns därutöver fyra bilagor till betänkandet. Kommittédirektivet återfinns i bilaga 1. Utredningens tilläggsdirektiv finns i bilaga 2. I bilaga 3 finns CER-direktivet. Bilaga 4 innehåller en parallelluppställning över direktivets artiklar och de bestämmelser i utredningens författningsförslag som genomför dem.

3 CER-direktivet

3.1 Direktiv 2008/114/EG

I detta avsnitt beskrivs det europeiska arbetet med skydd av kritisk infrastruktur till följd av bland annat 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. Enligt artikel 27 i CER-direktivet upphävs direktivet och upphör gälla med verkan från och med den 18 oktober 2024. Det finns dock anledning att översiktligt beskriva innehållet och hur arbetet med direktivet har bedrivits i Sverige fram till nu.

Historiskt 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. Terroristhotet är en högt prioriterad fråga, men arbetet ska omfatta alla slags hot och risker. En av de viktigaste delarna i programmet är direktiv 2008/114/EG.

Med kritisk infrastruktur avses (artikel 2 a) 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 europeisk kritisk infrastruktur avses (artikel 2 b) i medlemsstaterna belägen kritisk infrastruktur vars driftsstörning eller förstörelse skulle få betydande konsekvenser för minst två medlemsstater. Konsekvensernas omfattning ska bedömas utifrån sektorsövergripande kriterier. Detta inbegriper verkningar till följd av tvärsektoriella beroenden av andra typer av infrastruktur.

Direktivet omfattar energi- och transportsektorerna (artikel 3), och går huvudsakligen ut på att EU:s medlemsstater ska identifiera och utse europeisk kritisk infrastruktur, ECI.

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 MSB. Den nationella kontaktpunkten, MSB, ska samordna frågor kring skydd av kritisk infrastruktur i Sverige med andra medlemsstater och med EU-kommissionen.

Europaparlamentet och Europeiska rådet antog den 14 december 2022 CER-direktivet. Direktivet ska vara genomfört i svensk rätt den 17 oktober 2024. Genom artikel 27 upphävs direktiv 2008/114/EG.

I kapitel 16 redogörs för de författningsändringar som krävs i och med att direktiv 2008/114/EG upphör att gälla.

3.2 Bakgrund och syfte

I CER-direktivet konstateras att kritiska verksamhetsutövare spelar en avgörande roll för att upprätthålla viktiga samhällsfunktioner eller central ekonomisk verksamhet på den inre marknaden. Det är därför enligt direktivet viktigt att det på unionsnivå skapas en reglering som syftar till att stärka kritiska verksamhetsutövares motståndskraft genom att fastställa harmoniserade minimiregler. I CER-direktivet anges även att det är viktigt att bistå verksamhetsutövarna genom enhetligt stöd och tillsynsåtgärder. Vid utvärderingen av rådets direktiv 2008/114/EG[1] konstaterades att säkerhetsåtgärderna i det direktivet inte är tillräckliga för att förhindra alla störningar som kan uppstå. Det är därför nödvändigt att säkerställa att risker redovisas bättre, att skapa enhetlighet i rollen och uppgifterna för kritiska verksamhetsutövare och att det antas unionsregler för att stärka kritiska verksamhetsutövares motståndskraft. Kritiska verksamhetsutövare bör kunna öka sin förmåga att förebygga, skydda sig mot, reagera på, stå emot, begränsa, absorbera, anpassa sig till och återhämta sig från incidenter som kan störa tillhandahållandet av samhällsviktiga tjänster. Vidare anges i direktivet att kritiska verk-

[1] 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.

samhetsutövare behöver rustas bättre eftersom det finns en dynamisk hotbild och ett ökande ömsesidigt beroende mellan infrastruktur och de olika sektorerna. Direktivet syftar till att åstadkomma en solid harmoniseringsnivå för sektorer och kategorier av verksamhetsutövare som omfattas av tillämpningsområdet. Direktivet inrättar en övergripande ram för att hantera kritiska verksamhetsutövares motståndskraft med hänsyn till alla faror, oberoende av om det är naturliga faror eller orsakade av människan, olyckshändelser eller avsiktligt framkallade faror (skäl 1–4).

3.3 Riskbedömning av medlemsstaterna

Kommissionen ges i direktivet befogenhet att anta en delegerad akt senast den 17 november 2023 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.[2] De behöriga myndigheterna ska använda förteckningen för att göra en riskbedömning senast den 17 januari 2026 (medlemsstaternas riskbedömning). 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.

Inom tre månader från att riskbedömningen har gjorts ska medlemsstaten förse kommissionen med relevant information om de typer av risker som har identifierats och resultatet av riskbedömningen per sektor och undersektor (artikel 5).

3.4 Identifiering av kritiska verksamhetsutövare

Senast den 17 juli 2026 ska medlemsstaterna identifiera de kritiska verksamhetsutövarna för de sektorer och undersektorer som anges i direktivets bilaga. Bilagan innehåller följande 11 sektorer:

[2] 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.

- 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.

När en medlemsstat identifierar kritiska verksamhetsutövare ska den ta hänsyn till resultatet av sin riskbedömning samt den strategi för att stärka kritiska verksamhetsutövares motståndskraft som ska antas enligt artikel 4.

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 i eller till medlemsstaten, för det andra ska verksamhetsutövaren ha sin kritiska infrastruktur belägen där, för det tredje att en incident skulle få betydande störande effekter för tillhandahållandet av en eller flera samhällsviktiga tjänster. Samhällsviktig tjänst definieras i artikel 2.5 i direktivet som en tjänst som är avgörande för att upprätthålla viktiga samhällsfunktioner, ekonomisk verksamhet, folkhälsa och allmän säkerhet, eller miljön.

När en medlemsstat fastställer om en störande effekt är betydande ska den beakta följande kriterier:

- Antalet användare som är beroende av den samhällsviktiga tjänsten.
- Hur beroende andra sektorer som omfattas av direktivet är av den samhällsviktiga tjänsten.

- Vilken effekt incidenter kan få för ekonomisk och samhällelig verksamhet, miljön, den allmänna säkerheten och tryggheten eller befolkningens hälsa.
- Verksamhetsutövarens marknadsandel.
- Det geografiska område som skulle kunna påverkas av en incident.
- Verksamhetsutövarens betydelse för upprätthållandet av en tillräcklig nivå på den samhällsviktiga tjänsten.

Varje medlemsstat ska upprätta en förteckning över de kritiska verksamhetsutövare som har identifierats och säkerställa att dessa underrättas om att de har identifierats som kritiska inom en månad från identifieringen. Medlemsstaterna ska också informera verksamhetsutövarna 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 utan onödigt dröjsmål lämna följande information till kommissionen:

- En förteckning över samhällsviktiga tjänster i den medlemsstaten.
- Det antal kritiska verksamhetsutövare som har identifierats för varje sektor och undersektor, och för varje samhällsviktig tjänst.
- Eventuella tröskelvärden som har tillämpats för att fastställa om en störande effekt är betydande.

Därefter ska medlemsstaterna lämna informationen när det är nödvändigt men minst vart fjärde år (artikel 6–7).

3.5 Behöriga myndigheter och gemensam kontaktpunkt

Varje medlemsstat ska utse eller inrätta en eller flera behöriga myndigheter som är ansvariga för tillämpningen och efterlevnadskontrollen av direktivet. Därutöver ska varje medlemsstat också utse en gemensam kontaktpunkt. Den gemensamma kontaktpunkten ska utöva en sambandsfunktion som säkerställer gränsöverskridande samarbete med de gemensamma kontaktpunkterna i andra medlems-

stater och den grupp för kritiska verksamhetsutövares motståndskraft som inrättas genom direktivet. En medlemsstat får föreskriva att den gemensamma kontaktpunkten även ska ha en sambandsfunktion med kommissionen och säkerställa samarbete med tredjeländer. Varje medlemsstat ska säkerställa att dess behöriga myndigheter och gemensamma kontaktpunkt samråder och samarbetar med andra relevanta myndigheter när så är lämpligt (artikel 9).

3.6 Riskbedömning av kritiska verksamhetsutövare

Medlemsstaterna ska säkerställa att kritiska verksamhetsutövare gör en riskbedömning inom nio månader från mottagandet av underrättelsen om att de har identifierats som kritiska. Riskbedömningen ska göras på grundval av medlemsstaternas riskbedömningar och andra informationskällor, för att bedöma alla relevanta risker som kan störa tillhandahållandet av deras samhällsviktiga tjänster. Riskbedömningen 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 (artikel 12).

3.7 Kritiska verksamhetsutövares åtgärder för motståndskraft

Medlemsstaterna ska säkerställa att kritiska verksamhetsutövare vidtar lämpliga och proportionella tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa sin motståndskraft. Dessa ska inbegripa åtgärder som är nödvändiga för att

a) förhindra incidenter från att uppstå, med vederbörlig hänsyn till åtgärder för katastrofriskreducering och klimatanpassning,

b) säkerställa ett tillfredställande 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, och

f) öka medvetenheten om de åtgärder som anges i a-e hos berörd personal, med vederbörlig hänsyn till utbildningskurser, informationsmaterial och övningar.

Medlemsstaterna ska säkerställa att kritiska verksamhetsutövare har och tillämpar en plan för motståndskraft eller ett eller flera likvärdiga dokument med en beskrivning av de åtgärder som vidtagits enligt ovan. Medlemsstaterna ska också säkerställa att kritiska verksamhetsutövare utser en sambandsansvarig eller motsvarande som kontaktpunkt med de berörda myndigheterna (artikel 13).

3.8 Bakgrundskontroller

Medlemsstaterna ska ange de villkor enligt vilka en kritisk verksamhetsutövare får ansöka om bakgrundskontroller av personer som

a) innehar känsliga roller i eller till förmån för den känsliga verksamhetsutövaren, särskilt när det gäller den kritiska verksamhetsutövarens motståndskraft,

b) har bemyndigats att direkt eller på distans få tillgång till den kritiska verksamhetsutövarens lokaler eller dess informations- eller kontrollsystem,

c) övervägs för rekrytering till tjänster som omfattas av de kriterier som anges i a eller b.

Ansökningarna ska bedömas inom rimlig tid och hanteras i enlighet med nationell rätt och nationella förfaranden samt relevant och tillämplig unionsrätt. 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 kritiska verksamhetsutövaren.

En bakgrundkontroll ska åtminstone bekräfta identiteten på den person som är föremål för kontrollen samt kontrollera uppgifter ur kriminalregistret avseende brott som är relevanta för en viss tjänst (artikel 14).

3.9 Incidentanmälan

Medlemsstaterna ska säkerställa att kritiska verksamhetsutövare 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. Om det inte är operativt omöjligt ska en första anmälan lämnas inom 24 timmar efter det att verksamhetsutövaren fått kännedom om incidenten. En detaljerad rapport ska lämnas senast en månad därefter.

För att fastställa om störningen är betydande ska i synnerhet följande tas i beaktande:

a) antal användare som berörs av störningen,

b) störningens varaktighet, och

c) det geografiska område som påverkas av störningen, med beaktande av om 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 incidenten anmälas till kommissionen.

En incidentanmälan ska omfatta all tillgänglig information som är nödvändig för att den behöriga myndigheten ska förstå incidentens art, orsak och möjliga konsekvenser.

Den gemensamma kontaktpunkten ska informera dess motsvarigheter i andra medlemsstater som påverkas om incidenten har eller kan ha en betydande påverkan på kritiska verksamhetsutövare 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 verksamhetsutövaren relevant uppföljningsinformation, inklusive information som skulle kunna hjälpa verksamhetsutövaren att reagera ändamålsenligt på incidenten. Medlemsstaterna ska informera allmänheten om de anser att det skulle ligga i allmänhetens intresse (artikel 15).

3.10 Kritiska verksamhetsutövare av särskild europeisk betydelse

En kritisk verksamhetsutövare ska betraktas som en kritisk verksamhetsutövare 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. Medlemsstaterna ska säkerställa att en kritisk verksamhetsutövare informerar sin behöriga myndighet om den tillhandahåller samhällsviktiga tjänster till så många medlemsstater. Medlemsstaterna ska utan onödigt dröjsmål underrätta kommissionen om identiteten på dessa kritiska verksamhetsutövare. Kommissionen ska då samråda med behöriga myndigheter i de berörda medlemsstaterna och den kritiska verksamhetsutövaren i fråga. Om kommissionen på grundval av samråden fastställer att den berörda verksamhetsutövaren tillhandahåller samhällsviktiga tjänster till eller i fler än sex medlemsstater ska kommissionen, via den behöriga myndigheten, underrätta den berörda verksamhetsutövaren om att den betraktas som en kritisk verksamhetsutövare av särskild europeisk betydelse och informera om dess skyldigheter enligt direktivet (artikel 17).

3.11 Rådgivande uppdrag

På begäran av en medlemsstat som identifierat en kritisk verksamhetsutövare av särskild europeisk betydelse ska kommissionen anordna ett så kallat rådgivande uppdrag för att bedöma de åtgärder som den kritiska verksamhetsutövaren infört för att uppfylla sina skyldigheter enligt direktivet. Kommissionen får också anordna ett rådgivande uppdrag på eget initiativ eller på begäran av en eller flera medlemsstater till eller i vilka den samhällsviktiga tjänsten tillhandahålls. Detta under förutsättning att den medlemsstat som har identifierat verksamhetsutövaren samtycker till detta. Ett rådgivande uppdrag ska bestå av experter från den medlemsstat där den kritiska verksamhetsutövaren av särskild europeisk betydelse är belägen, experter från de medlemsstater till eller i vilka den samhällsviktiga tjänsten tillhandahålls och företrädare för kommissionen. Kommissionen ska anta en genomförandeakt om regler och förfaranden för rådgivande uppdrag. Medlemsstaterna ska säkerställa att kritiska verksamhetsutövare av särskild europeisk betydelse ger det rådgivande uppdraget åtkomst till uppgifter, system och anläggningar som rör tillhandahållandet av deras samhällsviktiga tjänster (artikel 18).

3.12 Gruppen för kritiska verksamhetsutövares motståndskraft

Genom CER-direktivet inrättas en grupp för kritiska verksamhetsutövares motståndskraft. Gruppen ska ge kommissionen stöd samt underlätta samarbete och informationsutbyte mellan medlemsstaterna i frågor som rör direktivet. Gruppen består av företrädare för medlemsstaterna och kommissionen. Kommissionens företrädare är ordförande i gruppen (artikel 19).

3.13 Tillsyn, efterlevnadskontroll och sanktioner

För att bedöma om de verksamhetsutövare som har identifierats enligt direktivet fullgör de skyldigheter som fastställs i direktivet ska medlemsstaterna säkerställa att de behöriga myndigheterna har befogenheter och medel att

a) genomföra inspektioner på plats av den kritiska infrastruktur och de lokaler som den kritiska verksamhetsutövaren använder för att tillhandahålla sina samhällsviktiga tjänster och tillsyn på distans av de åtgärder för motståndskraft som vidtagits av verksamhetsutövaren i enlighet med artikel 13, och

b) utföra eller beställa revisioner av kritiska verksamhetsutövare.

Medlemsstaterna ska också säkerställa att de behöriga myndigheterna har befogenheter och medel att kräva att verksamhetsutövare enligt NIS2-direktivet som identifierats som kritiska enligt CER-direktivet inom en rimlig tidsfrist lämnar

a) den information som är nödvändig för att bedöma om de åtgärder som verksamhetsutövarna har vidtagit för att säkerställa sin motståndskraft uppfyller kraven i artikel 13,

b) bevis på att åtgärderna faktiskt har genomförts, inklusive resultatet av en revision som har utförts av en oberoende och kvalificerad revisor som har valts av verksamhetsutövaren och som har utförts på verksamhetsutövarens bekostnad.

Medlemsstaterna ska säkerställa att de behöriga myndigheterna enligt CER-direktivet kan begära att de behöriga myndigheterna enligt NIS2-direktivet ska utöva sina tillsynsbefogenheter på en verksamhetsutövare enligt NIS2-direktivet som har identifierats som kritisk enligt CER-direktivet. För det ändamålet ska medlemsstaterna säkerställa att de behöriga myndigheterna samarbetar och utbyter information (artikel 21).

Medlemsstaterna ska 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 Beskrivning av sektorer i CER-direktivet

4.1 Inledning

De sektorer, undersektorer och kategorier av verksamhetsutövare som omfattas av CER-direktivet anges i direktivets bilaga. Sektorerna är energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, dricksvatten, avloppsvatten, digital infrastruktur, offentlig förvaltning, rymden samt produktion, bearbetning och distribution av livsmedel. Till största del överensstämmer dessa sektorer med de som finns i NIS2-direktivets bilaga 1 och 2. NIS2-direktivet omfattar dock fler sektorer än CER-direktivet. I detta kapitel beskrivs de skillnader som finns i de sektorer som omfattas av de båda direktiven. För en beskrivning av övriga sektorer se kapitel 4 i utredningens delbetänkande[1] och SOU 2017:36.[2]

4.2 Skillnader jämfört med NIS2-direktivet

4.2.1 Energi

Sektorn energi omfattar samma undersektorer och kategorier av verksamhetsutövare som i NIS2-direktivet med den skillnaden att laddningsoperatörer som har ansvar för förvaltning och drift av en laddningspunkt inte omfattas av CER-direktivet.

[1] SOU 2024:18.
[2] SOU 2017:36, s. 65 ff.

4.2.2 Transport

Sektorn transport omfattar samma undersektorer och kategorier av verksamhetsutövare som i NIS2-direktivet med den skillnaden att även undersektorn kollektivtrafik omfattas av CER-direktivet.

- Kollektivtrafikföretag enligt definitionen i artikel 2 d i Europaparlamentets och rådets förordning (EG) nr 1370/2007.[3]

Med kollektivtrafikföretag avses enligt den definitionen ett offentligt eller privat företag, eller en offentlig eller privat företagsgrupp, som bedriver kollektivtrafik, eller ett offentligt organ som tillhandahåller kollektivtrafiktjänster.

4.2.3 Hälso- och sjukvård

Sektorn hälso- och sjukvård omfattar samma undersektorer och kategorier av verksamhetsutövare som i NIS2-direktivet med den skillnaden att en ytterligare kategori av verksamhetsutövare lagts till i CER-direktivet, nämligen verksamhetsutövare med tillstånd att bedriva partihandel i den mening som avses i artikel 79 i direktiv 2001/83/EG.[4] Artikel 79 i det direktivet anger vilka minimikrav som en sökande ska uppfylla för att få tillstånd att bedriva partihandel med läkemedel. För att bedriva partihandel med läkemedel krävs i Sverige tillstånd från Läkemedelsverket. Alla som har tillstånd till partihandel i något land i EU eller EES får handla i alla länder i EU och EES med de läkemedel som tillståndet omfattar.

4.2.4 Offentlig förvaltning

Sektorn offentlig förvaltning omfattar samma undersektorer och kategorier av verksamhetsutövare som i NIS2-direktivet med den skillnaden att offentliga verksamhetsutövare på regional nivå inte omfattas av CER-direktivet. Det är därmed endast offentliga verksamhetsutövare hos nationella regeringar såsom de definieras av en

[3] 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.
[4] Europaparlamentets och rådets direktiv 2001/83/EG av den 6 november 2001 om upprättande av gemenskapsregler för humanläkemedel.

medlemsstat i enlighet med nationell rätt som ingår i sektorn, se vidare kapitel 5.

4.2.5 Produktion, bearbetning och distribution av livsmedel

Sektorn omfattar samma kategorier av verksamhetsutövare som i NIS2-direktivet med den skillnaden att livsmedelsföretag som uteslutande bedriver logistikverksamhet har lagts till. Vidare har ordet *storskalig* lagts till i CER-direktivet när det gäller livsmedelsföretag som bedriver industriell produktion och bearbetning.

5 Tillämpningsområdet

I detta kapitel ska tillämpningsområdet för den lag som införlivar CER-direktivet analyseras.

5.1 Direktivet ska genomföras i ny lag

Utredningens förslag: CER-direktivet ska i huvudsak genomföras genom en ny reglering: lag och förordning om motståndskraft hos kritiska verksamhetsutövare.

Syftet med lagen 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 lagen 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.

På samma sätt som för cybersäkerhet ska CER-direktivets krav samlas i en ny lag med tillhörande förordning.

Artikel 1 a riktar sig mot medlemsstaterna. Av artikeln följer att direktivet innehåller bestämmelser om skyldigheter för medlemsstaterna att vidta särskilda åtgärder som syftar till att säkerställa tjänster som är nödvändiga för att upprätthålla viktiga samhällsfunktioner eller central ekonomisk verksamhet på den inre marknaden.

Artikel 2 innehåller definitioner och i punkt 5 anges att samhällsviktig tjänst betyder en tjänst som är avgörande för att upprätthålla

viktiga samhällsfunktioner, ekonomisk verksamhet, folkhälsa, allmän säkerhet eller miljön. I direktivet pekas elva sektorer ut. Här ingår bland annat energi, transport och offentlig förvaltning. Samtliga sektorer tillhandahåller enligt utredningens bedömning samhällsviktiga tjänster som är avgörande för att säkerställa viktiga samhällsfunktioner. Det betyder att utredningen i sitt författningsförslag kommer att definiera samhällsviktig tjänst som en tjänst som är avgörande för att upprätthålla viktiga samhällsfunktioner, ekonomisk verksamhet, folkhälsa och allmän säkerhet, eller miljön.

Vidare anges i artikel 1 a att direktivet särskilt innehåller skyldigheter för medlemsstaterna att identifiera kritiska entiteter och att stödja dem i deras uppfyllande av skyldigheterna som följer av att vara en sådan entitet.

Utredningen drog i delbetänkandet för NIS2 slutsatsen att det 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.[1] Motsvarande ska även gälla för införlivandet av CER-direktivet.

En utmaning blir då de olika begreppen. Direktivet handlar om att tillhandahålla tjänster som är nödvändiga för viktiga samhällsfunktioner genom att identifiera och stärka motståndskraften hos kritiska entiteter. Utredningen ersatte i sitt delbetänkande begreppet entitet med verksamhetsutövare. Av förenklingsskäl föreslår utredningen att entiteter även i detta sammanhang ersätts med verksamhetsutövare.

Av artikel 1 följer vidare att direktivet innehåller skyldigheter för kritiska entiteter, dvs. kritiska verksamhetsutövare för att stärka deras motståndskraft och förmåga att tillhandahålla tjänster på den inre marknaden. Vidare framgår det att direktivet innehåller bestämmelser om tillsyn och efterlevnadskontroll samt gemensamma förfaranden för samarbete och rapportering. Slutligen följer också av direktivet att det finns särskilda bestämmelser för kritiska verksamhetsutövare av särskild europeisk betydelse.

Av det anförda följer att CER-direktivet sammantaget handlar om att säkerställa samhällsviktiga tjänster som är nödvändiga för att upprätthålla viktiga samhällsfunktioner. För att kunna göra det ska kritiska verksamhetsutövare som tillhandahåller sådana tjänster identifieras och deras motståndskraft ska stärkas. Sammantaget

[1] Se kapitel 5 i SOU 2024:18.

föreslår utredningen att syftet med lagen är att kritiska verksamhetsutövares motståndskraft och förmåga att tillhandahålla samhällsviktiga tjänster i de utpekade sektorerna och att detta styr lagens namn.

5.2 Vem kan omfattas av lagen?

Utredningens förslag: Lagen gäller för enskilda och offentliga verksamhetsutövare som har identifierats som kritiska enligt 2 kap. 1 § i den föreslagna lagen.

Som framgår ovan innehåller direktivet skyldigheter för kritiska verksamhetsutövare. Avgörande är därför definitionen i artikel 2.1. Där anges det att kritisk verksamhetsutövare betyder en offentlig eller privat verksamhetsutövare som medlemsstaten har identifierat i enlighet med artikel 6. Av den artikeln följer att medlemsstaterna ska identifiera de kritiska verksamhetsutövarna för de sektorer och undersektorerna som anges i bilagan. Systematiken innebär således att direktivets bestämmelser ska vara tillämpliga för verksamhetsutövare som omfattas av bilagan till direktivet och uppfyller rekvisiten för att kunna pekas ut som kritisk, samt att den har pekats ut som kritisk av en medlemsstat.

Innebörden av det anförda är att direktivet som huvudregel anger att verksamhetsutövare som omfattas av bilagan kan, men behöver inte, omfattas av direktivets bestämmelser. De verksamhetsutövare som kan omfattas är de som är verksamma inom de elva sektorerna energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, dricksvatten, avloppsvatten, digital infrastruktur, offentlig förvaltning, rymden och produktion, bearbetning och distribution av livsmedel. Som framgår av direktivets bilaga delas sedan vissa av dessa sektorer in i undersektorer. Definitionen av sektorn eller undersektorn anges också i bilagan, oftast genom hänvisning till andra EU-rättsakter. I denna del är CER-direktivet uppbyggt på samma sätt som NIS2-direktivet. Skillnaden mellan NIS2-direktivet och CER-direktivet är att det för CER-direktivet inte räcker att verksamheten ingår i en sektor för att omfattas av direktivets krav och därmed av utredningens förslag till lag. Därutöver tillkommer det alltså som krav för att omfattas att medlemsstaten enligt artikel 6 identifierat verksamhetsutövaren som kritisk. Utredningen kommer

att lämna förslag om identifiering av kritiska verksamhetsutövare i kapitel 6.

Vidare ska kommissionens delegerade förordning (EU) av den 25.7.2023 om komplettering av Europaparlamentets och rådets direktiv (EU) 2022/2557 genom upprättande av en förteckning över samhällsviktiga tjänster noteras.[2] Av artikel 1 i förordningen följer att det är en icke-uttömmande förteckning över samhällsviktiga tjänster i de sektorer och undersektorer som anges i bilagan till CER-direktivet. I motiveringen anges mot bakgrund av direktivets minimiharmoniseringsansats och förteckningens icke uttömmande karaktär att medlemsstaterna, i enlighet med EU-lagstiftningen, skulle kunna komplettera den med ytterligare samhällsviktiga tjänster på nationell nivå, särskilt för att ta hänsyn till nationella särdrag vid tillhandahållandet av samhällsviktiga tjänster.

Från MSB har anförts att för att fullt ut kunna nyttja CER-direktivets möjligheter att stärka samhällets motståndskraft och totalförsvar, bör den långsiktiga målsättningen vara att med stöd av lagen ge tillsynsmyndigheter möjlighet att peka ut verksamhetsutövare inom samtliga av de viktiga samhällsfunktioner som specificeras i MSB:s vägledning *Lista med viktiga samhällsfunktioner – Utgångspunkt för att stärka samhällets beredskap*. Detta förutsätter dock att antalet sektorer och delsektorer utvidgas.

Det anges i artikel 6 att medlemsstaterna ska identifiera de kritiska verksamhetsutövarna för de sektorer och undersektorer som anges i bilagan. Direktivet är ett minimidirektiv, varför det skulle vara möjligt för utredningen att lägga till sektorer eller tjänster inom respektive sektor/undersektor. Denna fråga har utredningen behandlat i avsnitt 2.1.2. Som framgår där är utgångspunkten för utredningen dock att förslagen utformas så att regelbördan och administrationen minimeras för berörda verksamhetsutövare. Om utredningen lämnar mer långtgående förslag ska utredningen motivera varför det är nödvändigt och göra en analys om förslagen är samhällsekonomiskt effektiva och hur svenska företags konkurrenskraft skulle påverkas. En slutsats är därför att tidsramen för uppdraget i hög grad utgör hinder för en utökning av sektorerna. Som vidare framgår ovan behandlar kommissionens förteckning också enbart verksamhetsutövare inom de utpekade sektorerna i bilagan. Denna förteckning är inte ut-

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=PI_COM:C(2023)4878, inhämtat 2024-03-28.

tömmande. Det betyder att utredningen inte kommer att begränsa sina förslag till förteckningen, men till verksamhetsutövare inom sektorerna i bilagan till direktivet. Av skäl 18 i CER-direktivet följer bland annat att medlemsstaterna bör ta vara på det arbete som gjorts och de erfarenheter som dragits utifrån arbetet med att identifiera samhällsviktiga tjänster enligt NIS-direktivet. Utredningen anser att MSB:s publikation *Lista med viktiga samhällsfunktioner – Utgångspunkt för att stärka samhällets beredskap* kan vara ett bra ingångsvärde i detta arbete.

Slutsatsen här är att den verksamhetsutövare som bedriver verksamhet i en sektor som anges i bilagan till direktivet kan omfattas av direktivets krav. För att omfattas krävs det att medlemsstaten identifierar verksamhetsutövaren som kritisk. Utredningen kommer att behandla identifieringen i kapitel 6.

5.2.1 Offentliga verksamhetsutövare

Utredningens förslag: En offentlig verksamhetsutövare är en aktör som bedriver verksamhet och är en statlig myndighet, region eller kommun.

Lagen gäller inte för regeringen, Regeringskansliet, utlandsmyndigheter, kommittéväsendet, Riksrevisionen, Riksdagens ombudsmän, Sveriges Riksbank, Riksdagsförvaltningen och Sveriges domstolar.

Statliga myndigheter

Begreppet offentlig förvaltning i bilagan till CER-direktivet betyder enligt punkt 9 i bilagan offentliga förvaltningsentiteter hos nationella regeringar såsom de definieras av en medlemsstat. I artikel 2.10 anges en definition för offentlig förvaltningsentitet. Det ska vara en entitet som erkänts som sådan i en medlemsstat enligt nationell rätt med undantag för rättsväsendet, parlament och centralbanker. Vidare ska fyra kriterier vara uppfyllda, som innebär att

1. verksamheten har inrättats för att tillgodose behov i det allmännas intresse och inte ha industriell eller kommersiell karaktär,

2. verksamheten har ställning som en juridisk person eller har lagstadgad rätt att företräda en annan verksamhet som har ställning som juridisk person,
3. verksamheten finansieras till största delen offentligt, och
4. verksamheten 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.

I NIS2-direktivet är innebörden av offentlig förvaltning i bilagan bredare, eftersom det ingår både offentliga förvaltningsentiteter hos nationella regeringar och offentliga förvaltningsentiteter på regional nivå, dvs. regioner. Enligt CER-direktivet omfattas inte regioner i sektorn offentlig förvaltning. Inte heller kommuner ingår i sektorn offentlig förvaltning enligt den definition som följer av bilagan.

Det ska dock noteras att definitionerna av offentliga förvaltningsentiteter på nationell nivå är identiska i NIS2- och CER-direktiven.[3] I sitt delbetänkande analyserade utredningen ingående innebörden av offentliga förvaltningsentiteter på nationell nivå för svensk rätt. Slutsatsen blev att som utgångspunkt kan samtliga statliga svenska myndigheter inklusive statliga affärsverk innefattas i definitionen. Eftersom det står ”hos regeringen” i definitionen i punkt 9 i bilagan till CER-direktivet och i NIS2-direktivet bör dock regeringen falla utanför, trots att det är en myndighet. Ordet ”hos” bör enligt utredningens tidigare bedömning även exkludera de fyra myndigheterna som lyder under riksdagen. Dessa är Riksrevisionen, Riksdagens ombudsmän (JO), Sveriges Riksbank och Riksdagsförvaltningen. Sveriges Riksbank är även uttryckligen undantagen i sin egenskap av centralbank. Detsamma gäller domstolarna, eftersom rättsväsendet är undantaget. I begreppet ”Sveriges domstolar” ingår enligt utredningens uppfattning även specialdomstolarna Arbetsdomstolen och Försvarsunderrättelsedomstolen. Däremot ska följande aktörer med funktioner kopplade till rättsväsendet ändå kunna omfattas av den föreslagna regleringen: Domstolsverket, Rättshjälpsmyndigheten, Rättshjälpsnämnden, Domarnämnden, Notarienämnden och Överklagandenämnden för nämndemannauppdrag. Riksdagen är ingen myndighet utan en beslutande för-

[3] Se avsnitt 5.2.4 i SOU 2024:18.

samling och faller därför utanför lagens tillämpning. Utredningen gör alltså samma bedömning för CER-direktivets definition som för den likalydande NIS2-defintionen. När det gäller Regeringskansliet inklusive kommittéväsendet gör utredningen samma bedömning som gjordes i delbetänkandet[4] att de på grund av sin särställning ska undantas.

Utredningen analyserade också särskilt de fyra kriterierna som redovisades ovan. Utredningen ansåg två av dem, att verksamheten har inrättats för att tillgodose behov i det allmännas intresse och inte har industriell eller kommersiell karaktär samt att verksamheten finansieras till största delen offentligt, vara självklara för offentlig verksamhet och menade därför att de inte behövde beröras närmare. Kriteriet om att det är tillräckligt med företrädesrätt utgör heller inget problem för statlig verksamhet. Däremot fann utredningen att det fjärde kriteriet för offentlig förvaltning om att verksamheten skulle ha befogenhet att rikta administrativa eller reglerade beslut till fysiska och juridiska personer som påverkar deras rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital utgjorde en svårighet. Enligt utredningens mening var det inte självklart att samtliga myndigheter fattar beslut som rör gränsöverskridande rörlighet. Samtidigt framstod det inte som ändamålsmässigt att analysera vilka myndigheter som kan fatta beslut om det. För NIS2-direktivet drog utredningen då slutsatsen att direktivets syfte inte var att göra en skiljelinje mellan offentlig verksamhet utifrån beslut om gränsöverskridande påverkan och beaktade då också att NIS2-direktivet är ett minimidirektiv. Utredningen drar motsvarande slutsats för CER-direktivet.

Sammantaget innebär det anförda att lagen om motståndskraft hos kritiska verksamhetsutövare kan omfatta samtliga statliga myndigheter i Sverige med undantag för regeringen, Regeringskansliet, utlandsmyndigheter, kommittéväsendet,[5] Riksrevisionen, JO, Sveriges Riksbank, Riksdagsförvaltningen och Sveriges domstolar. De statliga myndigheter som identifieras ska betecknas *offentliga verksamhetsutövare*.

[4] SOU 2024:18 s. 164.

[5] Det följer vidare av skäl 11, se nedan i 5.3, att utlandsmyndigheter är undantagna. Utredningen bedömde i det här sammanhanget för NIS2-direktivet att även Regeringskansliet och kommittéväsendet bör undantas och gör samma bedömning för CER-direktivet.

Kommuner och regioner

NIS2-direktivet omfattade sektorn offentlig förvaltning uttryckligen även offentliga verksamhetsutövare på regional nivå, det vill säga regioner. Avseende kommuner omfattades dessa inte uttryckligen, men har i utredningens delbetänkande ändå ansetts utgöra offentliga verksamhetsutövare.

I fråga om CER-direktivet ingår varken regioner eller kommuner i sektorn offentlig förvaltning. Samtliga regioner i Sverige är dock vårdgivare enligt en EU-rättslig definition[6] och ingår därmed i sektorn hälso- och sjukvård. Detsamma gäller majoriteten av alla kommuner i Sverige, genom att de bedriver hemsjukvård. Därutöver kan kommuner även ingå i andra sektorer som exempelvis energi eller avloppsvatten under förutsättning att den kommunala verksamheten i denna del inte bedrivs i bolagsform. Kommunalförbund som bildats enligt 3 kap. 8 § kommunallagen (2017:725) är att betrakta som en kommun eller region. Innebörden blir att även regioner och kommuner kan bedömas vara kritiska verksamhetsutövare, se vidare kapitel 6. De kommuner och regioner som identifieras ska betecknas *offentliga verksamhetsutövare*. När det gäller kommunfullmäktige och regionfullmäktige är dessa beslutande församlingar och faller därmed utanför lagens tillämpningsområde.

Avseende bolag som ägs av kommun eller region anser utredningen att det saknas skäl till någon annan bedömning än den som gjordes för NIS2 i delbetänkandet. Som följd ska kommunal- och regionägda bolag som bedriver verksamhet som omfattas av bestämmelserna i lagen om motståndskraft hos kritiska verksamhetsutövare betecknas som enskilda verksamhetsutövare. På motsvarande sätt ska bolag som helt eller delvis ägs av svenska staten anses vara enskilda verksamhetsutövare.

[6] Se 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, jfr 2 kap. 1–3 §§ samt 7 kap. hälso- och sjukvårdslagen (2017:30).

5.2.2 Enskilda verksamhetsutövare

Utredningens förslag: En enskild verksamhetsutövare är en juridisk eller fysisk person som bedriver verksamhet och som inte är en statlig myndighet, region eller kommun.

Direktivet innehåller som ovan anges skyldigheter för kritiska verksamhetsutövare. Kritiska verksamhetsutövare definieras alltså enligt artikel 2.1 som en offentlig eller privat verksamhetsutövare som har identifierats av en medlemsstat i enlighet med artikel 6 som tillhörande en av de kategorier som anges i bilagan till direktivet. Utredningen kommer att benämna privata verksamhetsutövare som enskilda verksamhetsutövare, vilket följer samma systematik som har använts i delbetänkandet. I CER-direktivet definieras inte enskild verksamhetsutövare. Utifrån systematiken i artikel 2.1 anser utredningen dock att den enda rimliga slutsatsen är att alla typer av privata rättssubjekt, dvs både fysiska och juridiska personer, omfattas av begreppet. En sådan tolkning motsvarar även utredningens motsvarande bedömningar avseende NIS2-direktivet. Detta innebär att en enskild verksamhetsutövare utgörs av en fysisk eller juridisk person som inte är en statlig myndighet, region eller en kommun och som bedriver verksamhet.

5.2.3 Kritiska verksamhetsutövare

Utredningens förslag: En kritisk verksamhetsutövare är en offentlig eller enskild verksamhetsutövare som har identifierats enligt 2 kap. 1 § i den föreslagna lagen.

Direktivets definition av kritisk verksamhetsutövare följer av artikel 2.1. Begreppet är centralt eftersom det endast är sådana verksamhetsutövare som identifierats som kritiska som omfattas av direktivets skyldigheter. Kraven för att kunna identifieras utvecklas i kapitel 6. Utredningen bedömer att definitionen ska genomföras i svensk rätt med tillägget att identifiering ska ske genom att den svenska föreslagna mekanismen för identifiering har tillämpats (som i sin tur överensstämmer med artikel 6 i CER-direktivet, se vidare kapitel 6).

Av direktivets definition av kritisk verksamhetsutövare följer att en sådan ska ha identifierats som tillhörande en av de kategorier av entiteter som följer av bilagan till CER-direktivet. Identifieringsprocessen i artikel 6 förutsätter i sin tur att den aktuella samhällsviktiga tjänsten går att härleda till bilagan till direktivet. Det synes inte finnas någon tydlig anledning varför definitionen i artikel 2.1 hänvisar till ”kategorier […] som följer av bilagan” i stället för att enbart hänvisa till bilagan på samma sätt som artikel 6 gör. Utredningen bedömer att denna skillnad saknar materiell betydelse, eftersom en verksamhetsutövare betecknas som kritisk först genom att den identifierats i enlighet med artikel 6, och en förutsättning för att detta ska kunna ske är att den samhällsviktiga tjänsten är hänförlig till bilagan. Utredningen anser mot denna bakgrund att definitionen av *kritisk verksamhetsutövare* i svensk rätt inte behöver nämna bilagan, så länge den hänvisar till identifieringsmekanismen.

5.3 Undantag från tillämpningsområdet

5.3.1 Undantag för sådant som regleras i lagen om cybersäkerhet

Utredningens förslag: Lagen gäller inte för sådant som regleras i lagen om cybersäkerhet (2025:000).

Artikel 1 innehåller undantag från direktivets tillämpningsområde. Det första undantaget följer av första delen av artikel 1.2. Där anges det att CER-direktivet inte är tillämpligt på frågor som omfattas av NIS2-direktivet. Det betyder att cybersäkerhetsregleringen har företräde, vilket ska följa av utredningens förslag till lagen om motståndskraft hos kritiska verksamhetsutövare. I CER-direktivet betonas att medlemsstaterna ska samordna införlivningen av NIS2- och CER-direktiven på grund av förhållandet mellan fysisk säkerhet och cybersäkerhet (artikel 1.1). Syftet med undantaget om att CER-direktivet inte är tillämpligt på sådant som regleras i cyberssäkerhetslagen bör vara att förhindra överlappande reglering. Det bör även noteras att en verksamhetsutövare som blir utpekad som kritisk

enligt CER-direktivet även ska betecknas som *väsentlig* verksamhetsutövare enligt NIS2-direktivet.[7]

Utredningen anser att den grundläggande frågan att ta ställning till är vad som regleras i cybersäkerhetslagen, och därmed ska undantas från lagen om motståndskraft hos kritiska verksamhetsutövare. Syftet med att undanta NIS2-regleringen är att en kritisk verksamhetsutövare inte ska behöva genomföra samma åtgärder, incidentrapportering med mera enligt båda regelverken. Det bör dock noteras att direktivens skyddsföremål är olika saker. NIS2-direktivet skyddar nätverks- och informationssystem, medan CER-direktivet ska skydda en samhällsviktig tjänst i sin helhet, inklusive dess kritiska infrastruktur. En verksamhetsutövare kan därför ha vidtagit riskhanteringsåtgärder enligt NIS2-direktivet för att skydda ett visst informationssystem, men fortfarande vara skyldig att vidta bredare åtgärder för motståndskraft avseende fysisk säkerhet och kontinuitetsåtgärder enligt CER-direktivet för att säkerställa tillhandahållandet av den samhällsviktiga tjänsten. Åtgärder och rapportering enligt NIS2-direktivet kan enligt utredningen därför ses som en delmängd av vad en kritisk verksamhetsutövare kan vara skyldig att vidta enligt CER-direktivet. Mot denna bakgrund ser utredningen två möjliga sätt att undanta NIS2-frågorna.

Det första alternativet är att peka ut lagen om cybersäkerhet som ett sådant undantag på författning som anses ha motsvarande verkan avseende något/några av områdena riskbedömning, åtgärder för motståndskraft, bakgrundskontroller och incidentanmälan (se vidare avsnitt 5.3.3). Utredningen anser att detta alternativ potentiellt skulle kunna bidra med ökad tydlighet i fråga vilka områden som ens kan övervägas ha motsvarande verkan enligt cybersäkerhetslagen. En sådan typ av skrivning kräver dock fortfarande tolkning avseende vad som är syftet med cybersäkerhetslagen, och vad som kan skyddas till följd av det regelverket. Att peka ut undantagna områden, som endast är undantagna inom vissa skyddsområden, skulle därför enligt utredningen kunna bidra till förvirring snarare än klargöranden. Alternativet bedöms därför inte vara en framkomlig väg.

Det andra alternativet är att, med en formulering liknande den som finns i direktivet, undanta frågor som omfattas av lagen om cybersäkerhet. Utredningen noterar att den typen av undantag också skapar behov av tolkning av vad både lagarna reglerar, för att kunna

[7] Se artikel 3.1 f i NIS2-direktivet.

avgöra vad som är undantaget från tillämpningen av lagen om motståndskraft hos kritiska verksamhetsutövare. Detta skulle kunna anses göra innebörden av undantaget svårtillgängligt för läsaren. Utredningen anser dock i gengäld att det tillåter undantaget i lagen om motståndskraft hos kritiska verksamhetsutövare att formuleras på ett tydligare sätt som inte riskerar att vilseleda läsaren. Utredningen anser att detta alternativ ska föreslås. Ett sådant undantag bör dock språkligt utformas som att den nu aktuella lagen inte gäller för sådant som regleras i lagen om cybersäkerhet. Detta markerar att lagen är subsidiär, men endast för sådant som faktiskt är reglerat och skyddas av cybersäkerhetslagen.

5.3.2 Undantag för verksamhetsutövare inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur

Utredningens förslag: För kritiska verksamhetsutövare inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur gäller inte kapitel 3–6 i den föreslagna lagen.

Utredningens bedömning: Vissa kritiska verksamhetsutövare kan identifieras som kritiska men ska endast omfattas av kapitel I, II (exkl. artikel 11) och V i CER-direktivet.

I artikel 8 anges att medlemsstaterna ska säkerställa att artikel 11 och kapitel III (krav om motståndskraft verksamhetsutövare), IV (bestämmelser om kritiska verksamhetsutövare av särskild europeisk betydelse) och VI (bestämmelser om tillsyn och efterlevnadskontroll) i direktivet inte är tillämpliga på kritiska verksamhetsutövare inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur. Artikel 11 avser samarbete mellan medlemsstaterna. I skäl 20 och 21 motiveras detta undantag. Av skäl 20 följer för digital infrastruktur att NIS2-direktivet redan ställer krav om åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem samt incidentrapportering. Dessa krav är minst likvärdiga med kraven i CER-direktivet. På motsvarande sätt anges i skäl 21 att det i olika EU-rättsakter redan finns heltäckande krav på finansiella verksamhetsutövare. För att undvika dubbelarbete och

onödig administration ska därför bestämmelserna i artikel 11 och kapitel III, IV och VI i direktivet inte gälla för dem.

Utredningens bedömning att innebörden av regleringen är att verksamhetsutövare inom dessa sektorer förvisso ska kunna pekas ut som kritiska, men att direktivet i mycket begränsad utsträckning ska gälla för dem. De bestämmelser i direktivet som gäller för dessa verksamhetsutövare är de som riktar sig mot medlemsstaten om att upprätta en strategi, en riskbedömning och att identifiera kritiska verksamhetsutövare, samt möjligheten att få stöd av medlemsstaten (artikel 10). Vidare ska de ha möjlighet att ingå i gruppen för kritiska entiteters motståndskraft (artikel 19) och begära stöd av kommissionen (artikel 20).

Utredningen kan sammanfattningsvis konstatera att de artiklar som gäller för de aktuella verksamhetsutövarna medför rättigheter snarare än skyldigheter. Detta behöver även framgå av författningsförslaget. Lagtekniskt föreslår utredningen att undantaget ska utformas så att vissa kapitel i författningsförslaget inte gäller för sådana aktörer.

5.3.3 Undantag för åtgärder enligt andra regelverk med motsvarande verkan

Utredningens förslag: 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.

I artikel 1.3 anges att om det i sektorsspecifika unionsrättsakter finns bestämmelser om krav för kritiska verksamhetsutövare att vidta åtgärder för att stärka sin motståndskraft som av medlemsstaten erkänns som åtminstone likvärdiga ska kraven i CER-direktivet inklusive bestämmelserna om tillsyn och efterlevnad inte gälla. De

bestämmelserna om åtgärder för att stärka sin motståndskraft bör då rimligen vara kraven om riskbedömning, åtgärder för motståndskraft, bakgrundskontroller och incidentanmälan som återfinns i direktivets kap. III och artiklarna 12–15. Om dessa krav inte gäller blir en följd att inte heller kraven om tillsyn och efterlevnad kan gälla. Utredningen föreslog i cybersäkerhetslagen en liknande bestämmelse, se delbetänkandet avsnitt 5.4, och det finns också nu redan en sådan bestämmelse i 9 § i nu gällande lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, NIS-lagen. Till utredningen hade det dock förts fram att tillämpningen av 9 § NIS-lagen var svår, eftersom bedömningen om kraven är likvärdiga är komplex. Utredningen föreslog därför också i delbetänkandet att regeringen i en bilaga till förordningen pekar ut de författningar som innehåller bestämmelser med motsvarande verkan. Bestämmelserna i bilagan bör beredas av den eller de myndigheter regeringen finner lämpligt.[8] Utredningen finner nu skäl att föreslå en motsvarande reglering för CER-direktivet. Även här bör regeringen peka ut de författningar som innehåller bestämmelser med motsvarande verkan. Detta rimmar väl med formuleringen i CER-direktivet om att det ska vara bestämmelser som medlemsstaten erkänner som likvärdiga. Ett sådant krav saknades i NIS2-direktivet. Utredningen föreslår också att regeringen ger 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 (se vidare kapitel 16).

5.3.4 Undantag för brottsbekämpning och Sveriges säkerhet

Utredningens förslag: 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.

[8] SOU 2024:18 s. 153.

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.

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.

En ny bestämmelse avseende underrättelse om kritiska verksamhetsutövare med följande lydelse införs i säkerhetsskyddslagen.

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 meddela huruvida den kritiska verksamhetsutövaren har anmält att den bedriver säkerhetskänslig verksamhet enligt 2 kap. 6 § säkerhetsskyddslagen (2018:585).

Av artikel 1.5 följer en generell inskränkning av direktivets tillämpningsområde. I bestämmelsen anges 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. Denna generella inskränkning omsätts i konkreta undantag i de följande delartiklarna.

I artikel 1.6 anges att direktivet inte är tillämpligt på offentliga verksamhetsutövare som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning. I begreppet brottsbekämpning innefattas utredning, upptäckt och lagföring av brott. Av skäl 11 följer dock att undantaget för offentliga verksamhetsutövare bör tillämpas på verksamhetsutövare vars verksamhet till övervägande del bedrivs inom områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning. För offentliga verksamhetsutövare som endast marginellt hänför sig till dessa områden bör dock omfattas av direktivets tillämpningsområde. Verksam-

hetsutövare som har tillsynsbefogenheter anses inte bedriva brottsbekämpning. Det framgår vidare att offentliga verksamhetsutövare som inrättats gemensamt med ett tredjeland i enlighet med internationellt avtal och medlemsstaternas diplomatiska och konsulära beskickning i tredje länder inte omfattas av direktivet.

Bestämmelserna är i denna del identiska med dem i NIS2-direktivet. Enda skillnaden är att i NIS2-direktiven är i denna del även anger nätverks- och informationssystem som drivs för användare i tredjeland inte omfattas av direktivet.

Vidare följer av artikel 1.7 en möjlighet för medlemsstaterna att undanta särskilda kritiska verksamhetsutövare från att tillämpa artikel 11 och kapitel III, IV och VI i CER-direktivet. Detta gäller om verksamhetsutövaren bedriver verksamhet inom områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet utredning, upptäckt och lagföring av brott, eller som uteslutande tillhandahåller tjänster till de offentliga verksamhetsutövare som till övervägande del bedriver motsvarande verksamhet. Ett sådant undantag kan alltså tillämpas på både enskilda och offentliga verksamhetsutövare. Utredningen noterar att undantaget innebär samma typ av undantag som redogjorts för under avsnitt 5.3.2 ovan. Vidare anser utredningen att det är motiverat att föreslå ett sådant undantag avseende både enskilda och offentliga verksamhetsutövare som till någon del bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen (2018:585), SäkL. Utformningen bör innebära att om den samhällsviktiga tjänst som en kritisk verksamhetsutövare upprätthåller till någon del omfattas av SäkL, ska den delen inte omfattas av kraven i lagen om motståndskraft hos kritiska verksamhetsutövare. Verksamhetsutövaren ska dock ha samma rättigheter som följer av avsnitt 5.3.2. Om den aktuella samhällsviktiga tjänsten uteslutande utgörs av säkerhetskänslig verksamhet ska endast ett begränsat antal av CER-direktivet bestämmelser (se avsnitt 5.3.2) tillämpas. Om det finns delar av den aktuella samhällsviktiga tjänsten som inte är säkerhetskänslig ska kraven tillämpas fullt ut i de delarna.

I delbetänkandet[9] har utredningen analyserat hur undantaget för offentliga och enskilda verksamhetsutövare bör utformas. Eftersom CER-direktivet, till skillnad från NIS2-direktivet, endast träffar en samhällsviktig tjänst kan dock inte samma utformning av undantaget

[9] SOU 2024:18 avsnitt 5.5.4 och 5.5.5.

användas här. I stället bör undantaget utformas på ett sådant sätt att den föreslagna lagen gäller för en samhällsviktig tjänst, även om den omfattas av reglerna i SäkL. Kraven ska dock inte tillämpas inom de delar som är säkerhetskänsliga. Däremot ska de möjligheter till stöd som följer av den föreslagna lagen finnas tillgängliga för verksamhetsutövaren.

Om en verksamhetsutövare uppger till sin tillsynsmyndighet att den samhällsviktiga tjänsten till någon del är säkerhetskänslig ska tillsynsmyndigheten underrätta berörd tillsynsmyndighet enligt säkerhetsskyddsregelverken. Detta för att en kritisk verksamhetsutövare inte ska kunna undvika tillsyn genom att uppge att en viss samhällsviktig tjänst är säkerhetskänslig trots att den inte är det, och på så sätt kringgå tillsyn enligt endera av regelverken. På motsvarande sätt bör det införas en skyldighet för den myndighet som är tillsynsmyndighet enligt SäkL och som mottagit underrättelsen att meddela tillsynsmyndigheten om den aktuella verksamhetsutövaren har anmält att den bedriver säkerhetskänslig verksamhet. Om så inte har skett bör tillsynsmyndigheten vara obehindrad att gå vidare i sin tillsyn av verksamhetsutövaren.

5.3.5 Uppgiftsskyldigheter omfattar inte uppgifter som omfattas av säkerhetsskyddslagen

Utredningens förslag: Skyldighet att lämna uppgifter enligt den föreslagna lagen gäller inte uppgifter som är säkerhetsskyddsklassificerade enligt säkerhetsskyddslagen (2018:585).

Av artikel 1.8 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. Utredningen föreslår därför att det införs en bestämmelse i lagen om att skyldighet att lämna uppgifter inte gäller uppgifter som är säkerhetsskyddsklassificerade enligt säkerhetsskyddslagen (2018:585). En likalydande bestämmelse finns i förslaget till cybersäkerhetslagen.[10]

[10] Se SOU 2024:18 avsnitt 5.5.3.

5.3.6 Tillträdesrätt till lokaler med mera som omfattas av säkerhetsskyddslagen

Utredningens förslag: Tillsynsmyndighetens undersökningsbefogenheter i den föreslagna lagen omfattar inte sådana delar av områden, lokaler eller andra utrymmen där säkerhetskänslig verksamhet enligt säkerhetsskyddslagen (2018:585) bedrivs.

Av artikel 1.5 framgår att CER-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 rådgivande uppdrag anges i artikel 18.8 att detta 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.

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 detta direktiv, ska 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 beskrivs i kapitel 9.

Utredningen föreslår därför att det införs en bestämmelse i lagen som begränsar undersökningsbefogenheten avseende sådana områden, lokaler och andra utrymmen där säkerhetskänslig verksamhet bedrivs. Begränsningen ska dock inte uppfattas som att den träffar alla sådana utrymmen där säkerhetsskyddsåtgärder har vidtagits, utan endast till sådana platser där den säkerhetskänsliga verksamheten bedrivs och i direkt anslutning till detta. Exempelvis kan en säkerhetsskyddsåtgärd bestå i att sätta upp ett stängsel med viss dimensionering utanför en byggnad. I byggnaden bedrivs både säkerhetskänslig verksamhet och upprätthållandet av en samhällsviktig tjänst som inte är säkerhetskänslig. Skulle begränsningen tolkas extensivt skulle tillsynsmyndigheten inte få beträda området

innanför stängslet. Detta är inte den avsedda tolkningen. Begränsningen avser tillträdet till det område, lokal eller utrymme där den säkerhetskänsliga verksamheten bedrivs, och i omedelbar anslutning till det. Om det finns en del av området eller byggnaden som förvisso omfattas av säkerhetsskyddsåtgärder men där säkerhetskänslig verksamhet inte bedrivs ska tillsynsmyndigheten ha rätt att få tillträde dit. Begränsningen i tillträdesrätten bör därför formuleras som att tillsynsmyndigheten inte har rätt till tillträde till de delar av områden, lokaler och andra utrymmen där säkerhetskänslig verksamhet enligt säkerhetsskyddslagen bedrivs.

6 Identifiering av kritiska verksamhetsutövare

I detta kapitel analyseras identifiering av kritiska verksamhetsutövare enligt artikel 6, betydande störande effekt i artikel 7 och definitionerna i artiklarna 2.4 och 2.5. Vidare analyseras artikel 5 om medlemsstaternas riskbedömning. Slutligen analyseras även artikel 2.3 och artikel 3.1 f i NIS2-direktivet.

6.1 Nationell riskbedömning

Utredningens förslag: 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 de andra sektorerna, inklusive betydande risker för medborgare och den inre marknaden.
3. Information om de incidenter som har rapporterats enligt 5 kap. i den föreslagna lagen.

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[1] och (EU) 2019/941[2] och Europaparlamentets och rådets direktiv 2007/60/EG[3] och 2012/18/EU[4].

Tillsynsmyndigheten ska bidra med underlag till den nationella riskbedömningen. Den som står under tillsyn ska på begäran tillhandahålla tillsynsmyndigheten den information som behövs för den nationella riskbedömningen.

Utredningens bedömning: Myndigheten för samhällsskydd och beredskap ska göra en nationell riskbedömning.

Myndigheten för samhällsskydd och beredskap ska delge tillsynsmyndigheterna och de kritiska verksamhetsutövarna relevanta delar av den nationella riskbedömningen.

Myndigheten för samhällsskydd och beredskap ska lämna relevant information till kommissionen om de typer av risker som har identifierats i den nationella riskbedömningen, per sektor och undersektor enligt bilagan till CER-direktivet inom tre månader från det att riskbedömningen har upprättats eller uppdaterats.

Av artikel 5 följer en skyldighet för varje medlemsstat att senast den 17 januari 2026 göra en riskbedömning (medlemsstaternas riskbedömning) och därefter när så är nödvändigt, men minst vart fjärde år. Vid upprättandet av riskbedömningen ska delegerade akter som meddelats med stöd av artikel 5.1 beaktas. Medlemsstaternas riskbedömning ska sedan användas av de behöriga myndigheterna vid identifiering av kritiska verksamhetsutövare, samt för att bistå de kritiska verksamhetsutövarna med att vidta åtgärder för motståndskraft (se avsnitt 8.2). Riskbedömningen 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

[1] 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).
[2] 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).
[3] 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).
[4] 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).

andra antagonistiska hot, inklusive terroristbrott enligt Europaparlamentets och rådets direktiv (EU) 2017/541.[5] Utöver detta ska riskbedömningen även ta hänsyn till:

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[6] och (EU) 2019/941[7] samt Europaparlamentets och rådets direktiv 2007/60/EG[8] och 2012/18/EU.[9]

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 verksamhetsutövare 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 punkten c ska medlemsstaterna samarbeta med de behöriga myndigheterna i andra medlemsstater och de behöriga myndigheterna i tredjeländer, när så är lämpligt. Vidare ska medlemsstaterna göra de relevanta delarna i riskbedömningarna tillgängliga för de verksamhetsutövare som har identifierats som kritiska.

Utredningen kan konstatera att den nationella riskbedömningen enligt CER ska identifiera relevanta hot, risker och sårbarheter, samt ska dra nytta av det arbete som redan görs till följd av andra EU-

[5] 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).
[6] 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).
[7] 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).
[8] 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).
[9] 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).

rättsakter. Exemplifieringen som anges i CER-direktivet bör föras in i den föreslagna lagen. Den nationella riskbedömningen ska även identifiera beroenden mellan sektorer, till andra medlemsländer och till tredje land, vilket också bör framgå av bestämmelsen. Riskbedömningen ska sedan läggas till grund för identifieringen av kritiska verksamhetsutövare, och att dessa ska vidta lämpliga och ändamålsenliga åtgärder för att stärka sin motståndskraft (jfr skäl 15). Riskbedömningen ska uppdateras vid behov men minst vart fjärde år. Eftersom tillsynsmyndigheten ska beakta den nationella riskbedömningen vid identifieringen av kritiska verksamhetsutövare behöver tillsynsmyndigheten få del av relevanta delar. Den nationella riskbedömningen ska även göras tillgänglig för kritiska verksamhetsutövare i landet (artikel 5.3) så att den kan ligga till grund för den kritiska verksamhetsutövarens riskbedömning och åtgärder för att stärka sin motståndskraft. När en nationell riskbedömning har upprättats eller uppdaterats ska medlemsstaten inom tre månader förse kommissionen med viss information.

MSB har redan i dag ansvar för att upprätta vissa av de riskbedömningar som omnämns i artikel 5, bland annat inom ramen för civilskyddsmekanism.[10] Andra delar av ansvaret ligger på Energimyndigheten och Svenska Kraftnät. Utredningen föreslår att en aktör får ett utpekat ansvar för att upprätta den nu aktuella nationella riskbedömningen. Enligt utredningen ligger det närmast till hands att föreslå MSB för denna uppgift. MSB kommer enligt utredningens förslag även vara den myndighet som ska ta emot incidentrapporter från kritiska verksamhetsutövare, och har därmed tillgång till den information som avses i artikel 5.2 d, se avsnitt 8.3. MSB har även i dag ansvar för att upprätta riskbedömningar samt har upparbetade kontaktvägar för att inhämta underlag till sådana.[11] Ett alternativ vore att regeringen själv ska behålla detta ansvar utan att delegera till någon av sina myndigheter. Utredningen har dock inte funnit några starkt vägande skäl som talar för en sådan lösning. Som följd ska MSB föreslås ansvara för att ta fram den nationella riskbedömningen enligt CER, samt i övrigt de uppgifter som följer av det ansvaret. Det innebär att det är MSB som ska delge tillsynsmyndigheten och de kritiska verksamhetsutövarna relevanta delar av den nationella risk-

[10] Jfr bland annat 9 § i förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.
[11] Jfr *Nationell risk- och sårbarhetsbedömning (NRSB) 2023* s. 13, dnr MSB 2022-11265-23, hämtad 2024-05-28 från https://rib.msb.se/filer/pdf/30546.pdf.

bedömningen och även lämna relevant information till kommissionen om de typer av risker som har identifierats i den nationella riskbedömningen, per sektor och undersektor enligt bilagan till CER-direktivet. Informationen till kommissionen ska lämnas inom tre månader från att den nationella riskbedömningen upprättats eller uppdaterats. Utredningen anser att det ska införas en skyldighet för tillsynsmyndigheterna att ge MSB den information som behövs för att myndigheten ska kunna upprätta den nationella riskbedömningen. På motsvarande sätt bör även tillsynsmyndigheterna ges möjlighet att inhämta de uppgifter som behövs från kritiska verksamhetsutövare för att den nationella riskbedömningen ska kunna upprättas.

6.2 Samhällsviktiga tjänster – vad ska skyddas?

6.2.1 Begreppen samhällsviktig tjänst kontra samhällsviktig verksamhet

I CER-direktivet är samhällsviktig tjänst ett centralt begrepp och definieras i artikel 2.5 som en tjänst som är avgörande för att upprätthålla viktiga samhällsfunktioner, ekonomisk verksamhet, folkhälsa och allmän säkerhet, eller miljön. Det är språkligt närliggande begreppet samhällsviktig verksamhet som återfinns i 6 § 2 förordningen (2022:524) om statliga myndigheters beredskap. I förordningen definieras begreppet som verksamhet, tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet. Exempelvis kan verksamheter såsom militärt försvar, diplomatiska förbindelser och centralbanksfunktioner ingå i samhällsviktig verksamhet. Som stöd för bedömningen av vad som kan utgöra en viktig samhällsfunktion som behövs för samhällets grundläggande behov, värden eller säkerhet, som samhällsviktig verksamhet i sin tur understödjer, har MSB tagit fram en lista.[12] Utredningen anser att det omfattande arbete som bedrivs och den kunskap som finns avseende att

[12] *Lista med viktiga samhällsfunktioner – Utgångspunkt för att stärka samhällets beredskap*, MSB1844 – reviderad oktober 2023. Hämtad 2024-03-29 från https://rib.msb.se/filer/pdf/29800.pdf.

identifiera samhällsviktig verksamhet[13] är av stort värde för att identifiera samhällsviktiga tjänster enligt CER-direktivet.

Utredningen anser att innebörden av begreppen *samhällsviktig tjänst* och *verksamhet* är likartad, men inte identisk. Samhällsviktig verksamhet är inte begränsad till att kunna återfinnas inom någon av de sektorer som anges i CER-direktivet, utan kan finnas inom hela samhället. Med detta sagt bedömer utredningen dock att en samhällsviktig tjänst många gånger också kommer att kunna anses utgöra en samhällsviktig verksamhet. Motsatsförhållandet gäller dock inte, eftersom flera samhällsviktiga verksamheter faller utanför CER-direktivets sektorer. Eftersom motsatsförhållandet inte gäller kan begreppen inte sägas ha en identisk betydelse. Som följd anser utredningen att begreppen inte är synonyma. Givet att utredningen av skäl som anförts (se avsnitt 2.1.2) inte avser föreslå någon utvidgning av de sektorer som ska träffas av CER-kraven bör begreppen redan av detta skäl undvika att blandas samman. Som följd kommer utredningen i det följande att använda begreppet *samhällsviktig tjänst* för att beskriva de tjänster som kan träffas av CER-kraven. Begreppet kommer inte att definieras i förhållande till samhällsviktig verksamhet, utan kommer få ha en egen betydelse som endast tar sikte CER-direktivets tillämpningsområde. Utredningen ser dock ett stort värde i att i framtiden se över både NIS2- och CER-direktivens koppling till det svenska beredskapssystemet, och där möjlighet att ensa så väl begrepp som sektorer som träffas av olika regelverk vore positivt.[14]

6.2.2 Vad utgör en samhällsviktig tjänst?

Utredningens bedömning: För att en viss tjänst ska kunna omfattas av CER-direktivets krav krävs att den

1. är avgörande för att upprätthålla viktiga samhällsfunktioner, ekonomisk verksamhet, folkhälsa och allmän säkerhet, eller miljön, och
2. omfattas av bilagan till CER-direktivet.

[13] Jfr 7 § 1 förordningen (2022:524) om statliga myndigheters beredskap.
[14] Liknande bedömningar har tidigare gjorts i fråga om NIS-regelverket, se prop. 2017/18:205 s. 22 f.

Av artikel 6.2 a i CER-direktivet följer att en verksamhetsutövare behöver tillhandahålla minst en samhällsviktig tjänst för att kunna pekas ut som kritisk. Utredningens uppfattning är att systematiken i CER-direktivet kretsar kring att vissa samhällsviktiga tjänster behöver omfattas av ett särskilt skydd. Genom att en verksamhetsutövare, som tillhandahåller en sådan samhällsviktig tjänst, identifieras uppstår skyldigheter för verksamhetsutövaren. En sådan verksamhetsutövare benämns genom identifieringen som kritisk verksamhetsutövare. Genom att verksamhetsutövaren underrättats om identifieringen uppstår även skyldigheter för den att skydda den aktuella samhällsviktiga tjänsten (eller tjänsterna).

Denna tolkning utesluter enligt utredningen att den samhällsviktiga tjänsten skulle benämnas ”kritisk samhällsviktig tjänst”, ”samhällskritisk tjänst” eller liknande. Det rör sig i stället om en viss samhällsviktig tjänst som tillhandahålls av en verksamhetsutövare som har identifierats som kritisk.

I artikel 2.5 i CER-direktivet definieras ”samhällsviktig tjänst” som en tjänst som är avgörande för att upprätthålla viktiga samhällsfunktioner, ekonomisk verksamhet, folkhälsa och allmän säkerhet, eller miljön. I direktivet anges dock inte vad som avses med ”tjänst”, och därmed inte heller vad som faller utanför tjänstebegreppet. Utredningen bedömer dock att det som utgångspunkt endast är sådana samhällsviktiga tjänster som träffas av definitionen i artikel 2.5 och som träffas av någon av sektors- eller undersektorsdefinitionerna i bilagan till CER-direktivet som kan omfattas av CER-kraven. Avseende vilka tjänster som kan avses så följer vissa närmare angivelser av den delegerade akt som kommissionen har meddelat.[15] Dessa behöver beaktas av den myndighet som ska bedöma om en viss samhällsviktig tjänst kan identifieras.

[15] 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. Kommissionen har meddelat förordningen med stöd av artikel 5.1 i CER-direktivet.

6.3 Krav för identifiering av kritiska verksamhetsutövare

Utredningens förslag: För att identifieras som kritisk verksamhetsutövare 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.

Samhällsviktig tjänst i eller till Sverige och som omfattas av bilagan

Det första kriteriet för att kunna identifieras som en kritisk verksamhetsutövare är att man tillhandahåller en samhällsviktig tjänst som omfattas av någon av sektorerna som finns i bilagan till CER-direktivet. Innebörden av begreppet samhällsviktig tjänst har redogjorts för ovan. Direktivet saknar en definition av vad begreppet ”tillhandahåller” innebär. Utredningens uppfattning är att begreppet allmänspråkligt kan förstås som att något görs tillgängligt för användning eller konsumtion, samt alla mellanliggande led av detta, exempelvis etablering, drift eller kontroll. Genom att tjänsten ska tillhandahållas i eller till Sverige krävs att tjänsten på något vis är tillgänglig för den svenska marknaden. Detta medför att Sverige inte kan identifiera en verksamhetsutövare som kritisk om den förvisso har kritisk infrastruktur i Sverige (se nedan) och en samhällsviktig tjänst tillhandahålls till en annan medlemsstat, men inte till den svenska marknaden. En verksamhetsutövare kan tillhandahålla flera

samhällsviktiga tjänster, vilket innebär att verksamhetsutövaren kan identifieras som kritisk av flera tillsynsmyndigheter. Detta medför att verksamhetsutövaren kan bli föremål för tillsyn av flera tillsynsmyndigheter, men avseende olika samhällsviktiga tjänster.

Verksamhet och kritisk infrastruktur belägen i Sverige

Av artikel 6.2 b följer ytterligare krav för att en verksamhetsutövare ska kunna identifieras som kritisk, nämligen att den bedriver verksamhet på medlemsstatens territorium och har sin kritiska infrastruktur belägen där. En verksamhetsutövare bör enligt skäl 16 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 verksamhetsutövarens kritiska infrastruktur, som används för att tillhandahålla tjänsten eller tjänsterna är belägen. Avseende ledet ”att bedriva verksamhet” anser utredningen att detta alltid är uppfyllt för en verksamhetsutövare som har uppfyllt kravet på att erbjuda en eller flera samhällsviktiga tjänster (jfr artikel 6.2 a) i landet. Utredningen kan inte se någon möjlighet för en verksamhetsutövare att erbjuda en sådan tjänst utan att samtidigt anses bedriva verksamhet. Det relevanta rekvisitet att bedöma i artikel 6.2 b är därför den kritiska infrastrukturens belägenhet.

Att den kritiska infrastrukturen ska vara belägen inom Sveriges gränser medför enligt utredningens uppfattning ett krav på svensk jurisdiktion för att identifiering ska kunna ske. Detta hänger samman med att möjligheterna att rikta ingripanden och sanktioner mot en kritisk verksamhetsutövare förutsätter svensk jurisdiktion.[16] Innebörden av att det måste finnas kritisk infrastruktur inom Sveriges gränser bör enligt utredningen inte kunna aktualisera några större tolkningssvårigheter. Dessa behöver befinna sig inom de svenska land- eller sjöterritorierna[17] på det som de definierats inom internationell och nationell rätt.

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. Definitionen

[16] Jfr skäl 40.
[17] Se lagen (2017:1272) om Sveriges sjöterritorium och maritima zoner.

är därmed mycket bred och kan träffa exempelvis byggnader, nätverks- och informationssystem, en maskin eller annat. Det saknas en nedre gräns för vad som kan anses utgöra ”en del” av den kritiska infrastrukturen. Utredningen bedömer därför att alla delar av kritisk infrastruktur, hur små de än är, träffas av begreppet. För att kunna identifiera vad som utgör kritisk infrastruktur bör ledning kunna sökas i vilken påverkan som en störning eller ett bortfall av (delen av) infrastrukturen skulle ha på den samhällsviktiga tjänsten. Om en störning eller ett bortfall av infrastrukturen på något sätt skulle påverka tillgängligheten hos den samhällsviktiga tjänsten så är den att betrakta som (en del av) kritisk infrastruktur.

Vidare tolkar utredningen kraven på att bedriva verksamhet och att kritisk infrastruktur inom landets gränser som kumulativa, dvs att de båda måste vara uppfyllda för att en medlemsstat ska ha rätt att peka ut en sådan verksamhetsutövare som kritisk. Konsekvensen av detta blir att om en verksamhetsutövare förvisso erbjuder en eller flera samhällsviktiga tjänster inom Sverige, men att kritisk infrastruktur för att upprätthålla tjänsten helt saknas i Sverige, så kan inte Sverige identifiera verksamhetsutövaren som kritisk. Samma slutsats gäller för en aktör som förvisso har kritisk infrastruktur i Sverige, men där ingen samhällsviktig tjänst tillhandahålls.

En incident skulle få en betydande störande effekt för tillhandahållandet av den samhällsviktiga tjänsten

Det sista kriteriet för att kunna identifiera en verksamhetsutövare som kritisk är enligt artikel 6.2 c att en incident skulle få betydande störande effekter på tillhandahållandet 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. Innebörden av detta rekvisit är omfattande och behandlas i avsnitt 6.4.

Beaktanden vid identifiering

Av artikel 6.2 följer att medlemsstaten vid identifieringen ska ta hänsyn till resultatet av sin riskbedömning och strategi. Vidare har kommissionen, i enlighet med artikel 5.1 och 23, meddelat en genom-

förandeakt innehållande en icke uttömmande lista över samhällsviktiga tjänster inom de sektorer och undersektorer som omfattas av bilagan till direktivet.[18] Utredningen anser att det ska framgå av den föreslagna lagen att samtliga dessa ska beaktas av tillsynsmyndigheten vid identifiering.

6.4 Betydande störande effekt

Utredningens förslag: Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om när en störande effekt är betydande.

Utredningens bedömning: Det ska införas en bestämmelse i förordningen om att följande kriterier ska beaktas vid fastställandet av när en störande effekt är betydande.

a) Antalet användare som är beroende av den samhällsviktiga tjänst som den berörda verksamhetsutövaren tillhandahåller,

b) den grad till vilken andra sektorer och undersektorer som anges i bilagan till CER-direktivet 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) verksamhetsutövarens 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, och

f) verksamhetsutövarens betydelse för upprätthållandet av en tillräcklig nivå på den samhällsviktiga tjänsten, med beaktande av tillgången till alternativa sätt för att erbjuda den samhällsviktiga tjänsten.

[18] 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.

Myndigheten för samhällsskydd och beredskap får, efter att ha gett tillsynsmyndigheterna tillfälle att yttra sig, meddela ytterligare föreskrifter om när en störande effekt enligt 2 kap. 2 § första stycket 3 är betydande.

Det tredje kriteriet för att identifieras som en kritisk verksamhetsutövare enligt artikel 6.2 c 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 i de sektorer som anges i bilaga till CER-direktivet och som är beroende av den eller de samhällsviktiga tjänsterna.

Enligt artikel 7.1 ska ett antal kriterier beaktas när det fastställs om en störande effekt är betydande. Dessa kriterier är antalet användare som är beroende av den samhällsviktiga tjänst som den berörda verksamheten tillhandahåller, den grad till vilken andra sektorer och undersektorer som anges i bilagan till CER-direktivet är beroende av den samhällsviktiga tjänsten i fråga, 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, verksamhetsutövarens marknadsandel på marknaden för den eller de berörda samhällsviktiga tjänsterna, 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 och verksamhetsutövarens betydelse för upprätthållandet av en tillräcklig nivå på den samhällsviktiga tjänsten, med beaktande av tillgången till alternativa sätt för att tillhandahålla den samhällsviktiga tjänsten.

För att underlätta tillämpningen av kriterierna som avses i artikel 7.1 och med beaktande av information som avses i artikel 7.2 ska kommissionen i samråd med gruppen för kritiska verksamhetsutövare motståndskraft anta icke-bindande riktlinjer. (artikel 7.3).

I skäl 18 anges att 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 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. Av skäl 15, som rör medlemsstaternas riskbedömning, framgår att medlemsstaternas åtgärder för att identifiera och bidra till att säkerställa kritiska verksamhetsutövares motståndskraft bör följa en riskbaserad ansats med inriktning på de verksamhetsutövare som är mest relevanta för att viktiga samhällsfunktioner och central ekonomisk verksamhet ska kunna upprätthållas.

Inledningsvis konstaterar utredningen att översättningen av artikel 6.2 c fått en utformning som skulle kunna leda till missförstånd. Den engelska språkversionen lyder ”an incident would have significant disruptive effects, as determined in accordance with Article 7(1), on the provision by the entity of one or more essential services or on the provision of other essential services in the sectors set out in the Annex that depend on that or those essential services”. Det är alltså en betydande störning på tillhandahållandet av tjänsten som avses och inte för verksamhetsutövarens verksamhet.

Detta begrepp bör för övrigt inte blandas ihop med begreppet ”betydande störning” som används i artikel 15 för att identifiera vilka incidenter som en kritisk verksamhetsutövare ska rapportera. Hur detta begrepp ska användas beskrivs närmare i avsnitt 8.3.

Enligt utredningens bedömning bör de tröskelvärden som ska tas fram för att fastställa när en störande effekt är betydande enligt artikel 7.1 bestämmas till en sådan nivå att de fastställda tröskelvärdena inte medför att samtliga verksamhetsutövare som erbjuder en samhällsviktig tjänst identifieras som kritisk verksamhetsutövare. Inriktningen enligt skäl 15 ska också vara att det är de kritiska verksamhetsutövare som är mest relevanta som ska identifieras. Utredningens bedömning avseende tröskelvärdenas nivå grundar sig även på att kritiska verksamhetsutövare genom identifieringen kommer att utgöra väsentliga verksamhetsutövare enligt 2 kap. 1 § cybersäkerhetslagen med särskilda krav på tillsyn- och efterlevnads-

kontrollåtgärder samt sanktioner enligt den lagen. Kritiska verksamhetsutövare är också undantagna från storlekskravet i 1 kap. 7 § cybersäkerhetslagen vilket får till följd att även småföretag kan komma att omfattas av cybersäkerhetslagen. Vidare kommer den nya regleringen genom kravet på bakgrundskontroller innebära ingrepp i den personliga integriteten.

Enligt 4 § lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala leverantörer, NIS-lagen, får regeringen eller den myndighet som regeringen bestämmer meddela föreskrifter om vad som avses med betydande störning enligt 3 kap. första stycket samma lag. I 4 § förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala leverantörer, NIS-förordningen, regleras vilka faktorer som ska beaktas vid bedömningen av vad som avses med en betydande störning. Vidare anges att MSB får, efter att ha gett tillsynsmyndigheterna tillfälle att yttra sig, meddela ytterligare föreskrifter om vad som avses med en betydande störning. MSB har meddelat sådana föreskrifter i myndighetens föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster (MSBFS 2024:4).

Enligt regeringens direktiv kan en motsvarande ordning vara lämplig för genomförandet av CER-direktivet.

Utredningens bedömning är att de kriterier som anges i artikel 7.1 och som ska beaktas när det fastställs om en störande effekt som avses i 2 kap. 2 § första stycket 3 är betydande ska meddelas i förordning.

Utredningen konstaterar därefter att MSB med stöd av tillsynsmyndigheterna i NIS-lagen har meddelat föreskrifter när det gäller vilka sektorsövergripande faktorer som ska beaktas vid bedömningen av vad som avses med en betydande störning enligt den lagen. I föreskrifterna anges sektorsvis vilka tröskelvärden som gäller för att en incident skulle medföra en betydande störning vid tillhandahållandet av den samhällsviktiga tjänsten. Det rör sig till exempel om antalet anställda, antalet personer till vilka tjänsten tillhandahålls eller antalet passagerare per år över en femårsperiod beroende på vilken sektor som avses.

MSB är enligt 12 § NIS-förordningen också CSIRT-enhet med bland annat uppdrag att ta emot incidentrapporter enligt NIS-lagen. MSB har genom sina uppdrag enligt NIS-lagen ett etablerat samarbete med i stort sett samtliga myndigheter som utredningen föreslår ska utses till tillsynsmyndigheter. MSB har även tagit fram en

vägledning *Lista med viktiga samhällsfunktioner – Utgångspunkt för att stärka samhällets beredskap.* Detta är ett arbete som gjorts i samråd med många myndigheter.

Utredningens bedömning är därför att MSB har den erfarenhet och kännedom om de aktuella sektorerna att myndigheten med stöd av respektive tillsynsmyndighet kan meddela ytterligare föreskrifter om när en störande effekt som avses i 2 kap. 2 § första stycket 3 är betydande. Utredningen föreslår att ytterligare bestämmelser om när en störande effekt är betydande meddelas i myndighetsföreskrift. Mot bakgrund av att föreskriften utgör en viktig förutsättning för identifieringsförfarandet bör enligt utredningens mening även syftet med CER-direktivet beaktas samt hur andra medlemsstater har fastställt dessa tröskelvärden. Vidare ser utredningen att det kan finnas skäl att inhämta synpunkter från SKR samt andra berörda branschorganisationer i arbetet med föreskriften.

Utredningens bedömning är att dessa föreskrifter kan behöva gå utöver vad regeringen eller den myndighet regeringen bestämmer kan meddela med stöd av 8 kap. 7 § regeringsformen (verkställighetsföreskrifter). Utredningen föreslår därför att det införs ett bemyndigande i den nya lagen som anger att regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om när en störande effekt enligt 2 kap. 2 § första stycket 3 är betydande.

6.5 Beslut om identifiering och underrättelse om skyldigheter

Utredningens förslag: Tillsynsmyndigheten ska genom beslut identifiera kritiska verksamhetsutövare inom sitt tillsynsområde.

Skyldigheten att göra en riskbedömning enligt 4 kap. 1 § i den föreslagna lagen börjar gälla nio månader efter den dag verksamhetsutövaren har fått del av beslutet i första stycket. Övriga skyldigheter i 4–6 kap. i den föreslagna lagen börjar gälla tio månader efter den dag verksamhetsutövaren fått del av samma beslut.

Tillsynsmyndigheten ska i sitt beslut upplysa den kritiska verksamhetsutövaren om

1. tidsfristerna som följer av 2 kap. 1 § andra stycket i den föreslagna lagen, 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.

Om tillsynsmyndigheten beslutar att en verksamhetsutövare inte längre är kritisk ska den omedelbart underrätta verksamhetsutövaren om detta.

Utredningens bedömning: Tillsynsmyndigheten ska underrätta den eller de tillsynsmyndigheter som utövar tillsyn över den kritiska verksamhetsutövaren enligt lagen om cybersäkerhet om besluten ovan.

Om den kritiska verksamhetsutövaren är verksam inom sektorerna bankverksamhet, finansmarknadsinfrastruktur eller digital infrastruktur ska underrättelsen enligt förra stycket även innehålla uppgift om att verksamhetsutövaren inte är skyldig att vidta sådana åtgärder som följer av 3–6 kap. lagen om motståndskraft hos kritiska verksamhetsutövare.

Enligt artikel 6.1 i CER-direktivet ska medlemsstaterna senast den 17 juli 2026 identifiera de kritiska verksamhetsutövarna inom de sektorer och undersektorer som anges i bilagan till direktivet.

Av artikel 6.3 och skäl 16 i CER-direktivet följer att medlemsstaterna ska underrätta en kritisk verksamhetsutövare om att den har identifierats som en sådan. Det är först efter att en sådan underrättelse har skett som skyldigheter uppstår för den kritiska verksamhetsutövaren. Underrättelsen ska ske senast en månad efter att identifieringen har skett, och skyldigheterna uppstår tio månader efter det att underrättelse har skett.

Utredningen anser att det ligger närmast till hands att låta tillsynsmyndigheten ansvara för identifiering enligt den nya lagen. Som följd bör samma myndighet, när förutsättningar föreligger, besluta om att en verksamhetsutövare är kritisk. Utredningen menar att det som i artikel 6.3 beskrivs som en underrättelse till en kritisk verksamhetsutövare bör ske genom ett beslut mot bakgrund av de skyldigheter som följer av en sådan underrättelse. En bestämmelse om

detta bör föras in i den nya lagen. Att ett sådant beslut som huvudregel ska föregås av kommunicering och en möjlighet för den kritiska verksamhetsutövaren att yttra sig följer redan av 25 § förvaltningslagen (2017:900) och behöver därför inte regleras särskilt.

Av artikel 6.3 i CER-direktivet följer att de skyldigheter som följer av direktivet ska vara tillämpliga tio månader efter att den kritiska verksamhetsutövaren tagit del av beslutet om att den identifierats som sådan. I artikel 12.1 anges vidare att utan hinder av vad som följer av artikel 6.3 ska skyldigheten att göra en riskbedömning gälla nio månader efter att den kritiska verksamhetsutövaren tagit del av samma beslut. Båda dessa frister behöver anges i den föreslagna lagen. Tillsynsmyndigheten ska även vara skyldig att upplysa om dessa frister i beslutet och en sådan bestämmelse ska följa av den föreslagna lagen.

Det bör även upplysas om att vissa bestämmelser i cybersäkerhetslagen blir tillämpliga i och med identifieringen, se avsnitt 6.6. Någon särskild bestämmelse om underrättelse om beslutets innehåll bedöms inte finnas behov av eftersom detta följer av 33 § förvaltningslagen (2017:900). Eftersom ett sådant beslut innebär skyldigheter ska beslutet gå att överklaga, se vidare avsnitt 11.9.

Utredningen anser dock inte att skyldigheten att underrätta verksamhetsutövaren inom en månad från det att identifiering har skett tillför något av materiell betydelse, och anser därför att ledet inte ska genomföras. Bedömningen grundar sig huvudsakligen på att det inte finns några uttryckliga konsekvenser av att en underrättelse inte har skett inom den angivna tiden och att skyldigheter för verksamhetsutövaren kan uppstå först efter att en underrättelse har skett, oaktat när den sker. Vidare följer redan av 9 § förvaltningslagen (2017:900) att tillsynsmyndighetens handläggning ska vara effektiv och snabb, samt att myndigheten är skyldig att så snart som möjligt underrätta en part i ett ärende om att beslut har fattats och innehållet i detsamma, se 33 § samma lag.

Av artikel 6.4 följer att medlemsstaterna ska säkerställa att deras behöriga myndigheter enligt CER-direktivet underrättar de behöriga myndigheterna enligt NIS2-direktivet. Denna underrättelse ska, i tillämpliga fall, innehålla information om att de berörda kritiska verksamhetsutövarna är verksamhetsutövare i de sektorer som anges i punkterna 3 (bankverksamhet), 4 (finansmarknadsinfrastruktur) och 8 (digital infrastruktur) i bilagan till CER-direktivet. Den ska även ange att sådana kritiska verksamhetsutövare inte har några

skyldigheter enligt kapitel III (Kritiska entiteters motståndskraft, artiklarna 12–16) och IV (Kritiska entiteter av särskild europeisk betydelse, artiklarna 17 och 18) i det direktivet. Utredningen anser att detta bör ingå i tillsynsmyndighetens uppdrag och att det ska framgå av förordningen.

Enligt artikel 6.5 är medlemsstaterna bland annat skyldiga att underrätta nya verksamhetsutövare som identifieras som kritiska. Om en verksamhetsutövare inte längre bedöms vara kritisk ska den underrättas om det i god tid och att den inte längre omfattas av skyldigheterna i kapitel III i CER-direktivet. Utredningen bedömer att två mekanismer kan utläsas ur denna del av artikeln.

Den första är en skyldighet för tillsynsmyndigheten att besluta om att en ny verksamhetsutövare är kritisk. Utredningen anser att en sådan skyldighet redan följer av den allmänna skyldigheten att besluta om att en verksamhetsutövare är kritisk och att någon ytterligare funktion därför inte behöver införas i lagen.

Den andra skyldigheten riktar sig också till den tillsynsmyndighet som ska besluta om att en verksamhetsutövare, som tidigare bedömts kritisk, inte längre bedöms vara det. Eftersom statusen som kritisk verksamhetsutövare medför betungande skyldigheter anser utredningen att det finns tungt vägande rättssäkerhetsintressen av att ett beslut om att statusen upphört ska ske omedelbart. Även detta bör följa av lagen. Följden av ett sådant beslut beror på om den identifierats som kritisk av en eller flera tillsynsmyndigheter. Om den endast identifierats som kritisk av den tillsynsmyndighet som nu gör bedömningen att den inte längre är kritisk upphör skyldigheterna enligt lagen omedelbart att gälla för verksamhetsutövaren. Skyldigheterna kvarstår emellertid om verksamhetsutövaren bedömts kritisk av fler tillsynsmyndigheter, eftersom avidentifieringen endast har verkan inom den sektor som tillsynsmyndigheten ansvarar för.

Slutligen bör båda besluten – både att en verksamhetsutövare är kritisk, och att den längre inte är det – även meddelas till den som är tillsynsmyndighet enligt cybersäkerhetslagen. Utredningen har föreslagit att tillsynsmyndigheterna enligt förslaget till cybersäkerhetslag även ska vara tillsynsmyndigheter, med motsvarande tillsynsområden, enligt lagen om motståndskraft hos kritiska verksamhetsutövare. Det går därför att ifrågasätta om en underrättelse är nödvändig att skicka till den egna myndigheten. Utredningen noterar dock att en verksamhetsutövare som omfattas av förslaget till cybersäker-

hetslag kan vara verksam inom flera olika sektorer, och att en underrättelse därför skulle kunna behöva skickas till fler än den egna myndigheten. Som följd bör en underrättelseskyldighet föreslås. En sådan underrättelse ska i förekommande fall även innehålla uppgift om att verksamhetsutövaren är undantagen från kraven enligt CER. Skyldigheten bör följa av förordning.

6.6 En kritisk verksamhetsutövare är en väsentlig verksamhetsutövare enligt cybersäkerhetslagen

Utredningens förslag: En ändring ska införas i 1 kap. 7 § cybersäkerhetslagen med följande lydelse.

Verksamhetsutövare som uppfyller kraven i 4 § med undantag för storlekskravet i 3 och som beslutats vara kritisk enligt 2 kap. 1 § lagen om motståndskraft hos kritiska verksamhetsutövare ska 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.

En ny punkt ska föras in i 2 kap. 1 § cybersäkerhetslagen med följande lydelse.

8. verksamhetsutövare som beslutats vara kritiska verksamhetsutövare enligt 2 kap. 1 § lagen om motståndskraft hos kritiska verksamhetsutövare.

Utredningens bedömning: Anmälan enligt 2 kap. 2 § cybersäkerhetslagen ska göras när verksamhetsutövaren har fått del av beslutet enligt 2 kap. 1 § lagen om motståndskraft hos kritiska verksamhetsutövare.

Av artikel 2.3 i NIS2-direktivet följer att, oavsett verksamhetsutövarens storlek, är direktivet tillämpligt på verksamhetsutövare som identifierats som kritiska verksamhetsutövare enligt artikel 6.1 i CER-direktivet.

I artikel 3.1 f i NIS2-direktivet anges vidare att verksamhetsutövare som identifierats som kritiska verksamhetsutövare enligt CER-direktivet är väsentliga.

Utredningens bedömning är att dessa verksamhetsutövare sannolikt redan omfattas av den föreslagna cybersäkerhetslagen. Bestämmelserna i NIS2-direktivet och nu i utredningens förslag innebär dock att även små företag kommer att omfattas av cybersäkerhetslagens krav. Detta medför också, som utredningens experter påpekat, att storlekskravet i NIS2-direktivet sätts ur spel för vissa verksamhetsutövare. Vidare innebär det att hela den kritiska verksamhetsutövarens verksamhet omfattas av den föreslagna cybersäkerhetslagen. Regleringen i NIS2-direktivet innebär att det bör införas en ändring i 1 kap. 7 § i förslaget till cybersäkerhetslag om att verksamhetsutövare som identifierats som kritiska enligt 2 kap. 1 § lagen om motståndskraft hos kritiska verksamhetsutövare oavsett storlek omfattas av lagen om cybersäkerhet. Utredningens bedömning är dock att en förutsättning för att omfattas av cybersäkerhetslagen är att verksamhetsutövare som beslutats vara kritiska enligt lagen om motståndskraft hos kritiska verksamhetsutövare dels bedriver verksamhet som omfattas av bilaga 1 eller 2 i NIS2-direktivet, dels uppfyller kravet på att verksamheten ska vara etablerad i Sverige. Dessa krav följer av 1 kap. 4 § 1–2 förslaget till cybersäkerhetslag som genomför artikel 2 i NIS2-direktivet. Utredningen menar att detta följer av att regleringen görs i NIS2-direktivet och att det enda undantaget från kraven i NIS2-direktivet avser storlekskravet. En annan bedömning skulle medföra komplicerade ställningstaganden kring jurisdiktion samt svårförutsägbara konsekvenser för både enskilda verksamhetsutövare och tillsynsmyndigheten. Exempelvis kan det till följd av skillnaderna i sektorer mellan direktiven kunna finnas aktörer som inte omfattas av NIS2-direktivet, men som kan identifieras enligt CER-direktivet. Sådana aktörer träffas inte av NIS2-tillsynsmyndigheternas tillsynsuppdrag. Om de däremot skulle identifieras enligt CER-direktivet och därmed bli väsentliga enligt NIS2-direktivet så skulle tillsynsansvaret enligt NIS2-direktivet utökas till att omfatta även dessa aktörer. Samma situation skulle kunna uppstå till följd av att en aktör inte bedöms vara etablerad i Sverige enligt NIS2-direktivet, men däremot uppfyller kraven för identifiering enligt CER-direktivet.

Mot bakgrund av att kritiska verksamhetsutövare som identifierats enligt CER-direktivet omfattas av cybersäkerhetslagen oavsett storlek menar utredningen att konsekvenserna för små företag måste beaktas när dessa verksamhetsutövare ska tillämpa cybersäkerhetslagen. Utredningens bedömning är, när det gäller verksamhetsutövare som inte uppfyller storlekskravet, att skyldigheterna enligt 3 kap. i förslaget till cybersäkerhetslag ska börja gälla först tio månader efter den dag verksamhetsutövaren har fått beslutet enligt 2 kap. 1 § lagen om motståndskraft hos kritiska verksamhetsutövare. Utredningen föreslår också att MSB inom ramen för sitt stödjande uppdrag särskilt bör identifiera dessa verksamhetsutövares behov av stöd.

När det gäller anmälningsskyldigheten i 2 kap. 2 § förslaget till lagen om cybersäkerhet ska anmälan göras när verksamhetsutövaren har fått del av beslutet 2 kap. 1 § lagen om motståndskraft hos kritiska verksamhetsutövare. I de fall den kritiska verksamhetsutövaren redan omfattas av cybersäkerhetslagen medför utredningens förslag inte att verksamhetsutövarens skyldigheter enligt cybersäkerhetslagen upphör att gälla i tio månader.

Utredningen föreslår vidare att det bör införas en ändring i 2 kap. 1 § förslag till lag om cybersäkerhet. Det ska införas en ny punkt 8 om att verksamhetsutövare som beslutats vara kritiska enligt 2 kap. 1 § lagen om motståndskraft hos kritiska verksamhetsutövare är väsentliga verksamhetsutövare. Det medför att bestämmelserna om tillsyn och sanktioner som gäller för väsentliga verksamhetsutövare enligt cybersäkerhetslagen ska tillämpas.

6.7 Förteckningar och information till kommissionen

Utredningens förslag: Den myndighet regeringen bestämmer ska upprätta en förteckning över kritiska verksamhetsutövare. Förteckningen ska uppdateras vid behov men minst vart fjärde år.

Utredningens bedömning: Tillsynsmyndigheten ska upprätta en förteckning över kritiska verksamhetsutövare inom sitt tillsynsområde. Av förteckningen ska framgå identiteten på den kritiska verksamhetsutövaren, antalet kritiska verksamhetsutövare som har identifierats för varje sektor och undersektor som anges i bilagan

till CER-direktivet samt antalet kritiska verksamhetsutövare för varje samhällsviktig tjänst.

Tillsynsmyndigheten ska för sitt tillsynsområde utan dröjsmål lämna förteckningen till Myndigheten för samhällsskydd och beredskap.

Myndigheten för samhällsskydd och beredskap ska upprätta en samlad förteckning över samtliga kritiska verksamhetsutövare. Av förteckningen ska framgå identiteten på den kritiska verksamhetsutövaren, antalet kritiska verksamhetsutövare som har identifierats för varje sektor och undersektor som anges i bilagan till CER-direktivet samt antalet kritiska verksamhetsutövare för varje samhällsviktig tjänst

Förteckningen ska uppdateras vid behov men minst var fjärde år.

Myndigheten för samhällsskydd och beredskap ska lämna följande information till kommissionen.

En förteckning över samhällsviktiga tjänster och om det finns ytterligare samhällsviktiga tjänster jämfört med den förteckning över samhällsviktiga tjänster som anges i kommissionens delegerade förordning[19], det antal kritiska verksamhetsutövare som har identifierats för varje sektor och undersektor som anges i bilagan till CER-direktivet och för varje samhällsviktig tjänst samt vilka föreskrivna tröskelvärden som har tillämpats.

Informationen ska lämnas utan dröjsmål och därefter när det är nödvändigt men minst vart fjärde år.

Av artikel 6.3 framgår att varje medlemsstat ska upprätta en förteckning över de kritiska verksamhetsutövare som har identifierats enligt artikel 6.2.

Enligt artikel 6.5 ska medlemsstaterna, när så är nödvändigt och minst vart fjärde år se över och när så är lämpligt, uppdatera förteckningen över identifierade kritiska verksamhetsutövare som avses i punkt 3 samma artikel.

Enligt artikel 7.2 ska varje medlemsstat, efter identifieringen av de kritiska verksamhetsutövarna enligt artikel 6.1, utan onödigt dröjsmål lämna en förteckning över samhällsviktiga tjänster i den medlemsstaten, om det finns ytterligare samhällsviktiga tjänster jämfört med

[19] 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.

den förteckning över samhällsviktiga tjänster som avses i artikel 5.1[20] och information om det antal kritiska verksamhetsutövare som har identifierats för varje sektor och undersektor som anges i bilagan till CER-direktivet och för varje samhällsviktig tjänst samt eventuella tröskelvärden som har tillämpats för att närmare fastställa ett eller flera av kriterierna för en störande effekt enligt artikel 7.1 till kommissionen.

De tröskelvärden som avses får presenteras som sådana eller i aggregerad form.

Därefter ska medlemsstaterna enligt artikel 7.2 sista stycket lämna denna information till kommissionen när så är nödvändigt och minst vart fjärde år.

Av skäl 17 framgår att 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 till CER-direktivet och för den eller de samhällsviktiga tjänster som varje entitet tillhandahåller och tröskelvärden om sådana tillämpas. 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.

Förteckningen i artikel 6.3 skiljer sig mot den förteckning över samhällsviktiga tjänster som omnämns i artikel 7.2 a. Till att börja med ska förteckningen som avses i artikel 6.3 inte delges kommissionen.[21] Den ska vidare innehålla identiteten på de kritiska verksamhetsutövare som har identifierats. Den förteckning som avses i artikel 7.2 a ska inte ange vilka verksamhetsutövare som identifierats som kritiska, utan endast vilka samhällsviktiga tjänster som identifierats. Enligt 7.2 b–c ska information lämnas om det antal kritiska verksamhetsutövare som identifierats för varje sektor och undersektor samt samhällsviktig tjänst, och eventuella tröskelvärden som har använts. En förteckning och information enligt artikel 7.2 kan således anses vara en delmängd, och upprättas av medlemsstaten med stöd av, en sådan förteckning som ska hållas enligt artikel 6.3.

[20] 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.
[21] Jfr artikel 7.2 i CER-direktivet.

Förteckning över kritiska verksamhetsutövare

Mot bakgrund av att det är tillsynsmyndigheten som beslutar om vilka verksamhetsutövare är kritiska inom sitt tillsynsområde är det enligt utredningens mening lämpligt att de även upprättar en sådan förteckning som avses i artikel 6.3 över kritiska verksamhetsutövare inom sitt tillsynsområde. Av tillsynsmyndighetens förteckning ska framgå identiteten på den kritiska verksamhetsutövaren, antalet kritiska verksamhetsutövare som har identifierats för varje sektor, undersektor som anges i bilagan till CER-direktivet samt antalet kritiska verksamhetsutövare för varje samhällsviktig tjänst. Tillsynsmyndighetens förteckning ska uppdateras vid behov men minst var fjärde år.

Av kravet på förteckning enligt artikel 6.3 följer också att det ska finnas en samlad förteckning över samtliga kritiska verksamhetsutövare som har identifierats enligt artikel 6.2. Utredningen ser också att det finns behov av en sådan samlad förteckning till exempel när det gäller stöd till de kritiska verksamhetsutövarna enligt artikel 10. En samlad förteckning ska innehålla identiteten på den kritiska verksamhetsutövaren, antalet kritiska verksamhetsutövare som har identifierats för varje sektor, undersektor som anges i bilagan till CER-direktivet samt antalet kritiska verksamhetsutövare för varje samhällsviktig tjänst.

Den samlade förteckningen ska uppdateras vid behov eller minst var fjärde år. Mot bakgrund av att utredningen föreslår att MSB ska lämna information till kommissionen enligt artikel 7.2 och MSB:s roll i övrigt bedömer utredningen att det är MSB som ska upprätta en samlad förteckning över kritiska verksamhetsutövare enligt ovan.

Utredningens förslag avseende en samlad förteckning medför att det bör införas en skyldighet för tillsynsmyndigheterna att lämna information om identiteten på den kritiska verksamhetsutövaren, antalet kritiska verksamhetsutövare som har identifierats för varje sektor och undersektor som anges i bilagan till CER-direktivet samt antalet kritiska verksamhetsutövare för varje samhällsviktig tjänst för sitt tillsynsområde till MSB. När förteckningen har uppdaterats ska tillsynsmyndigheten utan dröjsmål lämna den uppdaterade förteckningen till MSB.

När det gäller den förteckning över samhällsviktiga tjänster och information till kommissionen som avses i artikel 7.2 gör utredningen följande bedömning. Mot bakgrund av att utredningen föreslår att

MSB, efter att ha berett tillsynsmyndigheterna tillfälle att yttra sig, får meddela föreskrifter om vad som utgör en betydande störande effekt bör det också vara MSB som på lämpligt sätt lämnar den information som anges i artikel 7.2 till kommissionen.

Utredningen föreslår därför att MSB ska få i uppdrag att utan dröjsmål lämnar en förteckning över samhällsviktiga tjänster och om det finns ytterligare samhällsviktiga tjänster jämfört med den förteckning över samhällsviktiga tjänster som anges i Kommissionens delegerade förordning[22] samt lämnar information om det antal kritiska verksamhetsutövare som har identifierats för varje sektor och undersektor som anges i bilagan till CER-direktivet och för varje samhällsviktig tjänst och vilka föreskrivna tröskelvärden som har tillämpats till kommissionen.

Förteckningen ska uppdateras vid behov men minst var fjärde år. Frågan om sekretess för uppgift i en förteckning över verksamhetsutövare behandlas i avsnitt 13.4.

[22] 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.

7 Kritiska verksamhetsutövare av särskild europeisk betydelse

I detta kapitel analyseras identifiering av kritiska verksamhetsutövare av särskild europeisk betydelse enligt artikel 17 och rådgivande uppdrag enligt artikel 18. Av artikel 8 framgår att kapitel IV, Kritiska entiteter av särskild europeisk betydelse (artikel 17–18), inte är tillämpligt på kritiska verksamhetsutövare som har identifierats inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur.

I kommittédirektivet anges att utredningen ska analysera om särskilda nationella bestämmelser behövs i fråga om identifieringen och anmälan till kommissionen av kritiska verksamhetsutövare av särskild europeisk betydelse.

7.1 Inledning

Av skäl 35 och 36 i CER-direktivet framgår följande avseende kritiska verksamhetsutövare av särskild europeisk betydelse. Kritiska verksamhetsutövare bedriver 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, men vissa av dessa kritiska verksamhetsutövare 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 verksamhetsutövare av särskild europeisk betydelse. Dessa regler påverkar inte de regler om tillsyn och kontroll av efterlevnad som fastställs i CER- direktivet.

På motiverad begäran från kommissionen eller en eller flera medlemsstater till eller i vilka den samhällsviktiga tjänsten tillhanda-

hålls, och om det krävs ytterligare upplysningar för att man ska kunna ge råd till en kritisk verksamhetsutövaren avseende uppfyllandet av dess skyldigheter enligt direktivet eller för att man ska kunna bedöma huruvida en kritisk verksamhetsutövare av särskild europeisk betydelse uppfyller dessa skyldigheter, bör den medlemsstat som har identifierat en kritisk verksamhetsutövare av särskild europeisk betydelse som en kritisk verksamhetsutövare förse kommissionen med viss information i enlighet med detta direktiv. Kommissionen bör, i samförstånd med den medlemsstat som har identifierat den kritiska verksamhetsutövaren av särskild europeisk betydelse som en kritisk verksamhetsutövare, kunna anordna ett rådgivande uppdrag för att bedöma de åtgärder som den verksamhetsutövaren 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 verksamhetsutövarna av särskild europeisk betydelse har. Utan att det påverkar skyldigheten för den medlemsstat där det rådgivande uppdraget genomförs och för den berörda kritiska verksamhetsutövare att följa reglerna i direktivet, 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[1].

[1] 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).

7.2 Identifiering av kritiska verksamhetsutövare av särskild europeisk betydelse

Utredningens förslag: En kritisk verksamhetsutövare som identifierats enligt 2 kap. 1 § i den föreslagna lagen 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.

Den myndighet regeringen bestämmer ska delta i kommissionens samråd enligt artikel 17.2 i CER-direktivet.

En kritisk verksamhetsutövare som har anmält sig enligt 3 kap. 1 § i den föreslagna lagen ska delta i kommissionens samråd enligt artikel 17.2 i CER-direktivet.

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 3 kap. 5 § i den föreslagna lagen ska tillämpas från och med den dagen den kritiska verksamhetsutövaren mottagit kommissionens underrättelse.

Med begreppet kritisk verksamhetsutövare av särskild europeisk betydelse avses en kritisk verksamhetsutövare som tillhandahåller den samhällsviktiga tjänsten till eller i minst sex medlemsstater samt har mottagit en underrättelse från kommissionen om detta.

Utredningens bedömning: Tillsynsmyndigheterna ska, för sina respektive tillsynsområden, utan dröjsmål lämna uppgifter till Myndigheten för samhällsskydd och beredskap om vilka kritiska verksamhetsutövare som uppgett att de tillhandahåller samhällsviktiga tjänster till eller i minst sex medlemsstater, vilka samhällsviktiga tjänster som erbjuds samt till eller i vilka medlemsstater den kritiska verksamhetsutövaren tillhandahåller sådana tjänster.

Myndigheten för samhällsskydd och beredskap ska underrätta kommissionen om vilka kritiska verksamhetsutövare som till-

handahåller samhällsviktiga tjänster till eller i minst sex medlemsstater, vilka samhällsviktiga tjänster som tillhandahålls samt till eller i vilka medlemsstater den kritiska verksamhetsutövaren tillhandahåller sådana tjänster.

Myndigheten för samhällsskydd och beredskap ska delta i samråd enligt artikel 17.2 i CER-direktivet och informera kommissionen om tjänsten som omfattas av samrådet bedöms vara en samhällsviktig tjänst. Bedömningen ska göras i samråd med tillsynsmyndigheten.

Myndigheten för samhällsskydd och beredskap ska ta emot kommissionens underrättelse om att en kritisk verksamhetsutövare är att betrakta som kritisk verksamhetsutövare av särskild europeisk betydelse och vidarebefordra underrättelsen till tillsynsmyndigheten.

Tillsynsmyndigheten ska underrätta den kritiska verksamhetsutövaren att denna är att betrakta som kritisk verksamhetsutövare av särskild europeisk betydelse och lämna information om vilka skyldigheter som följer av att vara en kritisk verksamhetsutövare av särskild europeisk betydelse.

Enligt artikel 17 ska kritiska verksamhetsutövare av särskild europeisk betydelse identifieras. För att betraktas som en sådan verksamhetsutövare ska kraven i artikel 17.1 vara uppfyllda, nämligen att verksamhetsutövaren har identifierats som en kritisk verksamhetsutövare enligt artikel 6.1, tillhandahåller samma eller liknande samhällsviktiga tjänster till eller i minst sex medlemsstater, och har mottagit en underrättelse från kommissionen enligt artikel 17.3.

Av artikel 17.2 framgår att medlemsstaterna ska säkerställa att en kritisk verksamhetsutövare, efter den underrättelse som avses i artikel 6.3, informerar sin behöriga myndighet om att den tillhandahåller samhällsviktiga tjänster till eller i minst sex medlemsstater. I ett sådant fall ska medlemsstaterna säkerställa att den kritiska verksamhetsutövaren 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 utan dröjsmål underrätta kommissionen om identiteten på dessa kritiska verksamhetsutövare och den information de lämnat enligt denna punkt.

Kommissionen ska samråda med den behöriga myndigheten som identifierat en kritisk verksamhetsutövare som avses i artikel 17.2 första stycket, den behöriga myndigheten i andra berörda medlemsstater samt den kritiska verksamhetsutövaren i fråga. Vid detta samråd ska varje medlemsstat informera kommissionen om den bedömer att de tjänster som den kritiska verksamhetsutövaren tillhandahåller är samhällsviktiga tjänster.

Av artikel 17.3 framgår att om kommissionen, på grundval av de samråd som avses i punkt 2 i denna artikel, fastställer att den berörda kritiska verksamhetsutövaren tillhandahåller samhällsviktiga tjänster till eller i fler än sex medlemsstater, ska kommissionen underrätta den berörda verksamhetsutövaren, genom dess behöriga myndighet, om att den betraktas som en kritisk verksamhetsutövare av särskild europeisk betydelse och informera den kritiska verksamhetsutövaren om dess skyldigheter enligt kapitel IV i CER-direktivet 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 verksamhetsutövare som en kritisk verksamhetsutövare av särskild europeisk betydelse ska den behöriga myndigheten utan onödigt dröjsmål vidarebefordra den underrättelsen till den kritiska verksamhetsutövaren.

Enligt artikel 17.4 ska kapitel IV i CER-direktivet tillämpas på berörda kritiska verksamhetsutövare av särskild europeisk betydelse från och med den dagen för mottagandet av den underrättelse som avses i artikel 17.3.

Av artikel 8 framgår att kapitel IV Kritiska entiteter av särskild europeisk betydelse (artikel 17–18) inte är tillämpligt på kritiska verksamhetsutövare som har identifierats inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur.

Av 17 a § förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap framgår att MSB är Sveriges kontaktpunkt för 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. Det är också MSB som informerat kommissionen om antalet utsedda europeiska kritiska infrastrukturanläggningar enligt direktivet. Trafikverket ska vartannat år genomföra och till MSB redovisa ett identifieringsarbete av potentiella europeiska kritiska infrastrukturer inom

transportsektorn enligt direktivet.[2] När det gäller undersektorerna olja och gas enligt direktivet ska Statens energimyndighet till MSB vartannat år redovisa ett identifieringsarbete av potentiella europeiska kritiska infrastrukturer enligt direktivet.[3] Affärsverket svenska kraftnät ska vartannat år genomföra och, efter att ha hört Statens energimyndighet, till MSB redovisa ett identifieringsarbete av potentiella europeiska kritiska infrastrukturer inom undersektorn el enligt direktivet.[4] Utredningens bedömning är denna ordning är ändamålsenlig och bör överföras till den nya förordningen om motståndskraft hos kritiska verksamhetsutövare och omfatta samtliga sektorer.

Tillsynsmyndigheterna bör således få i uppdrag att utan dröjsmål till MSB redovisa vilka kritiska verksamhetsutövare som uppgett att den tillhandahåller samhällsviktiga tjänster till eller i minst sex medlemsstater och i dessa fall redovisa vilka samhällsviktiga tjänster som tillhandahålls samt till eller i vilka medlemsstater den tillhandahåller sådana tjänster.

Utredningen förslår vidare att MSB utan dröjsmål ska underrätta kommissionen om identiteten på dessa kritiska verksamhetsutövare, vilka samhällsviktiga tjänster som tillhandahålls samt till eller i vilka medlemsstater den kritiska verksamhetsutövaren tillhandahåller sådana tjänster. Detta bör regleras i förordningen.

Som framgår av avsnitt 6.5 ska tillsynsmyndigheten genom beslut identifiera kritiska verksamhetsutövare inom sitt tillsynsområde. I förfarandet för identifiering av kritiska verksamhetsutövare ingår dock inte att inhämta information om huruvida den kritiska verksamhetsutövaren tillhandahåller den samhällsviktiga tjänsten till eller i andra medlemsstater. För att kunna identifiera kritiska verksamhetsutövare av särskild europeisk betydelse behöver därför regleras hur tillsynsmyndigheten ska få denna information.

Utredningens bedömning är att den kritiska verksamhetsutövaren har denna information och att det därför ska införas en skyldighet för kritiska verksamhetsutövare att utan dröjsmål anmäla om den tillhandahåller den samhällsviktiga tjänsten till eller i minst sex medlemsstater till tillsynsmyndigheten. Av anmälan ska det framgå vilken samhällsviktig tjänst som tillhandahålls och till eller i vilka medlemsstater den tillhandahålls. Eftersom kapitel IV i CER-direk-

[2] Se 4 § 8 förordningen (2010:185) med instruktion för Trafikverket.
[3] Se 3 § 3 förordningen (2014:520) med instruktion för Statens energimyndighet.
[4] Se 3 § 13 förordningen (2007:1119) med instruktion för Affärsverket svenska kraftnät.

tivet inte ska tillämpas på kritiska verksamhetsutövare inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur ska anmälningsskyldigheten inte gälla för dessa kritiska verksamhetsutövare.

När det gäller det samråd som kommissionen ska ha med berörda behöriga myndigheter i de olika medlemsstaterna enligt artikel 17.2 andra stycket och där varje medlemsstat ska informera kommissionen om den bedömer att de tjänster som den kritiska verksamhetsutövaren tillhandahåller den medlemsstaten är samhällsviktiga tjänster är utredningens förslag att det bör ingå i MSB:s uppdrag att delta i samrådet. Även den berörda kritiska verksamhetsutövaren ska delta i samrådet vilket ska framgå av lagen. Om kommissionen på grundval av vad som framkommit i samrådet fastställer att den kritiska verksamhetsutövaren tillhandahåller samhällsviktiga tjänster till eller i fler än sex medlemsstater ska kommissionen underrätta den berörda kritiska verksamhetsutövaren om att den betraktas som en kritisk verksamhetsutövare av särskild europeisk betydelse. Underrättelsen görs lämpligtvis genom MSB som vidarebefordrar kommissionens underrättelse till tillsynsmyndigheten som i sin tur underrättar den kritiska verksamhetsutövaren och informerar verksamhetsutövaren om dess skyldigheter avseende rådgivande uppdrag och från vilken dag dessa bestämmelser ska tillämpas. MSB:s och tillsynsmyndighetens uppdrag bör framgå av förordningen.

Bestämmelsen om skyldigheter avseende rådgivande uppdrag ska tillämpas på kritiska verksamhetsutövare av särskild europeisk betydelse från och med dagen för mottagandet av kommissionens underrättelse.

Tillsynsmyndigheten ska underrätta den kritiska verksamhetsutövaren och lämna information om vilka skyldigheter som följer av att vara en kritisk verksamhetsutövare av särskild europeisk betydelse.

Det bör vidare framgå av lagens definitioner vad som avses med begreppet kritisk verksamhetsutövare av särskild europeisk betydelse.

7.3 Rådgivande uppdrag

Utredningens förslag: 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 enligt 4–6 kap. i den föreslagna lagen.

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 § i den föreslagna lagen.

Utredningens bedömning: Myndigheten för samhällsskydd och beredskap får begära att kommissionen anordnar ett rådgivande uppdrag. En sådan begäran ska ske på initiativ av den kritiska verksamhetsutövaren eller dennas tillsynsmyndighet.

Ett rådgivande uppdrag som anordnas på initiativ av kommissionen eller en annan medlemsstat får genomföras först efter samtycke av Myndigheten för samhällsskydd och beredskap. Myndigheten för samhällsskydd och beredskap ska samråda med den kritiska verksamhetsutövaren av särskild europeisk betydelse och dennas tillsynsmyndighet innan ett samtycke lämnas.

Myndigheten för samhällsskydd och beredskap ska, om begäran enligt artikel 18.3 är motiverad, tillhandahålla kommissionen information som inhämtats enligt 3 kap. 5 § lagen om motståndskraft hos kritiska verksamhetsutövare.

Tillsynsmyndigheten ska lämna uppgifter till Myndigheten för samhällsskydd och beredskap om tillsynsåtgärder, inbegripet bedömningar av efterlevnad eller beslut om förelägganden och sanktioner enligt 7 kap. 2 § och 8 kap. i den föreslagna lagen som tillsynsmyndigheten vidtagit avseende kritiska verksamhetsutövare av särskild europeisk betydelse.

Tillsynsmyndigheten ska lämna uppgifter till Myndigheten för samhällsskydd och beredskap om vilka åtgärder den kritiska verksamhetsutövaren av särskild europeisk betydelse har vidtagit enligt kommissionens yttrande enligt artikel 18.4 tredje stycket i CER-direktivet.

Myndigheten för samhällsskydd och beredskap ska lämna information till kommissionen och de medlemsstater till eller i vilka den samhällsviktiga tjänsten tillhandahålls om vilka åtgärder som vidtagits i enlighet med kommissionens yttrande enligt artikel 18.4 tredje stycket i CER-direktivet.

Myndigheten för samhällsskydd och beredskap ska lämna förslag på experter till sådana rådgivande uppdrag som kommissionen anordnar samt utfärda säkerhetsgodkännande enligt 6 kap. 7 § lagen om motståndskraft hos kritiska verksamhetsutövare för experter som ska delta i ett rådgivande uppdrag.

I artikel 18.1–2, 4, 9 och 10 finns bland annat bestämmelser om skyldighet för kommissionen att i vissa fall anordna rådgivande uppdrag och hur ett rådgivande uppdrag ska rapporteras samt bestämmelser om kommissionens yttrande till berörd medlemsstat.

Kommissionen ska enligt artikel 18.6 anta en genomförandeakt om regler för dessa förfaranden.

I artikel 18.3–4 finns även bestämmelser om medlemsstaternas delaktighet och skyldigheter vid sådan rådgivning.

I artikel 18.5 finns bestämmelser om experter i det rådgivande uppdraget, säkerhetsgodkännande av experterna samt 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 verksamhetsutövare 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.

Utredningen konstaterar att artikeln i stor utsträckning reglerar kommissionens förfaranden. Dock finns vissa artiklar som utredningen bör analysera och överväga om det finns behov av reglering i lagen eller förordningen om motståndskraft hos kritiska verksamhetsutövare.

Utredningen föreslår inledningsvis att det införs en bestämmelse i lagen som anger att syftet med ett rådgivande uppdrag är att bedöma de åtgärder som vidtagits av den kritiska verksamhetsutövaren av särskild europeisk betydelse för att uppfylla skyldigheterna enligt 4–6 kap. i den föreslagna lagen.

Begäran om och samtycke till rådgivande uppdrag

Kommissionen ska enligt artikel 18.1 på begäran av en medlemsstat som har identifierat en kritisk verksamhetsutövare av särskild europeisk betydelse anordna ett rådgivande uppdrag för att bedöma de åtgärder som den kritiska verksamhetsutövaren har infört för att uppfylla sina skyldigheter enligt kapitel III i CER-direktivet.

Behovet av ett rådgivande uppdrag bedöms lämpligen av den kritiska verksamhetsutövaren eller dess tillsynsmyndighet. Det är dessa som bäst har kunskap om den kritiska infrastrukturen och vilka åtgärder som det finns behov av att få stöd att bedöma.

Utredningens bedömning är att det är den myndighet som underrättar kommissionen om identiteten på dessa kritiska verksamhetsutövare, dvs. MSB, som ska kunna begära att kommissionen anordnar ett rådgivande uppdrag. En sådan begäran ska ha initierats av den kritiska verksamhetsutövaren eller dennas tillsynsmyndighet.

Av artikel 18.2 framgår att i de fall kommissionen eller en eller flera medlemsstater till eller i vilka den samhällsviktiga tjänsten tillhandahålls begär ett rådgivande uppdrag kan ett sådant uppdrag anordnas av kommissionen under förutsättning att den medlemsstat som har identifierat en kritisk verksamhetsutövare av särskild europeisk betydelse samtyckt till detta.

Även i detta fall är det den kritiska verksamhetsutövaren eller dess tillsynsmyndighet som kan bedöma behovet och om det är lämpligt att kommissionen anordnar ett rådgivande uppdrag. Det kan beroende på pågående tillsyn eller liknande vara lämpligt att ett rådgivande uppdrag genomförs vid en annan tidpunkt.

Utredningens bedömning är att sådant samtycke ska lämnas av MSB. MSB ska samråda med den kritiska verksamhetsutövaren och dennas tillsynsmyndighet innan samtycke lämnas.

Skyldighet att tillhandahålla information till kommissionen

I artikel 18.3 anges att 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 verksamhetsutövare av särskild europeisk betydelse som en kritisk verksamhetsutövare enligt artikel 6.1 tillhandahålla kommissionen följande:

a) Relevanta delar av riskbedömningen av kritiska verksamhetsutövare.

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 verksamhetsutövaren.

Mot bakgrund av utredningens bedömning och förslag att MSB ska underrätta kommissionen om de kritiska verksamhetsutövare som tillhandahåller samhällsviktiga till eller i minst sex medlemsstater, vilka samhällsviktiga tjänster som tillhandahålls samt till eller i vilka medlemsstater den kritiska verksamhetsutövaren tillhandahåller sådana tjänster är det utredningens bedömning att det även bör vara MSB som ansvarar för att tillhandahålla kommissionen begärda uppgifter samt bedömer om den begäran som inkommit är motiverad.

För att MSB ska få del av dessa uppgifter bör det enligt utredningens bedömning införas en bestämmelse i lagen om att en kritisk verksamhetsutövare av särskild europeisk betydelse på begäran av MSB ska tillhandahålla den information som ska tillhandahållas kommissionen, dvs. riskbedömning enligt 4 kap. 1 § lagen om motståndskraft hos kritiska verksamhetsutövare och en förteckning över relevanta åtgärder som vidtagits enligt 4 kap. 2 § samma lag. Skyldigheten att tillhandahålla informationen skulle kunna inträffa innan den tiomånadersfrist som anges i 2 kap. 1 § har löpt ut. Om detta skulle inträffa bör MSB enligt utredningens bedömning avvakta med sin begäran, eftersom någon skyldighet att vidta åtgärder ännu inte har inträtt. När det gäller punkten c) konstaterar utredningen att detta är uppgifter som tillsynsmyndigheten har. Det bör därför införas en bestämmelse i förordningen om att tillsynsmyndigheten på begäran

av MSB ska tillhandahålla uppgifter om de tillsynsåtgärder, inbegripet bedömningar av efterlevnad eller beslut om förelägganden och sanktioner enligt 7 och 8 kap. som tillsynsmyndigheten vidtagit avseende kritiska verksamhetsutövare av särskild europeisk betydelse.

Genomförande av rådgivande uppdrag

Enligt artikel 18.7 ska medlemsstaterna säkerhetsställa att kritiska verksamhetsutövare av särskild europeisk betydelse ger det rådgivande uppdraget åtkomst till uppgifter, system och anläggningar som rör erbjudandet av deras samhällsviktiga tjänster som är nödvändiga för utförandet av det berörda rådgivande uppdraget.

Utredningens bedömning är att ett rådgivande uppdrag som rör en kritisk verksamhetsutövare av särskild europeisk betydelse lämpligast sker inom ramen för en tillsyn. Det betyder att den tillsynsmyndighet som har identifierat den kritiska verksamhetsutövaren av särskild europeisk betydelse ska inleda en tillsyn när MSB har samtyckt till det rådgivande uppdraget enligt 16 § förordningen om motståndskraft hos kritiska verksamhetsutövare.

Tillsynsmyndigheten ska därför även utöva tillsyn för att genomföra ett rådgivande uppdrag. Detta ska framgå av lagen. Därmed blir också bestämmelserna i lagen om tillsynsmyndighetens undersökningsbefogenheter tillämpliga. Av detta följer att det är tillsynsmyndigheten som bedömer vilken åtkomst till uppgifter, system och anläggningar som rör den kritiska verksamhetsutövarens erbjudande av den samhällsviktiga tjänsten som är nödvändiga för utförandet det rådgivande uppdraget. Det innebär också att det inte behöver införas någon skyldighet för den kritiska verksamhetsutövaren av särskild europeisk betydelse att medverka i det rådgivande uppdraget.

Den information som ska tillhandahållas enligt ovan kan innehålla uppgifter som är sekretessbelagda och i vissa fall även säkerhetsskyddsklassificerade uppgifter. Utredningen har i kapitel 5 när det gäller säkerhetsskyddsklassificerade uppgifter och tillträde eller åtkomst till säkerhetskänslig verksamhet bedömt att uppgiftsskyldigheten i lagen om motståndskraft hos kritiska verksamhetsutövare inte gäller uppgifter som är säkerhetsskyddsklassificerade. Vidare omfattas inte tillsynsmyndighetens undersökningsbefogenheter sådana områden, lokaler eller andra utrymmen som omfattas av

säkerhetsskydd. Som en följd ska ett rådgivande uppdrag inte få utföras inom en verksamhet som är säkerhetskänslig. Detta ligger också helt i linje med artikel 18.8 som anger att det rådgivande uppdraget ska genomföras med respekt för den medlemsstatens ansvar för den nationella säkerheten och skyddet av sina säkerhetsintressen.

När det gäller uppgifter som är sekretessbelagda hänvisas till kapitel 13.

Analys av det rådgivande uppdragets rapport

När det gäller analys av de slutsatser som det rådgivande uppdraget rapporterat till kommissionen enligt artikel 18.4 andra stycket är utredningens bedömning att detta lämpligtvis görs av tillsynsmyndigheten. Detta bör framgå av bestämmelserna i förordningen om tillsynsmyndighetens uppgifter.

Även när det gäller medlemsstaternas skyldighet i artikel 18.4 fjärde stycket att säkerställa att den kritiska verksamhetsutövaren av särskild europeisk betydelse beaktar kommissionens yttrande bör det ingå i tillsynsmyndighetens uppdrag. Detta behöver inte regleras särskilt.

Tillsynsmyndigheten ska lämna uppgifter till MSB om vilka åtgärder den kritiska verksamhetsutövaren av särskild europeisk betydelse har vidtagit enligt kommissionens yttrande enligt artikel 18.4 tredje stycket i CER-direktivet. Skyldigheten att lämna information till kommissionen och de medlemsstater till eller i vilka den samhällsviktiga tjänsten tillhandahålls om vilka åtgärder som vidtagits i enlighet med yttrandet ska enligt utredningen ombesörjas av MSB. Detta bör framgå av förordningen.

Experter i det rådgivande uppdraget och säkerhetsgodkännande

Enligt artikel 18.5 ska varje rådgivande uppdrag bestå av experter från den medlemsstat där den kritiska verksamhetsutövaren 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

verksamhetsutövare av särskild europeisk betydelse som en kritisk verksamhetsutövare 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.

I CER-direktivet beskrivs inte närmare vad ett säkerhetsgodkännande avser eller vem som ska lämna ett sådant godkännande. Utredningen har tolkat kravet som att det ska ställas samma krav avseende bakgrundskontroll på deltagarna i ett rådgivande uppdrag som det ställs på de personer som har tillträde till den kritiska verksamhetsutövarens samhällsviktiga tjänst, se avsnitt 9.4.

Mot bakgrund av MSB:s uppdrag som samordnande roll mellan tillsynsmyndigheterna och deltagare i gruppen för kritiska verksamhetsutövares motståndskraft bedömer utredningen att det är MSB som ska föreslå experter till det rådgivande uppdraget samt utfärda säkerhetsgodkännande av de experter som ska delta i det rådgivande uppdraget. Utredningen ser också att det är lämpligt att i vart fall en expert kommer från berörd tillsynsmyndighet.

8 Riskbedömning, åtgärder för motståndskraft och incidentrapportering

8.1 Skyldighet att genomföra riskbedömning

Utredningens förslag: En verksamhetsutövare ska göra en riskbedömning senast nio månader efter att den har fått del av beslutet om att den har 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.

Utredningens bedömning: Tillsynsmyndigheten får inom sitt tillsynsområde meddela föreskrifter om riskbedömning. Myndigheten för samhällsskydd och beredskap ska ges tillfälle att yttra sig.

För sektorn offentlig förvaltning får Myndigheten för samhällsskydd och beredskap meddela föreskrifter om riskbedömning.

Av artikel 12.1 framgår att medlemsstaterna ska säkerställa att kritiska verksamhetsutövare gör en riskbedömning inom nio månader från mottagandet av den underrättelse som ska ske enligt artikel 6.3 (se avsnitt 6.5). Verksamhetsutövaren ska sedan göra en ny riskbedömning när det är nödvändigt och minst vart fjärde år. Det framgår av skäl 28 att verksamhetsutövarna bör göra riskbedömningar när det

är nödvändigt med hänsyn till deras specifika omständigheter och utvecklingen av riskerna, och under alla omständigheter vart fjärde år. Detta innebär enligt utredningen att riskbedömningen ska uppdateras vid behov men minst vart fjärde år. Det har framförts till utredningen av bland annat Säkerhetspolisen att riskbedömningen bör uppdateras åtminstone vartannat år. Detta är den tidsfrist som gäller för den säkerhetskyddsanalys som en verksamhetsutövare ska göra enligt 2 kap. 1 § säkerhetsskyddslagen. En verksamhetsutövares arbete med uppdateringen av riskbedömningen skulle då kunna ske samordnat och i samklang med uppdateringen av säkerhetsskyddsanalysen, för de som även bedriver säkerhetskänslig verksamhet. Utredningen instämmer i att det kan finnas synergier mellan säkerhetskyddsanalysen och riskbedömningen. Tidsgränsen på fyra år är dock en bortre gräns och bestämmelsen anger att riskbedömningen ska uppdateras vid behov. För de verksamhetsutövare som även bedriver säkerhetskänslig verksamhet kan en ny säkerhetsskyddsanalys utgöra ett sådant behov som innebär att riskbedömningen behöver uppdateras.

Riskbedömning definieras i artikel 2.7 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.

Artikel 12.1 anger att verksamhetsutövarna ska ta hänsyn till medlemsstaternas riskbedömningar (se avsnitt 6.1) och andra relevanta informationskällor, för att bedöma alla relevanta risker som kan störa tillhandahållandet av deras samhällsviktiga tjänster.

Av artikel 12.2 framgår vad en riskbedömning ska innehålla, nämligen en redogörelse för alla relevanta risker som skulle kunna leda till en incident. Detta inkluderar risker för naturolyckor och risker orsakade av människan. Artikeln nämner särskilt risker av sektorsövergripande eller gränsöverskridande slag, olyckor, naturkatastrofer, hot mot folkhälsan och hybridhot samt andra antagonistiska hot, inklusive terroristbrott. En riskbedömning ska vidare beakta om andra sektorer som omfattas av direktivet är beroende av den samhällsviktiga tjänst som erbjuds av den kritiska verksamhetsutövaren och om den kritiska verksamhetsutövaren är beroende av samhälls-

viktiga tjänster från dessa andra sektorer. Detta gäller även om dessa tjänster levereras från angränsande medlemsstater eller tredjeländer.

Slutligen anges i artikelns sista stycke att om en kritisk verksamhetsutövare har gjort andra riskbedömningar enligt andra rättsakter får den använda dessa för att uppfylla kraven enligt artikeln. Tillsynsmyndigheten får slå fast att en sådan befintlig riskbedömning helt eller delvis uppfyller skyldigheterna enligt artikeln. Detta behöver enligt utredningen inte regleras särskilt då det får anses ligga i tillsynsmyndighetens uppdrag att bedriva tillsyn att bedöma om en verksamhetsutövare har uppfyllt kraven på riskbedömning eller inte. När det gäller sektorn offentlig förvaltning så bör länsstyrelserna samverka med MSB vid en sådan bedömning eftersom MSB är föreskrivande myndighet. Inte heller detta behöver regleras särskilt eftersom det får anses följa av myndigheternas skyldighet att samverka enligt 8 § förvaltningslagen (2017:900).

Utredningen föreslår att kritiska verksamhetsutövares skyldighet att göra en riskbedömning regleras övergripande i lagen och att närmare föreskrifter om hur en riskbedömning ska göras och vad den ska innehålla bör meddelas i myndighetsföreskrifter. Ett bemyndigande ska därför föras in i den nya lagen.

Utredningen bedömer att dessa föreskrifter bör meddelas av tillsynsmyndigheten. Det ger en möjlighet att beakta eventuella sektorsspecifika risker eller informationskällor samt ta hänsyn till krav som finns enligt andra regleringar som träffar sektorn. Innan tillsynsmyndigheterna meddelar föreskrifter ska MSB ges tillfälle att yttra sig. För att hålla ihop bemyndigandet för sektorn offentlig förvaltning bör det vara MSB som meddelar eventuella föreskrifter om riskbedömning för den sektorn.

8.2 Åtgärder för motståndskraft

Utredningens förslag: 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.

Kritiska verksamhetsutövare ska utse en samverkansansvarig som utgör kontaktpunkt för berörda myndigheter.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om åtgärder och planer för motståndskraft.

Utredningens bedömning: Tillsynsmyndigheten får inom sitt tillsynsområde meddela föreskrifter om åtgärder och planer för motståndskraft. Myndigheten för samhällsskydd och beredskap ska ges tillfälle att yttra sig.

För sektorn offentlig förvaltning får Myndigheten för samhällsskydd och beredskap meddela föreskrifter om åtgärder och planer för motståndskraft.

Ett rådgivande uppdrag som anordnas för en kritisk verksamhetsutövare som inte är av särskild europeisk betydelse får anordnas endast om verksamhetsutövaren har lämnat samtycke.

Enligt artikel 13.1 ska medlemsstaterna säkerställa att kritiska verksamhetsutövare vidtar lämpliga och proportionella tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa sin motståndskraft. Av skäl 29 framgår att åtgärderna ska vara proportionella i förhållande till de risker verksamhetsutövaren ställs inför. Verksamhetsutövaren ska vid val av åtgärder ta hänsyn till medlemsstaternas riskbedömning samt resultatet av sin egen riskbedömning.

Åtgärderna ska enligt artikeln inkludera åtgärder som är nödvändiga för att

1. förhindra incidenter från att uppstå, med vederbörlig hänsyn till åtgärder för katastrofriskreducering och klimatanpassning,
2. säkerställa ett tillfredsställande fysiskt skydd av lokaler och kritisk infrastruktur, med vederbörlig hänsyn till exempelvis stängsel, barriärer, verktyg och rutiner för övervakning av områdesgränser, detektionsutrustning och åtkomstkontroller,
3. reagera på, stå emot och begränsa konsekvenserna av incidenter, med vederbörlig hänsyn till genomförandet av risk- och krishanteringsförfaranden och protokoll samt varningsrutiner,
4. återhämta sig från incidenter, med vederbörlig hänsyn till åtgärder för driftskontinuitet och identifiering av alternativa försörjningskedjor, för att återuppta tillhandahållandet av den samhällsviktiga tjänsten,
5. säkerställa 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,
6. öka medvetenheten om åtgärderna i 1–5 hos berörd personal, med vederbörlig hänsyn till utbildningskurser, informationsmaterial och övningar.

Vid tillämpningen av punkten 5 ska kritiska verksamhetsutövare beakta externa tjänsteleverantörers personal vid fastställandet av kategorier av personal som utför kritiska funktioner.

Artikeln innehåller ett flertal exempel på vad som avses med de åtgärder som beskrivs i punkterna ovan. I åtgärderna ingår exempelvis fysisk säkerhet och kontinuitetshantering. Fysisk säkerhet byggs upp genom en kombination av personal, rutiner, byggnadsteknik och säkerhetsteknik som tillsammans skapar en förmåga att upptäcka, försvåra och hantera säkerhetshotande händelser. Att åter-

hämta sig från incidenter innefattar driftskontinuitet eller kontinuitetshantering som handlar om att upprätthålla verksamheten på en tolerabel nivå vid en störning. Utredningen anser inte att alla dessa exempel ska återges i lagtext utan föreslår att åtgärderna regleras övergripande i lag och att närmare preciseringar av åtgärderna bör framgå av myndighetsföreskrifter. När det gäller bakgrundkontroller som är en del av att säkerställa ändamålsenlig hantering av personalsäkerhet så återkommer utredningen till detta i kapitel 9. Av skäl 29 framgår att åtgärderna ska vara lämpliga i förhållande till de risker verksamhetsutövaren ställs inför. Utredningen anser att detta inte behöver återges i lagtext eftersom det anges att åtgärderna ska vara proportionella i förhållande till risken. Att åtgärderna ska utgå ifrån ett allriskperspektiv följer av att riskbedömningen ska ta hänsyn till alla relevanta risker. Det har framförts till utredningen att det bör anges i lagen att verksamhetsutövarna ska bedriva ett systematiskt säkerhetsarbete. Utredningen menar att detta redan följer av de föreslagna bestämmelserna om krav på riskbedömning, att vidta åtgärder för motståndskraft och upprätta en plan för motståndskraft.

Vidare ska medlemsstaterna enligt artikel 13.2 säkerställa att kritiska verksamhetsutövare har och tillämpar en plan för motståndskraft eller ett eller flera likvärdiga dokument som beskriver de åtgärder som vidtagits för att säkerställa verksamhetsutövarens motståndskraft. Med ett eller flera likvärdiga dokument avses om kritiska verksamhetsutövare har upprättat dokument eller vidtagit åtgärder i enlighet med skyldigheter i andra rättsakter. Dessa kan då användas för att uppfylla kraven enligt CER-direktivet. Det är upp till tillsynsmyndigheten att bedöma om dessa dokument och åtgärder uppfyller skyldigheterna. Närmare föreskrifter om hur en plan för motståndskraft ska göras och vad den ska innehålla bör meddelas i myndighetsföreskrifter.

Utredningen föreslog i delbetänkandet att föreskrifter om riskhanteringsåtgärder och utbildning får meddelas av tillsynsmyndigheterna.[1] Som framgår i avsnitt 10.3 kommer det att vara samma tillsynsmyndigheter som utövar tillsyn enligt NIS2- och CER-direktiven. Det bör enligt utredningen också vara samma myndigheter som utfärdar föreskrifter om riskhanteringsåtgärder enligt NIS2-direktivet och åtgärder och planer för motståndskraft enligt CER-direktivet. På så sätt uppnås en sammanhållen reglering för de verk-

[1] SOU 2024:18 s. 227 ff.

samhetsutövare som träffas av de på båda regelverken. För sektorn offentlig förvaltning innebär det att det även för CER-direktivet bör vara MSB som får besluta om föreskrifter för sektorn. Innan tillsynsmyndigheterna meddelar föreskrifter ska MSB ges tillfälle att yttra sig.

MSB har framfört till utredningen att när det gäller de organisatoriska åtgärderna så är dessa i mycket hög utsträckning reglerade i standarden ISO 22316 och generellt tillämpbara i samtliga sektorer. För att minska fragmentering rörande hur en organisation arbetar med kontinuitetshantering med mera rekommenderar MSB därför en samlad föreskriftsrätt för de organisatoriska åtgärderna. Utredningen anser att fördelarna av en sammanhållen reglering för NIS2- och CER-direktiven väger tyngre samt att föreskriftsrätten för de olika åtgärderna inte bör separeras. Den standard MSB hänvisar till kan dock vara ett viktigt underlag när tillsynsmyndigheterna tar fram föreskrifter.

Enligt artikel 13.3 ska verksamhetsutövare utse en sambandsansvarig eller motsvarande som kontaktpunkt med de berörda myndigheterna. Det engelska uttrycket ”liaison officer” har i direktivet översatts till ”sambandsansvarig”. Skyldigheten innebär enligt utredningen att verksamhetsutövaren ska utse någon som är ansvarig för samverkan med berörda myndigheter. Att verksamhetsutövare ska utse en samverkansansvarig som kontaktpunkt för berörda myndigheter beskriver därför bättre vad skyldigheten avser. Detta ska följa av den föreslagna lagen. Innebörden av bestämmelsen bör enligt utredningen förstås som att det är en funktion för samverkan med myndigheter som ska upprätthållas. Detta innebär att den kritiska verksamhetsutövaren kan välja mellan att peka ut en specifik individ eller en funktion för att fullgöra uppgiften. Oavsett vilket val verksamhetsutövaren väljer ansvarar den dock för att upprätthålla kontinuitet för samverkansfunktionen, så att den också kan fullgöras.

Artikel 13.4 anger att kommissionen ska, på begäran av den medlemsstat som identifierat en kritisk verksamhetsutövare och med den kritiska verksamhetsutövarens samtycke, anordna rådgivande uppdrag i enlighet med vad som fastställs i artikel 18 (se avsnitt 7.3). Artikeln innebär att kommissionen ska anordna ett rådgivande uppdrag även för verksamhetsutövare som inte är av särskild europeisk betydelse om en medlemsstat begär det. En sådan begäran kräver dock verksamhetsutövarens samtycke. Det bör därför införas en

bestämmelse i förordningen som anger att ett rådgivande uppdrag som anordnas för en kritisk verksamhetsutövare som inte är av särskild europeisk betydelse får anordnas endast om verksamhetsutövaren har lämnat samtycke. I övrigt bör förfarandet följa samma process som framgår av avsnitt 7.3. Det innebär att MSB får begära att kommissionen anordnar ett rådgivande uppdrag men att en sådan begäran ska ske på initiativ av den kritiska verksamhetsutövaren eller dennas tillsynsmyndighet.

Av artikel 13.5 framgår att kommissionen ska anta icke-bindande riktlinjer för att fastställa de åtgärder som får vidtas enligt artikel 13.1. Slutligen anger artikel 13.6 att kommissionen ska anta genomförandeakter för att fastställa de nödvändiga tekniska och metodrelaterade specifikationerna för tillämpningen av åtgärderna i artikel 13.1.

Av artikel 16 framgår att medlemsstaterna ska, när det är användbart och utan att föreskriva eller gynna användningen av viss teknik, uppmuntra användningen av europeiska och internationellt erkända standarder och tekniska specifikationer som är relevanta för åtgärder för säkerhet och motståndskraft. Utredningen gjorde i delbetänkandet bedömningen att innebörden bör vara att medlemsstaterna inte kan uppställa krav om standarder och att det inte är möjligt att i lag föreskriva att standarder ska beaktas utan detta får uppmuntras på andra och frivilliga sätt.[2] Utredningen finner ingen anledning att göra en annan bedömning när det gäller den nu aktuella artikeln.

Stöd till kritiska verksamhetsutövare

Enligt artikel 10.1 ska medlemsstaterna stödja kritiska verksamhetsutövare 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 verksamhetsutövares personal. Utan att det påverkar tillämpningen av gällande regler för statligt stöd får medlemsstaterna också tillhandahålla ekonomiska resurser för kritiska verksamhetsutövare, om det är nödvändigt och av allmänt intresse.

MSB har redan i dag ett omfattade uppdrag när det handlar om att stärka samhällets förmåga att förebygga och hantera kriser. Till

[2] SOU 2024:18 s. 193.

exempel har myndigheten tagit fram en rad olika verktygslådor för att arbeta med att öka motståndskraften i samhällsviktig verksamhet. Stöden i verktygslådorna bygger på internationella standarder och andra vedertagna vägledningar. MSB bör därför få ett uppdrag av regeringen att tillsammans med tillsynsmyndigheterna se över om och hur dessa verktygslådor och annat befintligt stöd behöver anpassas och kompletteras för att kunna användas av kritiska verksamhetsutövare enligt CER-direktivet.

Utredningen föreslår också att regeringen ger Försvarshögskolan ett uppdrag att ta fram och tillhandahålla en utbildning för de som ansvarar för säkerheten hos kritiska verksamhetsutövare.

Av artikel 10.2 framgår att medlemsstaterna ska säkerställa att deras myndigheter utbyter information och god praxis med kritiska verksamhetsutövare i sektorerna. Medlemsstaterna ska också underlätta frivillig informationsdelning mellan kritiska verksamhetsutövare enligt artikel 10.3. MSB har redan i dag i uppdrag att verka för samordning mellan berörda samhällsaktörer för att förbygga och hantera kriser. Myndigheten har också en rad olika samverkansforum och upparbetade kontakter med många aktörer som kommer att omfattas av den föreslagna regleringen. Även inom beredskapssystemet sker i dag ett omfattande informationsutbyte.

Sammanfattningsvis bedömer utredningen att det inte behövs någon särskild reglering för att genomföra artikel 10 i CER-direktivet.

8.3 Incidentrapportering

Utredningens förslag: Kritiska verksamhetsutövare ska utan onödigt dröjsmål rapportera incidenter som medför eller kan medföra en betydande störning i tillhandhållandet 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.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om vad som utgör en betydande störning och om incidentrapporteringen.

Utredningens bedömning: Incidentrapportering ska göras till Myndigheten för samhällsskydd och beredskap.

Myndigheten för samhällsskydd och beredskap ska ge den kritiska verksamhetsutövaren eventuell information som skulle kunna hjälpa den kritiska verksamhetsutövaren att reagera ändamålsenligt på incidenten.

Vid bedömningen om en incident medför en betydande störning ska särskilt följande beaktas:

1. Antal och andel användare som berörs av störningen.
2. Störningens varaktighet.
3. Det geografiska område som påverkas av störningen och om området är geografiskt isolerat.

En incidentrapport ska innehålla information som är nödvändig för att förstå incidentens art, orsak och möjliga konsekvenser.

Om en incident har eller kan ha betydande påverkan på kontinuiteten i tillhandahållandet av samhällsviktiga tjänster i minst sex medlemsstater ska Myndigheten för samhällsskydd och beredskap anmäla incidenten till kommissionen.

Myndigheten för samhällsskydd och beredskap ska informera gemensamma kontaktpunkter i andra medlemsstater om en incident har eller kan ha betydande påverkan på kritiska verksamhetsutövare och kontinuiteten i tillhandahållandet av samhällsviktiga tjänster i den medlemsstaten.

Myndigheten för samhällsskydd och beredskap ska tillgängliggöra informationen i incidentrapporter utan dröjsmål för tillsynsmyndigheten.

Myndigheten för samhällsskydd och beredskap får i samband med en incident informera allmänheten.

Myndigheten för samhällsskydd och beredskap får meddela föreskrifter om vad som utgör en betydande störning och om incidentrapporteringen. Tillsynsmyndigheterna ska ges tillfälle att yttra sig.

Av artikel 15.1 framgår att kritiska verksamhetsutövare utan onödigt dröjsmål ska rapportera incidenter som medför eller kan medföra en betydande störning i tillhandahållandet av samhällsviktiga tjänster. En incident definieras i artikel 2 som varje händelse som kan medföra en betydande störning, eller som medför en störning, av tillhandahållandet av en samhällsviktig tjänst. Inledningsvis kan det noteras att kravet inte bara gäller när det inträffat en betydande störning i tillhandahållandet av en samhällsviktig tjänst utan även när en incident *kan* medföra en sådan störning. Det behöver alltså inte ha skett en störning i tillhandahållandet av tjänsten utan det är tillräckligt att en sådan kan uppstå. Dock så krävs att incidenten potentiellt kan medföra en störning i den samhällsviktiga tjänsten, dvs. det måste finnas viss sannolikhet för att en störning kan inträffa.

Verksamhetsutövaren ska rapportera incidenter utan dröjsmål vilket innebär att en första anmälan ska, om det inte är operativt omöjligt, lämnas inom 24 timmar efter det att verksamhetsutövaren fått kännedom om en incident. En detaljerad rapport ska sedan lämnas senast en månad därefter. Det framgår av skäl 33 att kravet på att lämna en första anmälan inte ska avleda den kritiska verksamhetsutövarens resurser från verksamhet som rör incidenthantering. Det framgår också att en sådan första anmälan endast bör innehålla den information som är absolut nödvändig för att göra myndigheten medveten om incidenten och för att den kritiska verksamhetsutövaren vid behov ska kunna söka hjälp. Utredningen föreslår att skyldigheten att rapportera incidenter regleras övergripande i lag och att regeringen eller den myndighet regeringen bestämmer får meddela ytterligare föreskrifter om incidentrapporteringen. Utredningen anser inte att det i lagen bör anges att verksamhetsutövaren kan avstå att rapportera inom 24 timmar om det är operativt omöjligt. En sådan reglering skulle innebära tolkningssvårigheter gällande när rapportering behöver ske inom 24 timmar och inte, samt riskera att sätta tidskravet ur spel. I stället bör den första rapporten kunna anpassas så att den bara behöver innehålla sådan mängd information som innebär att en rapportering inte inverkar negativt på verksamhetsutövarens arbete med att hantera incidenten. Det finns ett värde i att en incident rapporteras så fort som möjligt även om verksamhetsutövaren inte kan lämna fullständig information. Detta ger mottagande myndighet möjlighet att agera och att erbjuda stöd. Utredningen noterar att begreppet ”incident notification” i CER-

direktivet översatts till incidentanmälan. Utredningen föreslår att det mer vedertagna begreppet incidentrapportering används i den svenska regleringen.

Nedan följer bestämmelser i CER-direktivet som utredningen bedömer ska regleras i förordning.

För att fastställa om störningen är betydande ska enligt CER-direktivet i synnerhet följande parametrar tas i beaktande:

a) Antal och andel av användare som berörs av störningen.

b) Störningens varaktighet.

c) Det geografiska område som påverkas av störningen, med beaktande av om området är geografiskt isolerat.

Av artikel 15.1 sista stycket framgår att om en incident har eller kan ha betydande påverkan på kontinuiteten i tillhandahållandet av samhällsviktiga tjänster i minst sex medlemsstater ska incidenten anmälas till kommissionen.

Vad en incidentanmälan ska innehålla framgår av artikel 15.2. Den ska omfatta all tillgänglig information som är nödvändig för att myndigheten ska kunna förstå incidentens art, orsak och möjliga konsekvenser. Detta inkluderar information som krävs för att fastställa incidentens eventuella gränsöverskridande verkningar.

Enligt artikel 15.3 ska den myndighet som tar emot en incidentanmälan via den gemensamma kontaktpunkten informera gemensamma kontaktpunkter i andra medlemsstater som påverkas av incidenten. När den gemensamma kontaktpunkten skickar sådan information ska den behandla informationen på ett sätt som respekterar dess konfidentialitet och skyddar den berörda verksamhetsutövarens säkerhet och kommersiella intressen.

Av 15.4 framgår att behörig myndighet så snart som möjligt efter en incidentanmälan ska ge den kritiska verksamhetsutövaren relevant uppföljningsinformation, inklusive information som skulle kunna hjälpa den kritiska verksamhetsutövaren att reagera ändamålsenligt på incidenten. Slutligen ska medlemsstaten informera allmänheten om incidenten om de anser att det ligger i allmänhetens intresse.

Vem ska verksamhetsutövaren rapportera till?

Enligt utredningens delbetänkande[3] är det MSB i egenskap av CSIRT-enhet som ska ta emot incidentrapporter och erbjuda stöd när det gäller verksamhetsutövare som omfattas av NIS2-direktivet. I CER-direktivet finns ingen funktion som motsvarar CSIRT-enheten och frågan är därför till vilken myndighet som verksamhetsutövaren ska rapportera incidenter till.

De alternativ som enligt utredningen bör övervägas är om rapporteringen ska ske till tillsynsmyndigheten eller till MSB. En fördel om rapporteringen görs till MSB är att rapporteringen enligt de båda direktiven hålls samman. Detta underlättar för verksamhetsutövare som träffas av de båda regelverken i och med att de inte behöver incidentrapportera till olika myndigheter. Det innebär också att MSB har möjlighet att nyttja det digitala rapporteringsverktyg som myndigheten redan tagit fram för rapportering av incidenter enligt NIS-direktivet. Alternativet är annars att samtliga tillsynsmyndigheter behöver ta fram egna lösningar för incidentrapportering, vilket får antas vara ineffektivt. En ytterligare fördel är att MSB med en sådan ordning får en överblick över rapporteringen i samtliga sektorer både enligt CER-direktivet och NIS2-direktivet. I MSB:s uppdrag ingår operativ hantering av samhällsstörningar vid olyckor, kriser och krig. Incidentrapporter enligt CER-direktivet kan bli en viktig informationsskälla i detta arbete. Utredningen föreslår därför att det ska vara MSB som tar emot incidentrapporter enligt CER-direktivet. Därmed ska det även vara MSB som ska ge den kritiska verksamhetsutövaren eventuell information som skulle kunna hjälpa den kritiska verksamhetsutövaren att reagera ändamålsenligt på incidenten. I samband med detta kan det finnas behov av att samverka med tillsynsmyndigheten för den aktuella sektorn. Detta bedömer utredningen inte behöver regleras särskilt utan följer av 8 § förvaltningslagen (2017:900) och 6 § myndighetsförordningen (2007:515).

Utredningen föreslår också att MSB får meddela föreskrifter om vad som utgör en betydande störning och om incidentrapporteringen. Innan föreskrifterna meddelas ska MSB ge tillsynsmyndigheterna tillfälle att yttra sig.

Ett av MSB:s uppdrag är att samordna samhällets gemensamma krishanteringsarbete. I det uppdraget ingår bland annat att samordna

[3] SOU 2024:18.

de olika aktörernas kommunikation och samlade information till allmänheten. Detta görs bland annat via webbplatsen Krisinformation.se. MSB har därmed redan ett uppdrag att vid behov informera allmänheten om störningar. Av tydlighetsskäl så bör det ändå anges i förordningen att MSB kan komma att informera allmänheten i samband med att en incident rapporteras.

Incidentrapporteringen är även ett viktigt underlag för tillsynsmyndigheterna som övervakar tillämpningen av den nya lagen. MSB ska därför tillgängliggöra informationen i incidentrapporterna för den tillsynsmyndighet som ansvar för tillsyn i den sektor som incidentrapporten avser, på samma sätt som utredningen föreslog i delbetänkandet när det gäller NIS2-direktivet.

MSB bör även ansvara för att anmäla incidenter till kommissionen och gemensamma kontaktpunkter i andra medlemsstater enligt artikeln.

9 Bakgrundskontroll

9.1 Inledning

I detta kapitel analyseras CER-direktivets krav på bakgrundskontroll och hur införandet av kraven bör genomföras. Vidare analyseras kravet på säkerhetsgodkännande i artikel 18 och 19.

I artikel 14 i direktivet finns krav på bakgrundskontroller av personer som på olika sätt deltar i en kritisk verksamhetsutövares verksamhet. Artikeln anger att medlemsstaterna ska ange de villkor enligt vilka en verksamhetsutövare får ansöka om bakgrundskontroller av personer som innehar känsliga roller och som har tillgång till verksamhetsutövarens lokaler eller informationssystem eller övervägs för anställning i sådana roller och befattningar. Behovet av sådana kontroller ska styras av bland annat den riskbedömning som ska genomföras av verksamhetsutövare i syfte att uppnå en relevant motståndskraft. Bakgrundskontrollerna ska minst innefatta en identitetskontroll och relevanta uppgifter ur kriminalregistret. Riskbedömningens innehåll och syfte har behandlats i kapitel 8. Av artikel 14 följer vidare bestämmelser som tar sikte på förfarandet för bakgrundskontroller. Av artikel 13.1 i CER-direktivet följer bland annat en skyldighet för medlemsstaterna att säkerställa att kritiska verksamhetsutövare vidtar tekniska, säkerhetsmässiga och organisatoriska åtgärder för att säkerställa sin motståndskraft, inbegripet åtgärder som avser personalsäkerhet, förfarande för bakgrundskontroller samt fastställande av de kategorier av personer som måste genomgå sådana bakgrundskontroller. Vid fastställandet av kategorier av personer som ska genomgå bakgrundskontroll ska även externa tjänsteleverantörers personal beaktas. Av artikel 13.1 e framgår att verksamhetsutövarna ska säkerställa en ändamålsenlig hantering av personalsäkerheten för personal som utför kritiska funktioner, kritisk infrastruktur och känslig information. Bakgrundskontrollen har således betydelse för

åtkomsträttigheter avseende såväl fysiska lokaler och anläggningar som informationssystem. Syftet med en bakgrundskontroll är enligt artikel 14 att utvärdera en potentiell säkerhetsrisk för en kritisk verksamhetsutövare. Skälen till en bakgrundskontroll (skäl 32) är att anställda och uppdragstagare kan missbruka sina åtkomsträttigheter för skadliga ändamål och att det enligt direktivet är ett växande problem. En bakgrundskontroll ska därför vara möjlig att genomföra inför anställning i känsliga befattningar eller för personer som på annat sätt kan få tillgång till den kritiska verksamhetsutövarens lokaler eller anläggningar samt informations- eller kontrollsystem. En förutsättning är att befattningen eller deltagandet har betydelse för verksamhetens motståndskraft eller säkerhet. Enligt artikel 18.5 ska medlemmarna i det rådgivande uppdraget, när så krävs, ha ett giltigt och lämpligt säkerhetsgodkännande. I artikel 19.2 anges bland annat att gruppen ska bestå av företrädare för medlemsstaterna och kommissionen, vid behov med säkerhetsgodkännande. Utredningen ska enligt regeringens direktiv analysera hur direktivets krav på bakgrundskontroller ska genomföras i svensk rätt.

9.2 Rättsliga utgångspunkter

9.2.1 Ett system för bakgrundskontroller måste vara förenlig med regeringsformen och Europakonventionen

Av 2 kap. 6 § andra stycket regeringsformen (RF) följer att var och en är skyddad gentemot det allmänna 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 § RF är inte absolut utan får i vissa fall begränsas genom lag (se 2 kap. 20 § RF). 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. Även vissa andra villkor ska vara uppfyllda (2 kap. 21 § RF). För den som inte är svensk medborgare får särskilda begränsningar göras genom lag utan att de förutsättningar som anges i 2 kap. 21 § RF är uppfyllda (2 kap. 25 § RF).

Ett skydd mot integritetsintrång av olika slag följer även av Europakonventionen, vilken gäller som lag i Sverige.[1] I artikel 8.1 anges att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Inskränkningar i skyddet godtas bara om de har stöd i lag och om de i ett demokratiskt samhälle är nödvändiga med hänsyn till vissa uppräknade ändamål, däribland statens säkerhet, den allmänna säkerheten eller förebyggande av oordning eller brott.

Ett likartat skydd mot integritetsintrång följer av artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna (EU:s rättighetsstadga). I artikeln anges att var och en har rätt till skydd av de personuppgifter som rör honom eller henne. Personuppgifterna ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim grund. Vidare ska var och en ha rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få dem rättade. I den mån stadgan omfattar rättigheter som motsvarar sådana som garanteras av Europakonventionen ska de ha samma innebörd och räckvidd som i konventionen.

Enligt artikel 10 i allmänna dataskyddförordningen[2] får behandling av personuppgifter som rör fällande domar i brottmål med mera 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. Ett fullständigt register över fällande domar i brottmål får endast föras under kontroll av en myndighet. Av 3 kap. 8 och 9 §§ lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning följer att sådana personuppgifter som avses i artikel 10 i allmänna dataskyddsförordningen får behandlas av myndigheter, och att regeringen eller den myndighet regeringen bestämmer får meddela ytterligare föreskrifter om i vilka fall andra än myndigheter får behandla sådana uppgifter.

International Labour Organization (ILO), ett fackorgan under Förenta nationerna som utarbetar konventioner och rekommendationer på arbetslivets område, meddelade år 1996 riktlinjer angående

[1] Lagen (1994:1219) om den europeiska konventionen angående skydd för de mänskliga rättigheterna och de grundläggande friheterna. Enligt 2 kap. 19 § RF gäller vidare att lagar eller andra föreskrifter inte får meddelas i strid med Sveriges åtaganden på grund av konventionen.
[2] 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).

skydd för anställdas personuppgifter (*ILO Code on protection of workers' personal data*). Dessa riktlinjer är inte rättsligt bindande utan är avsedda som rekommendationer. Enligt dessa (avsnitt 6.1) ska personuppgifter som huvudregel i första hand inhämtas från arbetstagaren själv. Om uppgifterna hämtas in från utomstående ska arbetstagaren informeras och i förväg uttryckligen samtycka till detta. Vidare sägs bland annat att arbetsgivaren inte bör samla in personuppgifter om lagöverträdelser. Det ges dock undantag till denna rekommendation för det fall det är tillåtet enligt nationell lag och uppgifterna är relevanta för anställningen. En arbetstagare eller en arbetssökande ska dessutom i sådana fall vara skyldig att informera arbetsgivaren om domen.

Utredningen kan i denna del konstatera att det i svensk rätt finns ett starkt skydd för den personliga integriteten. Skyddet är dock inte absolut, och kan inskränkas genom lag.

9.2.2 Befintliga system för bakgrundskontroll i svensk rätt

Lagen och förordningen om belastningsregister

Uppgifter om den som dömts till påföljd för brott finns i belastningsregistret. Registret är centralt för bakgrundskontroller eftersom det innehåller en stor andel av de uppgifter som normalt anses omfattas av bakgrundskontroller i flera författningar. 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 till såväl nationella som utländska myndigheter och andra organ. Regleringen skiljer sig åt beroende på om den begärande parten är en svensk myndighet (6–8 §§), utländsk myndighet (11–14 §§), enskild som begär utdrag avseende sig själv (9 §) eller enskild som begär uppgifter om annan enskild (9 a–10 §§). Polismyndigheten ansvarar för belastningsregistret och prövar om uppgifter ska lämnas ut från det (1 § och 15 §). 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.

Skollagen

Av 2 kap. 31 § första stycket skollagen (2010:800) följer en skyldighet för den som erbjuds anställning inom skolverksamhet att visa upp ett registerutdrag. Registerutdraget ska inhämtas från det register som förs enligt lagen (1998:620) om belastningsregister. Utdraget ska visas upp för den som erbjuder anställningen, och får högst vara ett år gammalt. Den som inte visar upp ett sådant registerutdrag får inte anställas.

Av andra stycket i samma bestämmelse följer ett antal närliggande situationer där ett sådant registerutdrag ska visas upp, trots att det inte rör sig om ett sådant anställningsförhållande som avses i första stycket. Gemensamt för samtliga situationer i andra stycket är att de innebär att en individ, av andra skäl än anställning enligt första stycket, deltar i den verksamhet som ska skyddas. Av tredje stycket följer att ett sådant registerutdrag ska visas upp för den som beslutar om att anlita eller ta emot någon individ enligt andra stycket. Om detta inte skett får individen inte delta i verksamheten.

Enligt 2 kap. 32 § skollagen följer att dokumentationskrav (benämnd ”kontroll”) som träffar den verksamhet som beslutar om att anställa, anlita eller ta emot någon. Dokumentationskravet innebär att verksamheten är skyldig att anteckna att ett registerutdrag enligt 2 kap. 31 § samma lag har visats upp av en viss individ. Det anges uttryckligen att någon annan dokumentation om kontrollen inte får göras.

I 2 kap. 33 § skollagen anges ett undantag från skyldigheten att visa upp ett registerutdrag. Undantaget är tillämpligt då en individ erbjuds en förnyad anställning eller sådant deltagande som avses i 2 kap. 31 § andra stycket, inom ett år. Det anges inte i bestämmelsen från vilken tidpunkt ”inom ett år” ska beräknas. Ett sätt att tolka det på är att den tar sikte på datumet när den första anställningen ingicks. En annan tolkning är att tiden ska beräknas ett år från när utdraget från belastningsregistret utfärdades. Den förra tolkningen skulle innebära att ett utdrag som var giltigt vid första anställningstidpunkten, kan vara över ett år vid tidpunkten för den förnyade anställningen.

System som utformats på liknande sätt som skollagen

Utredningen har identifierat flera system för bakgrundskontroll vars huvuddrag påminner om det som redovisats avseende skollagen och som är av intresse.

Enligt lagen (2013:852) om registerkontroll av personer som ska arbeta med barn är en enskild på begäran skyldig att uppvisa ett utdrag ur belastningsregistret vid vissa anställningar och liknande situationer. Utdraget får vara högst ett år gammalt. Arbetsgivaren får, likt skollagen, inte dokumentera utdraget på något annat sätt än genom att anteckna att ett sådant utdrag har visats upp.

Av lagen (2007:171) om registerkontroll av personal vid vissa boenden som tar emot barn följer en skyldighet för den sökande att visa ett utdrag som både avser belastningsregistret och misstankeregistret (1 §). Detta gäller dock inte om verksamhetsutövaren själv inhämtar motsvarande utdrag (1 § tredje stycket). Ett utdrag får vara högst max sex månader gammalt, och ska överlämnas till verksamhetsutövaren för förvaring (1 § fjärde stycket). Den som erbjuds en ny anställning eller motsvarande inom sex månader behöver inte lämna nya registerutdrag (2 §). Registerutdrag (i original eller kopia) ska bevaras i minst två år från det att anställningen eller motsvarande påbörjades (3 §). Den enskilde har rätt att begära att få tillbaka utdraget i original (3 §).

I lagen (2010:479) om registerkontroll av personal som utför vissa insatser åt barn med funktionshinder finns liknande bestämmelser. Även enligt denna lag är det den som ska arbeta inom verksamheten som ska begära ut ett registerutdrag om sig själv och överlämna till arbetsgivaren (1 §). Enligt lagen får ett registerutdrag vara högst ett år gammalt (2 §), och på motsvarande sätt får arbetsgivaren underlåta att inhämta ett nytt utdrag vid återanställning inom ett år (3 §). Den enskilde har rätt att få tillbaka utdraget i original, men utdraget ska bevaras (i original eller kopia) hos verksamhetsutövaren i minst två år från det att anställningen eller motsvarande påbörjades (4 §).

Utredningen kan konstatera att skyddsintressena för de ovanstående författningarna är skyddet för barnens bästa enligt artikel 3 i barnkonventionen och att skydda elever från övergrepp.[3] Det rör sig således om skydd för individer. Dessa skyddsintressen skiljer sig

[3] FN:s konvention om barnets rättigheter samt lagen (2018:1197) om Förenta nationernas konvention om barnets rättigheter. Se vidare prop. 2020/21:152 s. 41 och 44.

markant mot vad som gäller för CER, där i stället en samhällsviktig tjänst och dess tillhandhållande ska skyddas. Utredningen bedömer att båda skyddsintressena är angelägna. Det finns därför inget hinder mot att samma system används även i lagen om motståndskraft hos kritiska verksamhetsutövare, trots att skyddsföremålen skiljer sig åt.

Vidare noterar utredningen att samtliga av de ovanstående systemen reglerar konsekvensen av att ett utdrag ur belastningsregistret inte visas upp (förbud mot anställning). Systemen synes dock inte reglera vad som händer om ett sådant utdrag visas upp, men där utdraget visar att den sökande har dömts för sådan brottslighet som är aktuell i respektive fall. Detta leder till att det inte finns något hinder mot att anställa personer som har fällts för relevant brottslighet, vilket lämnar det upp till arbetsgivaren att bedöma brottslighetens relevans för den aktuella anställningen och vad det ska anses ha för påverkan.[4]

Säkerhetsskyddslagen

Säkerhetsskyddslagen (2018:585), SäkL, gäller bland annat för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet (1 kap. 1 § första stycket). Syftet med lagen i stort är att skydda Sveriges säkerhet. Den som genom en anställning eller på något annat sätt ska delta i säkerhetskänslig verksamhet ska säkerhetsprövas (3 kap. 1 §). Syftet med säkerhetsprövningen är att klarlägga om en person kan antas vara lojalt mot de intressen som skyddas av SäkL och i övrigt pålitlig från säkerhetssynpunkt (3 kap. 2 §). Säkerhetsprövningen ska göras innan deltagandet i den säkerhetskänsliga verksamheten påbörjas och följas upp under tiden som deltagandet där pågår (3 kap. 3 §). Säkerhetsprövningen omfattar både grundutredning och registerkontroller, samt i vissa fall även en särskild personutredning. Det krävs samtycke från den som ska säkerhetsprövas för att registerkontroll och särskild personutredning ska få genomföras (3 kap. 18 §). Ansökan om registerkontroll görs av den som beslutar om placering i säkerhetsklass (5 kap. 14 § säkerhetskyddsförordningen [2021:955], SäkF). För enskilda verksamhetsutövare är det tillsynsmyndigheten som beslutar om placering i säkerhetsklass och därmed ansöker om registerkontroll. Ansvaret för säkerhetsprövning och bedömningen görs av den som beslutar

[4] Se även prop. 2006/07:37 s. 22.

om anställningen eller deltagandet i den säkerhetskänsliga verksamheten (3 kap. 4 §). Beslutet kan inte överklagas (8 kap. 4 §).

Registerkontrollerna omfattar både uppgifter ur lagen om belastningsregister och lagen (1992:621) om misstankeregister, samt vissa andra uppgifter (3 kap. 13 §). Sådana registerkontroller ska göras både inför och under deltagandet i den säkerhetskänsliga verksamheten (3 kap. 14 §). En uppgift som har kommit fram vid en registerkontroll får lämnas ut för säkerhetsprövning endast om uppgiften i det enskilda fallet kan antas ha betydelse för prövningen (3 kap. 19 §). Registerkontrolldelegationen vid Säkerhets- och integritetsskyddsnämnden prövar om en sådan uppgift ska lämnas ut för säkerhetsprövning (3 kap. 19 § andra stycket). Innan en uppgift lämnas ut ska den berörde ges tillfälle att yttra sig över uppgiften, så länge uppgiften inte omfattas av sekretess i förhållande till den enskilde enligt någon annan bestämmelse än 35 kap. 3 § OSL (3 kap. 20 § SäkL). Säkerhetspolisen ska höra Registerkontrolldelegationen innan den berörde ges tillfälle att yttra sig, om det inte är ett brådskande fall (5 kap. 18 § SäkF). Vid registerkontroll ska uppgifter löpande hämtas in under den tid deltagandet i den säkerhetskänsliga verksamheten pågår (3 kap. 14 § första stycket SäkL). Uppföljningsansvaret innebär att det ska ske en kontinuerlig bevakning av uppgifter som tillförs de register som är aktuella vid registerkontroll, s.k. spontanutfall.[5] En uppgift som efter beslut ska lämnas ut för prövning får inte åtföljas av något annat yttrande än en förtydligande kommentar till uppgiften. Det får inte framgå av svaret på en ansökan om registerkontroll att det finns någon uppgift om den kontrollerade som inte lämnas ut (5 kap. 19 § SäkF).

Det råder dock inte något förbud för en verksamhetsutövare att anställa en person som prövats och där det framkommit omständigheter av betydelse för säkerhetsprövningen.

[5] Se prop. 2017/18:89 s. 81 och 149.

Lagen och förordningen om bevakningsföretag

Enligt 4 § lagen (1974:191) om bevakningsföretag[6] ska all personal hos ett auktoriserat bevakningsföretag vara godkänd vid prövning med avseende på bland annat laglydnad och medborgerlig pålitlighet för att få vara anställd i ett sådant företag. Prövningen består i inhämtning av uppgifter om den prövade och kräver samtycke från den som ska prövas. Uppgifterna som inhämtas motsvarar de som inhämtas vid prövning mot säkerhetsklass 3 enligt SäkL (jfr 10 § förordningen [1989:149] om bevakningsföretag) och omfattar således både belastnings- och misstankeregistret samt vissa andra uppgifter. En sådan prövning om laglydnad och pålitlighet ska göras av en av sju utpekade länsstyrelser[7] (1 b § samma förordning) efter ansökan från ett bevakningsföretag (4 § nämnda lag och 9 § nämnda förordning). Ett godkännande kan återkallas (13 a § nämnda lag). Länsstyrelsens beslut får överklagas till allmän förvaltningsdomstol (15 § nämnda lag).

9.3 Ett system för bakgrundskontroll enligt CER

9.3.1 Utgångspunkter för utredningens förslag

Utredningens bedömning: Utformningen av systemet för bakgrundskontroll enligt CER-direktivet ska minimera ingreppet i den personliges integritet samtidigt som syftet med bakgrundskontrollen ska kunna uppnås.

Systemet ska utformas på ett sådant sätt att den person kontrollen avser ska begära ut uppgifter om sig själv.

Rätten att utfärda föreskrifter avseende bakgrundskontroller följer av den allmänna föreskriftsrätten avseende åtgärder för motståndskraft.

[6] Regleringen avseende ordningsvakter har i närtid setts över och reviderats (SOU 2021:38, prop. 2022/23:91 och bet. 2022/23:JuU23), men inte lett till förändringar av de här belysta bestämmelserna om bevakningsföretag.

[7] Från och med den 1 januari 2025 kommer prövningen i stället att göras av sex länsstyrelser.

Avvägningen mellan rätten till personlig integritet och de intressen som ska tillgodoses genom bakgrundskontroll

Vid all form av bakgrundskontroll aktualiseras en avvägning mellan behovet av skydd för de intressen som bakgrundskontrollen är tänkt att skydda, och den personliga integriteten hos den individ som kontrolleras. För att kunna utforma en bakgrundskontroll behöver man därför värdera båda dessa faktorer. Allmänna proportionalitetsavväganden gör också att sådana mekanismer inte ska utformas som mer ingripande än de behöver vara för att tillgodose skyddsintressena. Är skyddsintressena mycket starka, exempelvis i fråga om skyddet av Sveriges säkerhet, kan mycket ingripande kontroller anses såväl lämpliga, ändamålsenliga och proportionerliga. Vid sådana kontroller kan det vara nödvändigt att kunna vidta omfattande utredningsåtgärder, samt behandla och bevara en stor mängd personuppgifter, inklusive sådana som rör närstående till den kontrollerade. I andra fall kan individens rätt till skydd för den personliga integriteten vara den tyngst vägande faktorn, och ett sådant kontrollsystem utformas med betydligt mindre ingripande åtgärder. Av artikel 14.2 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 verksamhetsutövaren. Utredningen noterar att det inte av artikeln framgår vad det är som ska vara proportionellt vid bakgrundskontroller. Detta bör enligt utredningens tolkning ta sikte på 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 EKMR och regeringsformen som har redogjorts för i avsnitt 9.2.1. Som följd ska en bakgrundskontroll enligt CER utformas på ett sådant sätt att syftet med den uppnås med så litet ingrepp i den personliga integriteten som möjligt för den person kontrollen avser. Det kan övervägas hur pass ingripande ett sådant system bör utformas.

Utredningen anser att det finns tungt vägande intressen av att en kritisk verksamhetsutövare tillhandahåller sin samhällsviktiga tjänst. Verksamhetsutövare bör därför ges verktyg som kan bidra till tjänstens tillhandahållande. Dessa intressen är starka nog för att motivera att skyddet för den personliga integriteten hos den som erbjuds arbete hos den kritiska verksamhetsutövaren får stå tillbaka i vissa fall.

Detta gäller dock inte reservationslöst. De inskränkningar av skyddet som enligt utredningens uppfattning kan komma på fråga är sådana som är av omedelbar betydelse för att verksamhetsutövaren ska kunna bedöma den eventuella sårbarhet som den sökande utgör.

Frågan är därför vilket svenskt system som bör användas som förebild vid utformningen av CER-systemet. Ett omfattande system liknande det som återfinns inom säkerhetsskyddsregleringen ger goda förutsättningar att bedöma sårbarheter, men på bekostnad av personlig integritet hos den enskilde. Detta kan motiveras av det synnerligen betydelsefulla intresse – Sveriges säkerhet – som lagstiftningen finns till för att skydda. Lagen om motståndskraft hos kritiska verksamhetsutövare ska även den skydda betydelsefulla intressen, men enligt utredningens uppfattning når det inte upp till intresset för skyddet av Sveriges säkerhet. Detta hänger också samman med att säkerhetsskyddsregleringen föreslås ha företräde framför lagen om motståndskraft hos kritiska verksamhetsutövare (se kapitel 5). Bakgrundskontroller enligt CER ska heller inte utformas mer ingripande än vad som är nödvändigt för att uppnå syftet med kontrollen (se artikel 14.2). Detta ska enligt utredningen väga tungt vid valet av utformning av systemet för bakgrundskontroll enligt CER. Som följd bör en betydligt mindre ingripande lösning än den som gäller avseende säkerhetsskydd föreslås, och utgångspunkten bör i stället tas i systemet som finns i skollagen. Utredningen noterar dock i sammanhanget att en begränsad registerkontroll likt den som återfinns i skollagen endast kommer att kunna ha en liten påverkan på risken för infiltration, eftersom en kvalificerad antagonist kan antas undvika att använda sig av individer som förekommer i belastningsregistret.

Vem ska genomföra bakgrundskontrollen och ta fram underlag för den?

Av systematiken i artikel 14.1 följer att det är den kritiska verksamhetsutövaren som ska kunna ansöka om bakgrundskontroller av viss personal. Enligt utredningens direktiv (dir. 2023:30 s. 15) följer dock att utredningen bland annat behöver ta ställning till vem som ska ha rätt att begära ut uppgifterna, och att systemet inte ska bygga på att den kritiska verksamhetsutövaren själv begär ut uppgifterna. Utredningen anser mot denna bakgrund att det inte ingår i utredningens uppdrag att överväga en ordning där verksamhetsutövaren kan genom-

föra den delen av bakgrundskontrollen genom att begära utdrag ur belastningsregistret. Utredningen anser vidare att de två momenten i bakgrundskontrollen är så tätt förknippade att det saknas skäl att överväga andra lösningar än att det är den kritiska verksamhetsutövaren som ska kontrollera den prövades identitet. Som följd kommer utredningen endast att överväga två identifierade vägar, antingen att verksamhetsutövaren ska begära ett sådant utdrag via en tillsynsmyndighet, eller att den person kontrollen avser själv begär ut de aktuella uppgifterna.

Utredningen kan inledningsvis konstatera att de belysta systemen för bakgrundskontroll enligt svensk rätt uppvisar gemensamma drag, men skiljer sig åt avseende vad som ska skyddas och därmed också deras utformning.

Det första alternativet är att verksamhetsutövaren ansöker hos sin tillsynsmyndighet om att en bakgrundskontroll ska genomföras, och förser tillsynsmyndigheten med de uppgifter som krävs för en sådan registerslagning. Därefter kan antingen tillsynsmyndigheten genomföra bakgrundskontrollen och bedöma de uppgifter som framkommer, eller överlämna information till verksamhetsutövaren för att den ska göra motsvarande bedömning. En lösning där tillsynsmyndigheten ensam skulle både genomföra och bedöma uppgifterna i en bakgrundskontroll är enligt utredningen inte en tilltalande lösning, eftersom det är verksamhetsutövaren som är bäst lämpad att avgöra om uppgifterna påverkar den prövades lämplighet att delta i den samhällsviktiga tjänsten. En mekanism där tillsynsmyndigheten i stället lämnar ut uppgifter till verksamhetsutövaren som i sin tur gör prövningen medför också nackdelar, bland annat att insamling och behandlingen av personuppgifter sker av ytterligare en aktör, och att integritetsingreppet därmed blir större för den enskilde som bedöms. Utredningen anser att en sådan utformning är allt för ingripande i relation till skyddet för den enskildes integritet. Vidare noterar utredningen att en sådan lösning även väsentligt skulle öka den administrativa bördan på tillsynsmyndigheten. Utredningen anser vid en sammantagen bedömning att denna lösning inte är att föredra.

Den andra lösningen ansluter till den systematik som återfinns i skollagen och liknande författningar och innebär att den som ska prövas begär ut uppgifter om sig själv och visar upp, eller lämnar över, till verksamhetsutövaren för bedömning. En sådan lösning gör att den enskilde själv kan bestämma sig för att inte inhämta eller över-

lämna ett sådant utdrag till arbetsgivaren för att upprätthålla skyddet för sin personliga integritet. Vidare medför en sådan lösning att det är den berörda verksamhetsutövaren som avgör hur en uppgift i belastningsregistret kan påverka en anställning. Utredningen anser att en sådan systematik bäst ansluter sig till det tänkta systemet och utgör därför utredningens föreslagna lösning.

Rätten att utfärda föreskrifter avseende bakgrundskontroller

Bakgrundskontroller utgör en delmängd av personalsäkerheten, vilket är en åtgärd för motståndskraft enligt CER-direktivet, se vidare kapitel 8. Som följd följer föreskriftsrätten avseende bakgrundskontroller av den allmänna föreskriftsrätten avseende åtgärder för motståndskraft. Utredningen anser att det inte framkommit några skäl att föreslå en avvikande ordning för bakgrundskontroller. Detta innebär att varje tillsynsmyndighet kommer att ha möjlighet att meddela närmare bestämmelser avseende bakgrundskontrollerna. Utredningen noterar att bakgrundskontroller innehåller moment som bör vara så lika som möjligt oavsett vilken sektor en verksamhetsutövare är verksam inom, exempelvis avseende hur man ska bedöma risk för skada på den samhällsviktiga tjänsten. En sådan bedömning kommer i sin tur vara central för vilka befattningar som ska tas upp i befattningsanalysen och därmed ska genomgå bakgrundskontroll. Som följd anser utredningen att det är av särskild vikt att tillsynsmyndigheterna samverkar avseende fastställandet av sådana bedömningskriterier, i syfte att skapa gemensamma bedömningskriterier i de centrala delarna.

9.3.2 Syftet med en bakgrundskontroll

Utredningens förslag: 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.

Utredningens bedömning: Bakgrundskontrollen är inte den enda aspekten som bör vägas in vid bedömningen om en person anses lämplig.

I artikel 14 i CER-direktivet ges förutsättningar för vad som i direktivet benämns bakgrundskontroller. Utredningen konstaterar att direktivtexten inte lämnar något utrymme för medlemsstaterna att välja om detta institut ska implementeras i nationell lagstiftning eller inte, men det finns visst handlingsutrymme för dess innehåll och utformning. Utredningen noterar att begreppet bakgrundskontroll förekommer i flera författningar och i pågående utredningar.[8] Bakgrundskontroller är en företeelse som de senaste åren har haft en betydande utveckling inför rekrytering – särskilt mot bakgrund av en ökad medvetenhet hos såväl det allmänna som hos enskilda att en misslyckad rekrytering kan får stora negativa konsekvenser på en verksamhet. Bakgrundskontrollerna tillhandahålls ofta av företag som har specialiserat sig på denna tjänst och som på uppdrag – ofta vid rekrytering – genomför insamling av uppgifter om en person och gör en bedömning om vilka eventuella sårbarheter som kan föreligga. Innehållet i vad en sådan typ av formlös bakgrundskontroll omfattar är varierande. Utredningen bedömer mot denna bakgrund att bakgrundskontroll som begrepp har fått en generell betydelse i det svenska språket, låt vara inom det område som avser rekrytering och personalfrågor. Som följd kan begreppet även användas i den kontext som följer av CER-direktivets bestämmelser.

Av artikel 14.2 följer att syftet med en bakgrundskontroll är att utvärdera en potentiell säkerhetsrisk för den berörda kritiska verksamhetsutövaren. Enligt utredningens uppfattning utgör dock bakgrundskontrollen endast en formaliserad del av en större prövning där syftet är att bedöma den prövades lämplighet att delta i verksamhet där deltagandet kan orsaka skada på den samhällsviktiga tjänsten. Bakgrundskontrollen är dock nödvändig som mekanism för att den kritiska verksamhetsutövaren ska ha författningsstöd för att ta del av vissa uppgifter som den annars inte hade fått tillgång till. Utredningen anser emellertid att bakgrundskontrollen enligt CER-direktivet inte ensamt kommer kunna ge ett fullständigt underlag till stöd för en sådan bedömning. En kritisk verksamhetsutövare kommer därför att behöva väga in även annan information än den som framkommer vid bakgrundskontrollen, primärt sådant som ingår i rekryteringsförfaranden och bestående anställningsförhållanden. Detta kan exempelvis avse vad som framkommer under anställningsintervjuer, referenstagning samt validering av meriter och betyg. På motsvarande

[8] Se bl.a. *Uppdrag att förbättra bakgrundskontroller i kommunerna* (Ju 2024:A).

sätt kan uppgifter som framkommer vid bakgrundskontroll också verifiera sådana uppgifter som har framkommit under intervjuer och liknande. Som följd ska syftet med en bakgrundskontroll enligt CER-direktivet anges till att endast den som bedöms vara lämplig ska få vara anställd eller på annat sätt delta i befattningar som där deltagande kan orsaka mer än ringa skada på den samhällsviktiga tjänsten. Kravet på personalsäkerhetsåtgärder innebär bland annat att personer som inte bedöms lämpliga inte ska ges tillgång till den samhällsviktiga tjänsten. Det kan innebära att en person som inte bedömts lämplig inte får en sökt anställning eller att en redan anställd person måste omplaceras till en annan befattning alternativt få andra arbetsuppgifter.

9.3.3 Befattningsanalys utgör grunden för vilka som ska bakgrundskontrolleras

Utredningens förslag: 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.

Utredningens bedömning: En befattningsanalys är central för att identifiera vilket deltagande som ska kräva bakgrundskontroll.

Allmänna överväganden

Av artikel 13 e framgår att medlemsstaterna ska säkerställa en ändamålsenlig hantering av personalsäkerheten, vilket bland annat innefattar att de kategorier av personal som ska genomgå bakgrundskontroller ska fastställas. Givet syftet med bakgrundskontrollen som redogjorts för ovan är det centralt att en befattningsanalys tas fram, där de befattningar hos den kritiska verksamhetsutövaren som kan leda till skada på den samhällsviktiga tjänsten ska identifieras. Skyldig-

heten avser att föra en förteckning över de befattningar som innebär krav på bakgrundskontroll och kommer i det följande att benämnas *befattningsanalys*. Utredningen anser att denna skyldighet ska fullgöras av den kritiska verksamhetsutövaren.

Enligt artikel 14.1 ska bakgrundskontrollen endast ske avseende vissa typer ”känsliga roller”. Utredningen kommer i det följande att benämna sådana känsliga roller som *befattningar*. Med begreppet omfattas enligt utredningen alla typer av roller och funktioner som medför fysisk eller logisk tillgång till en kritisk verksamhetsutövares samhällsviktiga tjänst. Befattningarna avser både sådana befattningar som anställda innehar och sådana som uppdragstagare och leverantörer anlitas för att fullgöra. Analysen är således inte begränsat till den som är anställs, eller övervägs för anställning, hos den kritiska verksamhetsutövaren utan omfattar även exempelvis konsulter och underleverantörer vars deltagande ger motsvarande möjlig påverkan på den samhällsviktiga tjänsten. Det kan därför röra sig om personer som ges tillträde till lokaler där den samhällsviktiga tjänsten bedrivs, eller får åtkomst till sådana system som kan påverka den samhällsviktiga tjänsten. Det innefattar både kritisk infrastruktur och den samhällsviktiga tjänsten i sig. Verksamhetsutövaren behöver därför analysera och föra förteckning över vilka sådana befattningar, roller och funktioner i verksamheten som ska omfattas av kravet på bakgrundskontroll, samt skälen för det. Analysen ska bygga på den riskbedömning som verksamhetsutövaren ska genomföra (se kapitel 8) och på en verksamhetsbeskrivning som beskriver den samhällsviktiga tjänsten.

Befattningsanalysen ska dokumenteras och hållas uppdaterad, minst en gång om året eller i övrigt när behov uppstår. Detta gör att befattningsanalysen ska uppdateras vid förändringar som innebär att befattningar läggs till, tas bort från, eller modifieras i fråga om vilken skada de kan orsaka.

Utredningen vill framhålla att bakgrundskontroller är en av flera åtgärder för motståndskraft som kritiska verksamhetsutövare är skyldiga att vidta. Genom att vidta andra säkerhetsåtgärder, till exempel inom tillträdes- och åtkomstbegränsning, kan antalet befattningar som kan orsaka mer än ringa skada hållas så lågt som möjligt. Verksamhetsutövaren bör därför alltid överväga om verksamheten är organiserad på ett optimalt sätt utifrån skyddsbehovet och om alternativa åtgärder i stället kan användas.

Bakgrundskontroll ska endast göras för befattningar som kan orsaka mer än ringa skada på den samhällsviktiga tjänsten

En verksamhetsutövare som erbjuder en samhällsviktig tjänst – oavsett om den sker i det allmännas eller i enskild regi – har vanligtvis anställda i skilda funktioner och delverksamheter. Enbart det faktum att en verksamhetsutövare tillhandahåller en samhällsviktig tjänst innebär därför inte med automatik att alla anställda kan orsaka skada på den samhällsviktiga tjänsten. Snarare är fallet det omvända. Det är därför inte proportionerligt att samtliga befattningar hos en sådan verksamhetsutövare ska omfattas av krav på bakgrundskontroll inför och under anställning eller annat deltagande i verksamheten, till exempel för konsulter och entreprenörer.

Vidare medför en bakgrundskontroll till sin natur ett antal negativa konsekvenser som behöver beaktas vid bedömningen av skyldighetens omfattning. Innebörden av en bakgrundskontroll utvecklas nedan, men innebär i korthet att en kritisk verksamhetsutövare kan få tillgång till information från belastningsregistret och att det i samband med anställning eller motsvarande kan 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 kontrollen avser. Vidare ska uppgifternas relevans bedömas av den anställande eller anlitande verksamheten. Därutöver innebär aktiviteten som sådan innebär att tid och kostnader läggs för insamling och analys av uppgifter. Även om processen kan genomföras relativt fort innebär den med nödvändighet en försening i ett rekryteringsärende, vilket kan få negativa konsekvenser på en rekrytering. Det finns därför goda skäl att begränsa förutsättningarna när en bakgrundskontroll ska få genomföras. Utredningen anser mot denna bakgrund att bakgrundskontroll endast ska komma i fråga för deltagande som kan orsaka skada på den samhällsviktiga tjänsten.

En central punkt att bedöma i befattningsanalysen är därmed vilken skada som en person kan orsaka på den samhällsviktiga tjänsten till följd av sin befattning. En ytterligare avgränsning bör göras i fråga om befattningar där sådant deltagande som endast kan orsaka liten skada. Den mindre olägenhet som kan uppkomma genom sådana befattningar anser utredningen kunna vara hanterbara jämfört mot det intrång som en bakgrundskontroll innebär. Ett sådant kvali-

ficeringskrav gör systemet med bakgrundskontroll mer i linje med grundtanken om att det endast ska genomföras där det är nödvändigt. Det gör även att antalet personer som kan omfattas av bakgrundskontroller kan hållas lägre. Det medför i sin tur lägre administrativ börda hos verksamhetsutövarna och att färre behöver utsättas för det integritetsingrepp som bakgrundskontrollen innebär. Utredningen anser att det begrepp som ska användas är *ringa skada*, vilket ansluter till etablerad begreppsanvändning inom svensk rätt.[9] Sådant deltagande behöver inte omfattas av bakgrundskontroll, och därmed inte heller tas upp i befattningsanalysen.

9.3.4 När ska en bakgrundskontroll genomföras?

Utredningens förslag: 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.

Utredningens bedömning: Skyldigheten att genomföra bakgrundskontroll omfattar även den som har en sådan befattning vid tidpunkten när lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare träder i kraft.

Utredningen anser att artikel 14.1 ska tolkas som att den tar sikte både på de individer som vid lagstiftningens ikraftträdande redan har sådana befattningar som träffas av den kritiska verksamhetsutövarens befattningsanalys, och sådana individer som övervägs för rekrytering till sådana befattningar. Detta medför att när lagstiftningen har trätt

[9] Se 2 kap. 5 § första stycket 4 säkerhetsskyddslagen (2018:585), se vidare prop. 2017/18:89 s. 65.

i kraft ska den kritiska verksamhetsutövaren vara skyldig att genomföra bakgrundskontroll på personal som redan deltar eller övervägs att få delta i sådana befattningar som identifierats i befattningsanalysen. Som följd anser utredningen att bakgrundskontroll ska genomföras av båda dessa personalkategorier.

Utöver en sådan inledande kontroll uppstår frågan om, och i sådana fall när, en förnyad bakgrundskontroll ska göras av personal som även fortsatt deltar i verksamheten. Någon reglering av denna fråga följer inte av CER-direktivet. En möjlig tolkning av direktivet vore därför att bakgrundskontroll endast är relevant vid nyrekrytering. Utredningen anser dock att en så restriktiv tolkning inte är förenlig med CER-direktivets syfte. Som följd anser utredningen att en förnyad bakgrundskontroll även ska göras med viss periodicitet vid fortsatt deltagande. Frågan är därmed vilken periodicitet som bör föreslås. En frekvent bakgrundskontroll tillser att verksamhetsutövaren får tillgång till uppdaterad information som underlag för sin bedömning av den prövades lämplighet. Detta sker dock på bekostnad av att den administrativa bördan ökar för både verksamhetsutövaren och den person kontrollen avser. Utredningen anser att det intervall som bör övervägas är vart annat år eller en gång om året. En kontroll vartannat år framstår som det minst ingripande alternativet samtidigt som det medför relativt få försämringar för att kunna upptäcka brottslighet i jämförelse med att det görs varje år.

En sådan mekanism bör enligt utredningen kompletteras med en möjlighet för verksamhetsutövaren att genomföra en förnyad bakgrundskontroll om det framkommit skäl som föranleder det. Detta fångar upp situationer som när arbetsgivaren av andra skäl uppfattat att det kan ha uppstått sårbarheter hos den person kontrollen avser och som behöver kontrolleras närmare.

Den kritiska verksamhetsutövaren ska därför vara skyldig att genomföra bakgrundskontroll av den personal som ska delta i sådana befattningar som har identifierats i befattningsanalysen. Om sådan bakgrundskontroll inte genomförs ska det råda ett förbud att låta personen att delta i verksamhet där deltagandet kan orsaka mer än ringa skada på den samhällsviktiga tjänsten. Detta gäller både inför och under pågående anställning eller annat deltagande.

9.3.5 Bakgrundskontrollens innehåll och omfattning

Utredningens förslag: 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 en ny punkt i 9 § andra stycket 7 lagen (1998:620) om belastningsregister för verksamhetsutövaren. Utdraget får högst vara ett år gammalt vid tidpunkten för bakgrundskontrollen.

Den person kontrollen avser ska styrka sin identitet

Utredningen har att ta ställning till vilka skyldigheter som ska gälla för den som är anställd, eller övervägs för att på annat sätt delta i sådan verksamhet som omfattas av kravet på bakgrundskontroll.

Det första kravet som enligt artikel 14.3 a är att individens identitet ska kunna bekräftas. Skäl 32 anger att det för en sådan bekräftelse är lämpligt att medlemsstaterna kräver ett identitetsbevis såsom pass, nationellt identitetskort eller digitala identifieringsformer i enlighet med tillämplig rätt. Utredningen noterar att det inte finns någon legaldefinition av begreppet identitet, utan det har givits olika innebörd på olika rättsområden.[10] Utredningen bedömer dock att begreppet 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.[11] Utredningen anser att ett beviskrav för dessa omständigheter bör sättas relativt högt och ansluta till vad som används i liknande situationer i svensk rätt.[12] En sådan lösning kan även dra nytta av den praxis som finns avseende beviskravets innebörd. Som följd anser utredningen att den person kontrollen avser ska vara skyldig att *styrka sin identitet* för den kritiska verksamhetsutövaren.

[10] Jfr SOU 2023:61 s. 57.
[11] Jfr MIG 2019:18.
[12] Se exempelvis 6 § första stycket 2 passlagen (1978:302), 3 § andra stycket 3 förordningen (2005:661) om nationellt identitetskort och 2 § 2 lagen (2015:899) om identitetskort för folkbokförda i Sverige.

Vilka identitetshandlingar som kan godtas bör inte anges i lagen, utan överlämnas till regeringen att bedöma. Eftersom bakgrundskontroller är en åtgärd för motståndskraft omfattas dock frågan om godtagbara identitetshandlingar av den allmänna föreskriftsrätten som tillkommer regeringen och tillsynsmyndigheterna enligt 4 kap. 2 § tredje stycket i den föreslagna lagen och 22 § i den föreslagna förordningen. Utredningen anser att som utgångspunkt att samma typer av identitetshandlingar som godtas enligt 4 § i Skatteverkets föreskrifter (SKVFS 2009:14)[13] om identitetskort ska anses utgöra godtagbara identitetshandlingar. Dessa utgörs av

1. identitetskort utfärdat av Skatteverket
2. vanligt svenskt pass
3. svenskt nationellt identitetskort
4. svenskt körkort
5. svenskt tjänstekort utfärdat av statlig myndighet
6. SIS-märkt företagskort, tjänstekort eller identitetskort
7. EU-pass utfärdat från och med den 1 september 2006
8. pass utfärdat av Island, Liechtenstein, Norge eller Schweiz från och med den 1 september 2006, och
9. nationellt identitetskort för EU-medborgare utfärdat från och med den 2 augusti 2021.

Utredningen anser att denna lista kan komma att behöva kompletteras, särskilt i fråga om e-legitimation (jfr skäl 32). En sådan statlig e-legitimation har föreslagits av *Utredningen om säker och tillgänglig digital identitet* i SOU 2023:61 och bör beaktas vidare i den fortsatta lagstiftningsprocessen.

Identitetshandlingen i fråga ska undantagslöst vara giltig. Om den person kontrollen avser visar upp en ogiltig identitetshandling är bakgrundskontrollen i denna del inte uppfylld.

För att minimera behandlingen av personuppgifter ska den kritiska verksamhetsutövaren inte vara skyldig att bevara en kopia på den identitetshandling som har visats upp. Denne ska i stället anteckna att den som prövningen avser har styrkt sin identitet.

[13] Senaste lydelse enligt SKVFS 2021:9.

Ett begränsat utdrag ur belastningsregistret

Utredningens bedömning: Den brottslighet som omfattas av det utdrag från belastningsregistret som den sökande ska vara skyldig att hämta in om sig själv ska vara begränsad. En ny punkt ska föras in i 22 § förordningen (1999:1134) om belastningsregister med följande lydelse.

Ett registerutdrag enligt 9 § andra stycket 7 lagen (1998:620) om belastningsregister ska endast innehålla uppgifter om domar, beslut eller strafföreläggande där

1. någon annan påföljd än böter har dömts ut,
2. dagsböter har dömts ut för brott mot 3 kap. 5 §, 4 kap. 4 och 5 §§, 8, 9 och 14 kap. samt 17 kap. 1, 2 och 4 §§ brottsbalken eller lagen (2014:307) om straff för penningtvättsbrott, eller
3. böter har dömts ut för brott som avses i 6 kap. 8 och 10 §§ samt 16 kap. 11 § brottsbalken, narkotikastrafflagen (1968:64), lagen (1991:1969) om förbud mot vissa dopningsmedel, vapenlagen (1996:67), vapenförordningen (1996:70) och äldre vapenlagstiftning.

Registerutdrag bör endast inhämtas från belastningsregistret

I samtliga system som redogjorts för ovan utgör registerkontrollen en central åtgärd. Det bör dock noteras att en registerkontroll aldrig kan utgöra en garanti för att olämpliga personer hindras från att delta i verksamhet. En registerkontroll minskar dock risken för att sådana olämpliga personer anställs i verksamheten utan att sådan brottslighet kommer till arbetsgivarens kännedom. Utredningen anser därför att en registerkontroll bör vara central även vid utformningen av en bakgrundskontroll enligt CER.

Inom exempelvis säkerhetsskyddslagstiftningen kompletteras i många fall utdraget ur belastningsregistret även med att ett utdrag ur misstankeregistret[14] inhämtas. Utredningen anser dock inte att utdraget enligt CER även bör omfatta misstankeregistret. Bedömningen grundar sig huvudsakligen i två delar: dels att intrånget i den

[14] Se lagen (1998:621) om misstankeregister.

enskildes personliga integritet ska begränsas så långt som möjligt,[15] dels att utdrag ur misstankeregistret kan leda till skönsmässiga bedömningar kring den enskildes lämplighet. Därtill bör det noteras att misstankeregistret även kan innehålla uppgifter om misstanke som inte delgivits den enskilde, vilket vore direkt olämpligt att låta den enskilde få inhämta om sig själv. Om en kritisk verksamhetsutövare får kännedom om att den sökande har delgivits misstanke om brott, men där misstanken inte har lett till fällande dom är det oklart vad det förväntade agerandet från verksamhetsutövaren bör vara. Utredningen anser att utdrag från misstankeregistret inte ska ingå i bakgrundskontrollen enligt CER.

Utdraget ur belastningsregistret ska begränsas

Ett utdrag som begärs av en enskild ska begränsas så att omfattningen är tillräckligt stor för att syftet med kontrollen ska kunna tillgodoses, samtidigt som ingrepp i den personliga integriteten ska vara så liten som möjligt. Enligt 9 § lagen (1998:620) om belastningsregister har en enskild rätt att begära ett skriftligt utdrag av samtliga uppgifter som finns i registret. Ett sådant utdrag kan därför komma att innehålla uppgifter som saknar betydelse för verksamhetsutövarens bakgrundskontroll. Utredningen anser att ett sådant utdrag vore allt för omfattande i relation till de skyddsintressen som bakgrundskontrollen är tänkt att tillgodose. Det bör därför skapas förutsättningar för den enskilde att begära ut särskilt utdrag där endast viss utpekad brottslighet redovisas. I dag finns sådana system för flera andra typer av utdrag ur belastningsregistret.[16] Utredningen anser att uppgifterna i det aktuella utdraget behöver kunna ge verksamhetsutövaren ett bra underlag för bakgrundskontrollen samtidigt som inte onödigt många uppgifter lämnas ut. Utredningens förslag är därför 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.[17] Dessa uppgifter kan typiskt sett vara relevanta för att bedöma en persons lämplighet att

[15] Se motsvarande bedömning i prop. 2004/05:133 s. 68.
[16] Se 9 § andra stycket lagen (1998:620) om belastningsregister och 22 § och 22 a § förordningen (1999:1134) om belastningsregister.
[17] Se 9 § andra stycket 1 lagen (1998:620) om belastningsregister och 22 § första och andra stycket förordningen (1999:1134) om belastningsregister.

delta i verksamhet där deltagandet kan orsaka mer än ringa skada på den samhällsviktiga tjänsten. En ny punkt om detta bör därför införas i 9 § lagen om belastningsregister med en korresponderande förteckning över uppgifter i en ny bestämmelse i 22 § förordningen (1999:1134) om belastningsregister. Utredningen anser dock att eftersom förteckningen som föreslås är densamma som redan i dag anges i 22 § första stycket bör den bestämmelsen lagtekniskt kompletteras med en hänvisning till den föreslagna CER-grunden för utdrag i 9 § lagen om belastningsregister.

Enligt utredningens mening finns det, i likhet med vad som gäller enligt skollagen, anledning att införa ett krav på att utdraget får vara högst ett år gammalt vid uppvisandet.

Sammanfattningsvis ska den person kontrollen avser alltså vara skyldig att visa upp giltig och godtagbar legitimation samt inhämta och visa upp ett särskilt utdrag ur belastningsregistret i enlighet med vad som redogjorts för ovan. Brister i någon del av detta kan komma att ha stor påverkan på om, och i sådana fall vilken befattning, den prövade kan få delta i hos den kritiska verksamhetsutövaren.[18] För att underlätta för den enskilde bör dock skyldigheterna gälla först vid förfrågan från den kritiska verksamhetsutövaren.

Vad ska den kritiska verksamhetsutövaren bedöma?

Den kritiska verksamhetsutövaren ska utifrån det uppvisade underlaget bedöma om den person kontrollen avser är lämplig att delta i verksamhet där deltagandet kan orsaka mer än ringa skada på den samhällsviktiga tjänsten. Genom den föreslagna konstruktionen kommer registerutdraget endast att avse viss brottslighet och påföljder. Som följd kan utdraget endast utgöra en delmängd av den fullständiga prövning som den kritiska verksamhetsutövaren ska göra av en persons lämplighet. Det finns enligt utredningens mening varken grund för slutsatsen att förekomst i belastningsregistret alltid innebär att man är olämplig, eller att en brist på förekomst innebär att man alltid är lämplig. Utdragets riktighet bör i fall när det inhämtats

[18] Utredningen noterar särskilt den pågående *Utredningen om en förbättrad process för säkerhetsprövningar* (Ju 2023:11). Utredningen har bland annat i uppgift att överväga vilka uppgifter som ska ingå i underlaget vid en säkerhetsprövning, bedöma om det bör finnas en möjlighet överklaga ett säkerhetsprövningsbeslut och analysera vilka ytterligare möjligheter som bör finnas att stänga av en statligt anställd när denne inte längre godkänns vid säkerhetsprövningen.

digitalt även kontrolleras digitalt hos Polismyndigheten.[19] Analysen av utdragets eventuella innehåll och innebörd behöver i stället göras av verksamhetsutövaren utifrån annan tillgänglig information, och verksamhetsutövaren kan komma att behöva ställa uppföljande frågor kopplat till utdraget under en eventuell intervju för att kartlägga eventuella sårbarheter och dess påverkan på individens lämplighet, se vidare avsnitt 9.3.2 ovan. 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. Som följd ska ett beslut om lämplighet att få eller fortsätta delta i viss befattning endast kunna angripas med de arbetsrättsliga regelverken, och därför inte överklagas med stöd av den föreslagna lagen om motståndskraft hos kritiska verksamhetsutövare.

Krav på dokumentation och bevarande

Utredningens förslag: Vid bakgrundskontroll ska den kritiska verksamhetsutövaren anteckna om den person kontrollen avser har visat upp giltig och godtagbar identitetshandling, samt ett särskilt utdrag ur belastningsregistret.

Anteckningar enligt första stycket ska bevaras i två år från tidpunkten för bakgrundskontrollen.

Verksamhetsutövaren ska vara skyldig att genomföra de två kontroller som avses, samt dokumentera att kontroll har skett. I båda fallen bygger de på att den person kontrollen avser – efter förfrågan från verksamhetsutövaren – visar upp godkänd och giltig identitetshandling respektive utdrag från belastningsregistret, att dessa granskas av verksamhetsutövaren och att anteckning om att sådana har visats upp görs. Avseende identitetskontrollen har utredningen ovan bedömt vilka identitetshandshandlingar som ska kunna vara godtagbara. Kontrollen i denna del består därför av att säkerställa att identitetshandlingen är av godkänd typ och därtill att den är giltig. Avseende utdraget ur belastningsregistret avser kontrollen att rätt form av intyg har inhämtats, och att det inte är äldre än ett år gammalt vid

[19] Se Polismyndighetens *Kontrolltjänst för digitala registerutdrag* tillgänglig på https://polisen.se/tjanster-tillstand/belastningsregistret/kontrolltjanst-for-digitala-registerutdrag/, hämtad 2024-06-12.

tidpunkten för granskningen. Utdragets äkthet kan även kontrolleras. Bedömningen om det eventuella innehållet i utdraget kan anses påverka den prövades lämplighet ska dock inte överprövas av någon tillsynsmyndighet, utan kravet för verksamhetsutövaren är att denne ska anteckna att ett utdrag från belastningsregistret har uppvisats.

Frågan är därefter vilken reglering som bör föreslås avseende bevarandet av de anteckningar som har visats upp. Offentliga verksamhetsutövare är skyldiga att registrera och bevara handlingar enligt offentlighets- och sekretesslagen (2009:400) och arkivlagen (1990:782). De registerutdrag som har lämnats till en aktör som har att tillämpa de författningarna är således redan reglerade och kräver ingen vidare åtgärd. Avseende enskilda verksamhetsutövare som inte träffas av regleringen behöver en bortre gräns för bevarande anges. Utredningen har bedömt att en förnyad bakgrundskontroll för den som är anställd ska göras vartannat år. Det har inte framkommit några skäl till att registeranteckningen skulle behöva bevaras längre än samma tid. Bevarandekravet bör därför anges till två år.

Underlåtelse att anteckna att identitetshandling och utdrag ur belastningsregistret har uppvisats innebär att det saknas skriftlig bevisning om att det har skett. Utevaron av sådana anteckningar bör därför presumeras innebära att någon bakgrundskontroll inte har skett, och därmed ska tillsynsmyndigheten ingripa. Samma slutsats gäller avseende att sådana anteckningar inte bevaras under den angivna tiden. Överträdelser av dessa skyldigheter ska därför kunna angripas med sanktioner, se vidare i kapitel 11.

9.3.6 Sammanfattning

Den kritiska verksamhetsutövaren har flera skyldigheter avseende bakgrundskontroll. Den initiala handlar om att analysera och dokumentera vilka befattningar och annat deltagande som kan orsaka mer än ringa skada på den samhällsviktiga tjänsten. Analysen ska dokumenteras i en befattningsanalys, som ska hållas uppdaterad. Bakgrundskontroll ska därefter genomföras på den personal som deltar eller kan komma att delta i sådana befattningar som framkommer av befattningsanalysen. Kravet gäller således både vid rekryteringar och pågående anställningar. Bakgrundskontrollen syftar till att bedöma om personen är lämplig att delta i sådan befattning. Om en person inte

bedöms lämplig vid rekrytering får den inte anställas i den aktuella befattningen, men det finns inte hinder mot att personen anställs i annan befattning. På motsvarande sätt kan en person som redan är anställd och som vid bakgrundskontroll inte längre bedöms lämplig omplaceras till annan befattning med stöd av arbetsledningsrätten. Den föreslagna regleringen ger bland annat författningsstöd för genomförande av bakgrundskontroll, samt att neka individer deltagande i vissa befattningar om de inte bedöms lämpliga.

Själva bakgrundskontrollen består dels av kontroll av personens identitetshandling som ska vara giltig och godtagbar, dels av kontroll av ett begränsat utdrag ur belastningsregistret. Att sådan kontroll har skett ska antecknas och anteckningarna ska bevaras.

9.4 Säkerhetsgodkännande enligt CER

Utredningens förslag: Ett säkerhetsgodkännande enligt CER-direktivet ska ha samma innebörd som en bakgrundskontroll enligt den föreslagna lagen.

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.

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.

Utredningens bedömning: Myndigheten för samhällsskydd och beredskap får utfärda säkerhetsgodkännande för experter i ett rådgivande uppdrag enligt 3 kap. 4 § den föreslagna lagen.

I CER-direktivet förekommer begreppet *säkerhetsgodkännande* i artiklarna 18.5 och 19.2 samt skäl 37. I skäl 37 anges bland annat att avseende *gruppen för kritiska entiteters motståndskraft* (CERG)[20] bör medlemsstaterna sträva efter att säkerställa att de utsedda företrädarna från deras behöriga myndigheter i gruppen för kritiska entiteters mot-

[20] Se vidare avsnitt 12.3.

ståndskraft samarbetar ändamålsenligt och effektivt, inbegripet genom att när så är lämpligt utse företrädare med säkerhetsgodkännande.

CERG behandlas vidare i artikel 19 där det i artikel 19.2 bland annat anges att gruppen ska bestå av företrädare för medlemsstaterna och kommissionen, vid behov med säkerhetsgodkännande. Utredningen noterar att det inte nämns något behov av säkerhetsgodkännande för den övriga krets av möjliga deltagare i CERG som nämns i artikel 19.2 (”andra berörda parter” respektive ”experter från Europaparlamentet”). Utredningen tolkar skrivningen restriktivt som att säkerhetgodkännande endast ska kunna omfatta företrädare för medlemsstaterna i denna del.

Avseende rådgivande uppdrag enligt artikel 18 anges i artikel 18.5 att medlemmarna i det rådgivande uppdraget ska när så krävs ha ett giltigt och lämpligt säkerhetsgodkännande. Sverige kan bli behörig att föreslå experter till det rådgivande uppdraget, vilket har redogjorts för i avsnitt 7.3. Sådana experter behöver därför kunna omfattas av ett säkerhetsgodkännande.

Utredningen kan konstatera att innebörden av begreppet *säkerhetsgodkännande* inte förklaras i direktivet och behöver därför tolkas av utredningen.[21] Vidare anges inte vad syftet med säkerhetsgodkännandet är, vilket försvårar tolkningen. Säkerhetsgodkännande saknar entydig innebörd inom svensk rätt och kan ta sikte på godkännande av exempelvis it-system, säkerhetsprodukter eller personal.[22] Utredningen anser dock att den mest närliggande tolkningen är att CER-direktivet tar sikte på personalsäkerhetsperspektivet.

I den engelska språkversionen av direktivet används begreppet *security clearance*.[23] Utredningen anser att den etablerade översättningen av det engelska begreppet *security clearance* i personalsäkerhetssammanhang är *säkerhetsklarering*.[24] 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.[25] Utredningen kan dock inte med säkerhet säga att det deltagande som CER-direktivet

[21] Det är vidare oklart om skrivningarna har bäring på den typ av deltagande som bland annat behandlas i förslaget till Europaparlamentets och rådets förordning om informationssäkerhet i unionens institutioner, organ och byråer COM(2022) 119, se vidare Regeringskansliets faktapromemoria 2021/22:FPM78.
[22] SOU 2021:63 s. 151, 297 och 307.
[23] Jfr artikel 18.5, 19.2 och skäl 37.
[24] Se prop. 2017/18:89 s. 76 och SOU 2015:25 s. 45, 120 och 567.
[25] Se 5 kap. 1 § säkerhetsskyddslagen (2018:585).

har bäring på säkerhetskänslig verksamhet eller verksamhet som är i behov 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 omnämnas i CER-direktivet.

Utredningen anser därför i stället att systemet för säkerhetsgodkännande ska likställas med systemet för bakgrundskontroll. Som följd ska det i lagen anges att ett säkerhetsgodkännande ska anses ha samma innebörd som en bakgrundskontroll enligt den föreslagna lagen. Utifrån skrivningarna i artiklarna 18.5 och 19.2 anser utredningen att möjligheten att utfärda ett säkerhetsgodkännande ska göras fakultativ. Det ska således vara upp till den beslutande aktören att avgöra om ett säkerhetsgodkännande är nödvändigt för deltagande.

Avseende deltagande i ett rådgivande uppdrag enligt artikel 18 har utredningen föreslagit (se avsnitt 7.3) att MSB ska få föreslå experter för sådant deltagande. Det faller sig därför naturligt att det är MSB som i sådana situationer ska ha möjlighet att utfärda säkerhetsgodkännande. MSB har till utredningen angett att det vore bättre om processen för säkerhetsgodkännande enligt CER inte genomfördes som en bakgrundskontroll, utan att aktuella individer i stället borde säkerhetsprövas enligt SäkL samt att prövningen skulle kunna ske på samma sätt som gäller för säkerhetsklass 3. Utredningen konstaterar att säkerhetsprövning enligt SäkL är ett betydligt mer omfattande och ingripande verktyg i jämförelse med den typ av bakgrundskontroll som avses i CER-direktivet. Det finns därför inte finns skäl att likställa processen för säkerhetsgodkännande med säkerhetsprövning enligt SäkL. Vidare konstaterar utredningen att den föreslagna lagen är subsidiär till SäkL, och att det inte finns hinder mot att en viss befattning kan vara föremål för bakgrundskontroll enligt CER och samtidigt placerad i säkerhetsklass med säkerhetsprövning enligt SäkL som följd.

Rörande deltagande i gruppen för kritiska entiteters motståndskraft föreslås regeringen (se avsnitt 12.3) fatta beslut om sådant deltagande. Som följd bör regeringen vara ensamt behörig att utfärda säkerhetsgodkännande för sådant deltagande.

9.5 Processen för registerkontroll och närliggande frågor

9.5.1 Slagningar mot vissa system och tidsfrister

Av artikel 14.3 följer att medlemsstaterna är skyldiga att tillse att de bakgrundskontroller som genomförs med stöd av direktivet ska använda vissa system. Dessa system är Ecris[26] och i förekommande och tillämpliga fall Ecris-TCN[27] avseende tredjelandsmedborgare. Utredningens förslag på system innebär att en den prövade själv ska inhämta ett utdrag ur belastningsregistret om sig själv, med stöd av 9 § andra stycket lagen om belastningsregister. En sådan ordning innebär redan att en slagning mot Ecris ska göras.[28] Något författningsförslag behöver därför inte lämnas för att uppfylla direktivets krav i denna del.

Rörande slagning mot Ecris-TCN finns svenska bestämmelser i lagen (2022:733) med kompletterande bestämmelser till EU:s förordning om Ecris-TCN. Även där (3 § samt 6 §) finns en rätt för enskilda att få en slagning genomförd mot systemet om sökningen avser en enskild som begär uppgifter om sig själv.[29] Det bör dock noteras att lagen med kompletterande bestämmelser till EU:s förordning om Ecris-TCN ännu inte har trätt i kraft, utan detta ska ske vid den tidpunkt regeringen bestämmer. Utredningen anser att den av utredningen föreslagna mekanismen även kan anses uppfylla kravet på slagning mot Ecris-TCN från den tidpunkten lagen trätt i kraft.

Av artikel 14.3 i CER-direktivet följer vissa tidsfrister som hänvisar till rambeslutet för Ecris respektive EU:s förordning om Ecris-TCN. De tidsfrister som anges i CER-direktivet är enligt utredningens bedömning en redogörelse för vad som följer av Ecris-regelverken. Utredningen noterar att tidskravet på att besvara en begäran enligt artikel 8.1 i rambeslut 2009/315/RIF i sin tur hänvisar till artikel 6.1 i samma rambeslut. Den senare artikeln reglerar situationer som inte

[26] Europeiska 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, Celex 32009F0315).
[27] 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.
[28] 22 c § förordningen (1999:1134) om belastningsregister, se vidare prop. 2021/22:172 s. 45 f. och Ds 2011:15 s. 70 f.
[29] Se vidare prop. 2021/22:172 s. 33 och 70.

innebär att en person begär ut information om sig själv. Sådana situationer regleras i stället av artikel 6.2–3 och innebär enligt artikel 8.2 en längre svarsfrist på 20 dagar från mottagandet av en begäran. Utredningens nu föreslagna system bygger som sagt på att en enskild begär ett utdrag om sig själv, och således inte på att en myndighet eller kritisk verksamhetsutövare har rätt att begära ett utdrag. Denna lösning gör att den längre svarsfristen om 20 dagar ska tillämpas på sådana utdrag. Att Polismyndigheten, i egenskap av att vara utpekad centralmyndighet i Sverige, dock har att beakta den kortare tidsfristen vid en begäran som inkommer från en annan medlemsstat följer dock redan av Ecris-regelverken. De i CER-direktivet angivna tidsfristerna kräver enligt utredningen därför ingen vidare lagstiftningsåtgärd.

9.5.2 Utländska myndigheters tillgång till uppgifter vid motsvarande bakgrundskontroller enligt CER

Utredningens förslag: Ett nytt stycke med följande lydelse ska tillföras 12 a § lagen om belastningsregister.

Trots att motsvarande rätt saknas för en svensk myndighet 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.

I 12 a § lagen om belastningsregister finns en begränsning i när uppgifter i registret får lämnas ut till en utländsk myndighet som gjort en framställan med stöd av med stöd av rådets rambeslut 2009/315/RIF för annat än brottmålsförfaranden. För att utlämnande ska få ske krävs att motsvarande rätt att få del av uppgifterna finns för en svensk myndighet (reciprocitetskrav). Utlämnande av uppgifter med stöd av CER-direktivet är inte en del av ett brottmålsförfarande, och begränsningen är därför tillämplig på sådana utlämnanden.[30] Genom den konstruktion utredningen föreslår där det i Sverige är den enskilde som begär ett utdrag om sig själv saknas en sådan motsvarande rätt för en svensk myndighet att begära ut samma uppgifter. Detta medför att svensk rätt skulle utgöra ett hinder mot att dela med sig

[30] Jfr prop. 2011/12:163 s. 57 f.

av uppgifter till en annan medlemsstat som gör en sådan framställan till följd av CER-direktivet. Det svenska genomförandet av direktivet skulle därför, om ingen åtgärd vidtas, innebära problem för det inomeuropeiska informationsutbyte som förutsätts. Utredningen anser därför att ett undantag behöver införas i anslutning till lagen om belastningsregister med innebörden att reciprocitetskravet i 12 a § första stycket inte ska utgöra ett hinder mot att lämna ut uppgifter ur registret efter en begäran från en annan medlemsstat om begäran görs med stöd av CER-direktivet.

9.6 Behandling av personuppgifter kopplade till bakgrundskontroller enligt CER

Utredningens bedömning: Det är inte nödvändigt att föreslå någon särskild reglering gällande behandling av personuppgifter som rör lagöverträdelser.

Skyldigheten för enskilda kritiska verksamhetsutövare att göra anteckningar om uppvisande av identitetshandlingar och registerutdrag medför att deras behandling av personuppgifter är tillåten såsom nödvändig för att fullgöra en rättslig förpliktelse.

Enligt artikel 10 i dataskyddsförordningen får behandling av personuppgifter som rör bland annat fällande domar i brottmål endast utföras under kontroll av myndighet eller när behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder för de registrerades rättigheter och friheter fastställs. Utredningens förslag är att bakgrundskontrollen ska dokumenteras genom en anteckning om att identitetskontroll har gjorts och att utdraget ur belastningsregistret har visats upp. Någon annan dokumentation ska inte få göras. De föreslagna bestämmelserna medger inte att verksamhetsutövaren sparar uppgifter om innehållet i utdraget. Att den som gör kontrollen tar del av innehållet i registerutdraget och antecknar att ett registerutdrag visas upp utan att något om innehållet i utdraget noteras innebär enligt utredningen inte en behandling av uppgifter om lagöverträdelser enligt artikel 10 i dataskyddsförordningen. Någon särskild reglering gällande behandling av personuppgifter som rör lagöverträdelser är därför inte nödvändig. Anteckningen om att kontrollen har genomförts utgör dock en

personuppgiftsbehandling om den personen kontrollen rör. Om en sådan anteckning förs elektroniskt eller är avsedd att ingå i ett register krävs att denna personuppgiftsbehandling har stöd i dataskyddsförordningen för att vara tillåten. För behandling av personuppgifter gäller de allmänna principer som anges i artikel 5 i dataskyddsförordningen och för att behandlingen ska vara laglig krävs det också att det finns en rättslig grund för behandlingen enligt artikel 6 i förordningen. I de fall det sker en personuppgiftsbehandling om att ett registerutdrag har visats upp, och den sker i syfte att fullgöra den föreslagna skyldigheten enligt den föreslagna lagen, kan personuppgiftsbehandlingen ske med stöd av den rättsliga grunden rättslig förpliktelse i artikel 6.1 c i förordningen. Syftet med behandlingen är fastställt i nationell rätt. Syftet med den föreslagna regleringen är att bedöma den enskildes lämplighet. Det är uppgifter om innehållet i registerutdraget som kan vara integritetskänsliga och som bör skyddas från spridning. Den anteckning som ska göras får inte innehålla något om innehållet i registerutdraget. Att en anteckning görs om att ett registerutdrag som krävs enligt lag har visats upp bedöms vara ett mycket marginellt intrång i den personliga integriteten. Den föreslagna regleringen bedöms därför vara proportionerlig. Samma slutsats gäller för de anteckningar om uppvisande av identitetshandlingar (se avsnitt 9.3.5) som verksamhetsutövare är skyldiga att göra och bevara.

10 Tillsyn

10.1 Inledning

Av artikel 9 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, efterlevnadskontroll av direktivet på nationell nivå. Vidare följer av artikeln att för sektorerna bankverksamhet och finansmarknadsinfrastruktur ska detta i princip vara samma myndigheter som avses i artikel 46 i Dora-förordningen. När det gäller sektorn digital infrastruktur så ska det i princip vara samma myndigheter som enligt NIS2-direktivet. Medlemsstaterna får dock utse andra myndigheter i enlighet med befintliga nationella ramar.

I kommittédirektivet anges att det är en naturlig utgångspunkt att samma myndighet som utövar tillsyn över en viss verksamhetsutövare enligt NIS2-direktivet även gör detta enligt CER-direktivet.

10.2 System för tillsyn

Utredningens förslag: Den myndighet som regeringen bestämmer ska vara tillsynsmyndighet.

Utredningens bedömning: Det ska finnas en eller flera tillsynsmyndigheter för varje sektor som utövar tillsyn.

I delbetänkandet föreslår utredningen att det utses en tillsynsmyndighet för varje sektor vid implementeringen av NIS2-direktivet. I kommittédirektivet anges att det bör vara samma tillsynsmyndigheter för NIS2- och CER-direktiven. Med hänsyn till detta är det utredningens förslag att systemet för tillsyn för CER-direktivet följer den struktur som föreslås för NIS2-direktivets genomförande

i Sverige. Den myndighet som regeringen bestämmer ska därför vara tillsynsmyndighet och det ska finnas en eller flera tillsynsmyndigheter för varje sektor.

10.3 Tillsynsmyndigheter i Sverige

Utredningens bedömning: Följande myndigheter ska vara tillsynsmyndigheter för respektive sektor:

- Statens energimyndighet för sektorn energi,
- Transportstyrelsen för sektorn transport,
- Finansinspektionen för sektorerna bankverksamhet och finansmarknadsinfrastruktur,
- Inspektionen för vård och omsorg för del av sektorn hälso- och sjukvård,
- Läkemedelsverket för del av sektorn hälso- och sjukvård,
- Livsmedelsverket för sektorerna dricksvatten, avloppsvatten samt produktion, bearbetning och distribution av livsmedel,
- Post- och telestyrelsen för sektorerna digital infrastruktur och rymden,
- Länsstyrelserna i Stockholms, Skåne, Västra Götalands och Norrbottens län för sektorn offentlig förvaltning

Som framgår ovan är det utredningens utgångspunkt att det ska vara samma myndighet som utövar tillsyn över en viss verksamhetsutövare enligt NIS2-direktivet och enligt CER-direktivet. Det kan dock finnas anledning att göra avsteg från denna princip, till exempel om det är stor skillnad på vilka verksamhetsutövare som omfattas av sektorerna enligt de båda direktiven. Utredningen föreslår nedan vilka myndigheter som ska utöva tillsyn över vilka sektorer.

10.3.1 Energi

Sektorn energi omfattar samma undersektorer och kategorier av verksamhetsutövare som i NIS2-direktivet med den skillnaden att laddningsoperatörer som har ansvar för förvaltning och drift av en laddningspunkt inte omfattas av CER-direktivet. Statens energimyndighet är tillsynsmyndighet för sektorn när det gäller NIS2-direktivet enligt utredningens förslag i delbetänkandet. Statens energimyndighet bör därför även ansvara för tillsyn av sektorn när det gäller CER-direktivet.

10.3.2 Transport

Sektorn transport omfattar samma undersektorer och kategorier av verksamhetsutövare som i NIS2-direktivet med den skillnaden att även undersektorn kollektivtrafik omfattas av CER-direktivet. Transportstyrelsen är tillsynsmyndighet för sektorn när det gäller NIS2-direktivet enligt utredningens förslag. Myndigheten utför också tillsyn enligt lagen (2010:1065) och den anslutande förordningen (2011:1126) om kollektivtrafik. Transportstyrelsen bör därför ansvara för tillsyn av sektorn även när det gäller CER-direktivet.

10.3.3 Bankverksamhet och finansmarknadsinfrastruktur

Direktivets bestämmelser gäller i mycket begränsad utsträckning för kritiska verksamhetsutövare inom sektorerna bankverksamhet och finansmarknadsinfrastruktur, se avsnitt 5.3.2. Sektorerna omfattar samma kategorier av verksamhetsutövare som i NIS2-direktivet. Det anges även i CER-direktivets artikel 9 att det i princip ska vara samma myndigheter som avses i artikel 46 i Dora-förordningen som ansvarar för sektorerna. Finansinspektionen är tillsynsmyndighet för sektorerna när det gäller NIS2-direktivet enligt utredningens förslag. Det är också Finansinspektionen som avses i artikel 46 i Dora-förordningen. Finansinspektionen bör därför ansvara för sektorerna även när det gäller CER-direktivet.

10.3.4 Hälso- och sjukvård

Sektorn hälso- och sjukvård omfattar samma undersektorer och kategorier av verksamhetsutövare som i NIS2-direktivet med den skillnaden att även verksamhetsutövare med tillstånd att bedriva partihandel med läkemedel omfattas. Enligt utredningens förslag när det gäller NIS2-direktivet så är IVO tillsynsmyndighet för vårdgivare och Läkemedelsverket tillsynsmyndighet för resterande del av sektorn. Läkemedelsverket utfärdar partihandelstillstånd till handlare som har förutsättningar för att uppfylla de krav som finns på handeln. Läkemedelsverket är också tillsynsmyndighet enligt lagen (2009:366) om handel med läkemedel.

Utredningen föreslår att IVO ska vara tillsynsmyndighet för vårdgivare i sektorn och att Läkemedelsverket ska vara tillsynsmyndighet för resterande kategorier av verksamhetsutövare i sektorn.

10.3.5 Dricksvatten och avloppsvatten

Sektorerna omfattar samma kategorier av verksamhetsutövare som i NIS2-direktivet. Livsmedelsverket är tillsynsmyndighet när det gäller NIS2-direktivet för sektorerna enligt utredningens förslag. Livsmedelsverket bör därför ansvara för sektorerna även när det gäller CER-direktivet.

Naturvårdsverket har framfört till utredningen att tillsynsansvaret för avloppsvatten bör placeras på antingen Naturvårdsverket eller länsstyrelserna och framfört bland annat följande. Naturvårdsverket är den centrala myndighet som har kunskap och kompetens avseende frågor som berör avloppsvatten. Detta var en av anledningarna till att myndigheten blev beredskapsmyndighet. Om tillsynsansvaret placeras på Livsmedelsverket kommer Naturvårdsverkets roll enligt beredskapsförordningen att reduceras inom sektorn avlopp. Avseende länsstyrelserna har de olika typer av uppgifter som berör såväl miljörätt som beredskap och säkerhetsskydd. Länsstyrelserna har ett tillsynsansvar i enlighet med miljöbalken gentemot avloppsreningsverken och vissa utpekade länsstyrelser har miljöprövningsdelegationer där avloppsreningsverken tillståndsprövas och meddelas miljörättsliga villkor för sin verksamhet.

Som framgått i avsnitt 6.2.1 ser utredningen ett stort värde i att i framtiden se över CER-regleringens koppling till det svenska bered-

skapssystemet, och då möjligheten att ensa så väl begrepp som sektorer som träffas av olika regelverk. Vid en sådan översyn finns även möjligheten att samordna myndighetsansvar enligt de olika regelverken. När det gäller utredningens nuvarande uppdrag så bedömer utredningen att samordningen mellan NIS2- och CER-regleringen väger tyngre än samordning med övrig reglering. Det innebär att tillsynsansvar enligt NIS2- och CER-regleringen i vissa sektorer kan komma att placeras på en annan myndighet en den som är ansvarig enligt beredskapssystemet.

10.3.6 Digital infrastruktur

Direktivets bestämmelser gäller i mycket begränsad utsträckning för kritiska verksamhetsutövare inom sektorn digital infrastruktur, se avsnitt 5.3. Sektorn omfattar samma kategorier av verksamhetsutövare som i NIS2-direktivet. Det anges även i CER-direktivets artikel 9 att det i princip ska vara samma myndigheter som ansvarar för tillsyn av sektorn som enligt NIS2-direktivet. PTS är tillsynsmyndighet för sektorn när det gäller NIS2-direktivet enligt utredningens förslag. PTS bör därför ansvara för sektorn även när det gäller CER-direktivet.

10.3.7 Offentlig förvaltning

Sektorn offentlig förvaltning omfattar endast offentliga förvaltningsentiteter hos nationella regeringar så som de definieras av en medlemsstat i enlighet med nationell rätt. Det innebär att det endast är statliga myndigheter som kan komma att omfattas i sektorn. Det är alltså en relativt stor skillnad mellan sektorn offentlig förvaltning enligt CER- och NIS2-direktiven. Med anledning av detta behöver det analyseras om det bör vara samma myndigheter som ansvarar för tillsyn i sektorn offentlig förvaltning enligt respektive regelverk.

Utredningen föreslog i delbetänkandet att tillsyn över offentlig förvaltning enligt NIS2-direktivet bör följa det system som finns enligt säkerhetsskyddsregleringen och att fyra utpekade länsstyrelser ska ansvara för sektorn.

Hur många statliga myndigheter som kommer att pekas ut i sektorn kommer att klarläggas först vid identifieringen av kritiska

verksamhetsutövare. Det kan dock antas att det kommer att röra sig om ett begränsat antal i förhållande till det totala antalet myndigheter (367[1]). I förhållande till storleken på sektorn offentlig förvaltning enligt NIS2-direktivet kommer det alltså endast att röra sig om en liten del av dessa verksamhetsutövare.

Som följd bör det övervägas om tillsynsansvaret bör vila på en central myndighet. Utredningen övervägde i delbetänkandet om tillsynsansvaret skulle ligga hos MSB eller länsstyrelsen. Utredningen bedömde att MSB:s roll bör vara stödjande och samordnande snarare än att bedriva tillsyn. MSB erbjuder ett omfattande stöd för att upprätthålla samhällsviktig verksamhet bland annat avseende arbete med kontinuitetshantering. MSB kommer också som gemensam kontaktpunkt att ha en samordnande roll när det gäller CER-direktivet. Utredningen drar därför samma slutsats som i delbetänkandet att MSB inte bör vara tillsynsmyndighet för sektorn.

Även om det först vid en identifiering av verksamhetsutövare klargörs vilka myndigheter som kommer att pekas ut som kritiska i sektorn så kan det antas att en stor del av dem kommer att vara myndigheter som också bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen och därmed faller under Säkerhetspolisens övergripande tillsynsansvar. Detta talar enligt utredningen för att Säkerhetspolisen bör ansvara för tillsyn av de myndigheter som identifieras som kritiska verksamhetsutövare i sektorn. Arbetet skulle då kunna samordnas med den tillsyn som bedrivs enligt säkerhetskyddsregleringen.

Från Säkerhetspolisen har framförts att ett sådant uppdrag inte skulle ligga i linje med myndighetens nuvarande uppdrag. Säkerhetspolisens uppdrag är tydligt kopplat till antagonistiska hot medan CER-direktivet har ett vidare syfte. Säkerhetspolisen bör därför inte ansvara för sektorn.

Med hänsyn till det som framförts ovan bedömer utredningen att det mest lämpliga är att det är samma tillsynsmyndigheter som ansvarar för sektorn som enligt utredningens förslag om NIS2-direktivets genomförande. Detta trots att det endast är statliga myndigheter som omfattas i sektorn. De skäl som utredningen redogjorde för i delbetänkandet[2] gällande vilka länsstyrelser som bör ansvara för tillsyn gäller även vid implementeringen av CER-direktivet. Utred-

[1] Antal den 1 januari 2024 enligt Statskontorets webbplats, inhämtat 2024-06-27.
[2] SOU 2024:18 s. 219 ff.

ningen föreslår därför att Länsstyrelsen i Stockholms län ska vara tillsynsmyndighet för statliga myndigheter som identifierats som kritiska i sektorn offentlig förvaltning och har sitt säte i Stockholms, Uppsala, Södermanlands, Västmanlands, Värmlands, Gotlands, Örebro, Dalarnas eller Gävleborgs län samt Länsstyrelsen i Norrbottens län. Länsstyrelsen i Skåne län ska vara tillsynsmyndighet för statliga myndigheter som identifierats som kritiska i sektorn offentlig förvaltning och har sitt säte i Kronobergs, Blekinge, Kalmar eller Skåne län samt Länsstyrelsen i Stockholms län. Länsstyrelsen i Västra Götalands län ska vara tillsynsmyndighet för statliga myndigheter som har identifierats som kritiska i sektorn offentlig förvaltning och har sitt säte i Hallands, Jönköpings, Västra Götalands eller Östergötlands län samt Länsstyrelsen i Skåne län. Länsstyrelsen i Norrbottens län ska vara tillsynsmyndighet för statliga myndigheter som har identifierats som kritiska i sektorn offentlig förvaltning och har sitt säte i Västernorrlands, Jämtlands, Västerbottens eller Norrbottens län samt Länsstyrelsen i Västra Götaland.

Utredningen föreslår i sitt delbetänkande[3] att fyra länsstyrelser ska vara tillsynsmyndigheter för kommuner, regioner och statliga myndigheter inom vissa län, dvs. även andra länsstyrelser. Utredningen föreslår vidare att Länsstyrelsen i Stockholms län och Länsstyrelsen i Norrbottens län ska vara tillsynsmyndigheter för varandra och att Länsstyrelsen i Västra Götaland och Länsstyrelsen i Skåne län ska vara tillsynsmyndighet för varandra. Samtliga länsstyrelser som har lämnat remissvar har avstyrkt förslaget att vissa länsstyrelser ska utöva tillsyn över resterande länsstyrelser eftersom länsstyrelserna har en gemensam it-drift och gemensamma strukturer för informationssäkerhet och utveckling.

Utredningens bedömning är att det inte föreligger samma problematik när det gäller CER-direktivet men att det mest lämpliga är att det är samma tillsynsmyndigheter som ansvarar för sektorn offentlig förvaltning enligt CER-direktivet som enligt utredningens förslag om NIS2-direktivets genomförande. Utredningen föreslår därför att om regeringen beslutar att en annan myndighet ska vara tillsynsmyndighet över länsstyrelserna enligt lagen om cybersäkerhet så ska den myndigheten även vara tillsynsmyndighet enligt lagen om motståndskraft hos kritiska verksamhetsutövare.

[3] SOU 2024:18 s. 217 ff.

10.3.8 Rymden

Sektorn omfattar samma kategorier av verksamhetsutövare som i NIS2-direktivet. PTS är tillsynsmyndighet för sektorn enligt utredningens förslag om NIS2-direktivets genomförande. PTS bör därför ansvara för sektorn även när det gäller CER-direktivet.

10.3.9 Produktion, bearbetning och distribution av livsmedel

Sektorn omfattar samma kategorier av verksamhetsutövare som i NIS2-direktivet med den skillnaden att livsmedelsföretag som uteslutande bedriver logistikverksamhet har lagts till. Vidare har ordet *storskalig* lagts till i CER-direktivet när det gäller livsmedelsföretag som bedriver industriell produktion och bearbetning. Livsmedelsverket är tillsynsmyndighet för sektorn i NIS2-direktivet enligt utredningens förslag. Livsmedelsverket bör därför ansvara för sektorn även när det gäller CER-direktivet.

10.4 Tillsynsmyndighetens uppdrag

Utredningens förslag: Tillsynsmyndigheten ska utöva tillsyn över att lagen om motståndskraft hos kritiska verksamhetsutövare och föreskrifter som meddelats i anslutning till lagen följs samt inom ramen för tillsyn genomföra rådgivande uppdrag

Tillsynsmyndigheten ska även bidra med underlag till den nationella riskbedömningen.

Av artikel 9 framgår att varje medlemsstat ska utse eller inrätta en eller flera behöriga myndigheter som ansvariga för den korrekta tillämpningen och, vid behov, efterlevnadskontroll av direktivet på nationell nivå. En bestämmelse om att tillsynsmyndigheten ska utöva tillsyn över att den nya lagen och föreskrifter som har meddelats i anslutning till lagen följs bör därför införas.

Tillsynsmyndigheten ska också inom ramen för tillsyn genomföra rådgivande uppdrag, se avsnitt 7.3 och som framgår av avsnitt 6.1 ska tillsynsmyndigheten även bidra med underlag till den nationella riskbedömningen.

10.5 Tillsynsmyndighetens undersökningsbefogenheter

Utredningens förslag: Den som står under tillsyn ska på begäran tillhandahålla tillsynsmyndigheten den information som behövs för tillsynen och den nationella riskbedömningen.

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.

Tillsynsmyndigheten får förelägga den som står under tillsyn att tillhandahålla information och ge tillträde.

Ett sådant föreläggande får förenas med vite.

Tillsynsmyndigheten får begära handräckning av Kronofogdemyndigheten. Vid handräckning gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande.

Utredningens bedömning: När en tillsynsmyndighet begär information ska tillsynsmyndigheten ange syftet med begäran och precisera vilken information som krävs.

För att kunna utöva en effektiv tillsyn krävs att tillsynsmyndigheten får tillgång till den information som behövs samt vid behov tillträde till lokal eller liknande.

Av artikel 21.1 a framgår att tillsynsmyndigheten ska ha befogenhet att genomföra inspektioner på plats av den kritiska infrastruktur och de lokaler som verksamhetsutövaren använder för att erbjuda sina samhällsviktiga tjänster. Tillsynsmyndigheten ska också ha befogenhet att genomföra tillsyn på distans av de åtgärder som vidtagits i enlighet med artikel 13 (åtgärder för motståndskraft). Enligt artikel 21.1 b ska tillsynsmyndigheten även ha befogenhet att utföra eller beställa revisioner av kritiska verksamhetsutövare. Av artikel 21.2 framgår vidare att tillsynsmyndigheterna ska ha befogenhet att kräva den information som är nödvändig för att bedöma om de åtgärder som verksamhetsutövarna vidtagit för att säkerställa sin motståndskraft uppfyller kraven i artikel 13 samt bevis på att åtgärderna faktiskt har genomförts. Slutligen ska tillsynsmyndigheten när den begär information ange syftet med kravet och specificera vilken information som krävs.

Artikeln innebär att tillsynsmyndigheten ska kunna bedriva både platstillsyn och skrivbordstillsyn. En verksamhetsutövare ska också på begäran av tillsynsmyndigheten tillhandahålla den information och de handlingar som behövs för tillsynen och den nationella riskbedömningen[4]. Tillsynsmyndigheten ska också ha rätt att få till tillträde till områden, lokaler och andra utrymmen där verksamhet som omfattas av lagen bedrivs. Tillträdesrätten bör av integritetsskäl inte omfatta bostäder. Detta bör följa av lagen. Tillsynsmyndighetens möjlighet att utföra och beställa revisioner får anses ingå i uppgiften att bedriva tillsyn och möjligheten att begära in uppgifter och handlingar som behövs för tillsynen samt att få tillgång till områden, lokaler och andra utrymmen som används för verksamhet som omfattas av lagen. Att tillsynsmyndigheten när den begär information ska ange syftet med begäran och specificera den begärda informationen bör anges i förordning.

Om en verksamhetsutövare inte samarbetar med tillsynsmyndigheten vid tillsynen bör tillsynsmyndigheten kunna meddela de förelägganden som behövs för att förmå verksamhetsutövaren att tillhandahålla den information och ge det tillträde som behövs för tillsynen. Ett beslut om föreläggande bör kunna förenas med vite.

Allmänna bestämmelser om viten finns i lagen (1985:206) om viten, viteslagen. Där anges bland annat hur ett vitesföreläggande ska vara utformat i olika avseenden. Det framgår också att ett vitesföreläggande ska delges adressaten.

När det gäller vitesbeloppet framgår av viteslagen till exempel att detta ska 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 (3 § viteslagen). Med omständigheterna i övrigt avses bland annat kostnaderna för föreläggandets fullgörande och omfattningen av de åtgärder som krävs. Beloppet bör vidare bestämmas med hänsyn till hur angeläget det är att föreläggandet följs. Om föreläggandet avser att tillgodose ett betydelsefullt samhällsintresse, kan ett högre belopp vara motiverat. Myndigheterna kan emellertid inom ramen för 3 § viteslagen bestämma hur högt eller lågt belopp som helst. Vitet ska som huvudregel fastställas till ett bestämt belopp. Om det är lämpligt med hänsyn till omständigheterna, får vite dock enligt 4 § viteslagen föreläggas som löpande vite.

[4] Se avsnitt 6.1 gällande den nationella riskbedömningen.

Vitet bestäms då till ett visst belopp för varje tidsperiod av viss längd under vilken föreläggandet inte har följts eller, om föreläggandet avser en återkommande förpliktelse, för varje gång adressaten underlåter att fullgöra denna. Om ett föreläggande inte följs, kan myndigheten behöva upprepa föreläggandet. Det kan i dessa fall vara lämpligt att höja vitesbeloppet.

Frågor om utdömande av viten prövas enligt 6 § viteslagen av förvaltningsrätt på ansökan av den myndighet som har utfärdat vitesföreläggandet.

Enligt utredningens mening finns det inte anledning att införa bestämmelser som avviker från viteslagen.

Om en verksamhetsutövare ändå vägrar att ge tillsynsmyndigheten information eller tillträde till en lokal kan tvångsåtgärder behöva användas. För att tillsynsmyndigheten i en sådan situation ska kunna genomföra sin tillsyn bör myndigheten kunna begära handräckning av Kronofogdemyndigheten.

10.6 Samordning och informationsutbyte

10.6.1 Samarbetsforum

Utredningens bedömning: Myndigheten för samhällsskydd och beredskap ska leda ett samarbetsforum där tillsynsmyndigheterna ingår. Syftet med forumet ska vara att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn.

MSB leder i dag ett samarbetsforum där tillsynsmyndigheterna enligt NIS-lagen ingår. Utredningen föreslår i delbetänkandet att MSB även fortsättningsvis ska leda ett sådant samarbetsforum.[5]

I kommittédirektivet anges att 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.

Utredningen föreslår att MSB ska leda ett samarbetsforum för tillsynsmyndigheterna även när det gäller CER-direktivet. Det kommer sannolikt att finnas ett liknande behov av samordning och erfarenhetsutbyte gällande CER-direktivet som det gjort för NIS-

[5] SOU 2024:18 s. 240.

direktivet. I detta uppdrag bör också anses ingå att samordna information om den nya regleringen. Enligt artikel 9.1 ska medlemsstaterna säkerställa ett effektivt samarbete om det utses flera behöriga myndigheter enligt direktivet. Ett samarbetsforum bidrar till att möjliggöra ett sådant samarbete.

10.6.2 Övrigt samarbete

Utredningens bedömning: Det behövs ingen särskild reglering av myndigheternas övriga samarbete.

Enligt artikel 9.5 ska medlemsstaterna säkerställa att dess behöriga myndigheter samråder och samarbetar med andra relevanta myndigheter, inbegripet de som ansvarar för civilskydd, brottsbekämpning och skydd av personuppgifter, samt med kritiska verksamhetsutövare och relevanta berörda parter.

Enligt 8 § förvaltningslagen (2017:900) ska en myndighet inom sitt verksamhetsområde samverka med andra myndigheter. Enligt 6 § myndighetsförordningen (2007:515) ska myndigheten också verka för att genom samarbete med myndigheter och andra ta till vara de fördelar som kan vinnas för enskilda samt för staten som helhet. Mot den bakgrunden bedömer utredningen att det inte behövs någon särskild bestämmelse för att reglera myndigheternas övriga samverkan.

Enligt artikel 21.5 ska medlemsstaterna säkerställa att behöriga myndigheter enligt CER- och NIS2-direktiven samarbetar och utbyter information. Utredningens förslag innebär att det är samma myndighet som utövar tillsyn enligt de två direktiven. Det behövs därför ingen reglering av samarbetet. Detsamma gäller därmed för samarbete enligt NIS2-direktivets artikel 32.9 som utredningen behandlade i delbetänkandet.[6]

[6] SOU 2024:18 s. 243.

11 Ingripanden och sanktioner

11.1 Inledning

I kapitel 10 behandlas tillsynsmyndigheternas befogenheter i samband med tillsyn enligt CER-direktivet. Av direktivet följer även en skyldighet för medlemsstaterna att införa regler om sanktioner för överträdelser av de nationella bestämmelser som antagits enligt direktivet, samt se till att dessa tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. Bestämmelserna ska anmälas till kommissionen senast den 17 oktober 2024, och eventuella ändringar av dem ska anmälas utan dröjsmål.[1]

CER-direktivet innehåller inte några närmare bestämmelser om vilka sanktioner som ska införas, eller deras utformning. Utredningen behöver därför bedöma vilka ingripanden och sanktioner som bör föreslås, samt hur dessa bör utformas. I denna bedömning ingår även frågan om vilka överträdelser som sanktionerna ska kunna användas för att komma till rätta med.

11.2 Allmänna utgångspunkter

11.2.1 Systemets utformning

Utredningens bedömning: Systemet för ingripande och sanktioner avseende CER bör utformas på ett liknande sätt som föreslagits avseende NIS2.

Av artikel 22 i CER-direktivet följer en skyldighet för medlemsstaterna att fastställa regler om sanktioner för överträdelser av de nationella bestämmelser som antagits för att genomföra CER-direktivet. Det

[1] Se artikel 22 i CER-direktivet.

lämnas åt medlemsstaterna att avgöra utformning av dessa sanktioner, inklusive om de ska utgöras av administrativa sanktioner eller straffrättsliga påföljder.

När det i EU-rättsakter inte föreskrivs särskilda sanktioner för överträdelser följer av rättspraxis att medlemsstaterna är bundna enligt lojalitetsprincipen att vidta alla åtgärder som är ägnade att säkerställa unionsrättens tillämplighet och verkan. Detta innebär bland annat att medlemsstaterna ska se till att överträdelser av EU-rätten beivras på ett sätt som motsvarar vad som gäller för sådana överträdelser av nationell rätt som är av liknande art och svårighetsgrad. En sådan sanktion ska vara effektiv, stå i rimlig proportion till överträdelsen och vara avskräckande.[2]

Utredningens utgångspunkt är att systemet för när och på vilket sätt en tillsynsmyndighet enligt CER-direktivet ska ingripa mot överträdelser bör utformas på ett sätt som är så likt som möjligt det som föreslagits i delbetänkandet avseende NIS2-direktivet. En sådan utformning underlättar för så väl tillsynsmyndigheterna som verksamhetsutövarna. Utredningen bedömer dock att de sanktioner som föreslås inte behöver vara identiska för att uppnå syftet. Överträdelser av liknande art och svårighetsgrad återfinns bland annat i nuvarande NIS-lagen. Som följd anser utredningen att de sanktioner som föreslås avseende CER-direktivet åtminstone bör motsvara vad som gäller enligt NIS-lagen, och eftersträva likformighet med de förslagna cybersäkerhetsbestämmelserna där det är möjligt.

11.2.2 Val och utformning av sanktion

Utredningens bedömning: Val och utformning av sanktion enligt den föreslagna lagen behöver inte regleras särskilt.

Som redogjorts för ovan följer av artikel 22 i CER-direktivet att sanktionerna ska vara effektiva, proportionella och avskräckande. Dessa aspekter bör enligt utredningen därför beaktas vid samtliga ingripanden enligt den föreslagna lagen, och avse både vilken sanktion som väljs och utformningen av den. Tillsynsmyndigheten är

[2] Se till exempel EU-domstolens dom av den 21 september 1989 i mål nr C-68/88 (ECLI:EU:C:1989:339) p. 24 och dom av den 7 oktober 2010 i mål nr C-382/09 (CLI:EU:C:2010:596) p. 44 samt däri angiven praxis.

skyldig att följa förvaltningslagen (2017:900), där krav på att ingripanden ska vara effektiva och proportionella redan följer av 5 § tredje stycket. Utredningen bedömer mot denna bakgrund att dessa krav inte behöver regleras särskilt i den föreslagna lagen. Att sanktionerna ska vara avskräckande anser utredningen, i likhet med bedömningen som gjordes i avsnitt 9.4.1 i delbetänkandet, bäst löses genom att låta tillsynsmyndigheterna få handlingsutrymme i fråga om val av ingripandeåtgärd och utformningen av den. Slutsatsen i denna del är att val och utformning av ingripanden inte behöver regleras särskilt i den föreslagna lagen.

11.3 Administrativa sanktioner eller straffrättsliga påföljder?

Utredningens bedömning: Tillsynsmyndigheten ska kunna besluta om administrativa sanktioner för överträdelser av bestämmelser i den föreslagna lagen och föreskrifter som har meddelats med stöd av den lagen.

Utredningen har i sitt delbetänkande föreslagit att överträdelser av bestämmelserna i lagen om cybersäkerhet ska förenas med administrativa sanktioner, och inte straffrättsliga påföljder.[3] Bedömningen grundar sig huvudsakligen på att det både är effektivare och lämpligare att överträdelser av NIS2-direktivet beivras med administrativa sanktioner. Utredningen anser att denna bedömning gör sig gällande även avseende skyldigheterna i lagen om motståndskraft hos kritiska verksamhetsutövare. Detta får även till följd att sanktionssystemen kan utformas på likartat sätt. De sanktioner som föreslås kommer därför att vara av administrativt slag.

[3] SOU 2024:18 s. 251.

11.4 Tillsynsmyndigheten ska vara skyldig att ingripa mot överträdelser

Utredningens förslag: Tillsynsmyndigheten ska ingripa om en kritisk verksamhetsutövare har åsidosatt sina skyldigheter enligt den föreslagna lagen, eller föreskrifter som har meddelats med stöd av bestämmelserna.

Utredningen anser som ovan nämnt att den ordning som föreslagits avseende lagen om cybersäkerhet bör gälla även avseende lagen om motståndskraft hos kritiska verksamhetsutövare. Det innebär att tillsynsmyndigheten ska vara skyldig att ingripa mot överträdelser av den nu aktuella lagens skyldigheter. Detta bidrar enligt utredningens mening till ökad likabehandling mellan tillsynsmyndigheterna, genom att ingripande görs obligatoriskt. Den alternativa vägen att låta tillsynsmyndigheten själv välja om den ska ingripa hade på motsatt sätt kunnat bidra till minskad likabehandling och ökad splittring i tillsynspraxisen. Som följd bör ingripande vara obligatoriskt även avseende lagen om motståndskraft hos kritiska verksamhetsutövare, med undantag för vad som följer nedan.

11.5 Tillsynsmyndigheten ska i särskilda fall kunna avstå från att ingripa

Utredningens förslag: Tillsynsmyndigheten får avstå från att ingripa om överträdelsen är ringa eller ursäktlig, eller om det annars med hänsyn till omständigheterna vore oskäligt att besluta om sanktion.

Genom den föreslagna konstruktionen är en tillsynsmyndighet alltid skyldig att ingripa genom att meddela sanktioner mot samtliga överträdelser. En sådan lösning medför en hög grad av likabehandling och förutsägbarhet för tillsynssystemet, men riskerar att äventyra vissa rättssäkerhetsintressen och därtill göra tillsynssystemet omotiverat onyanserat. Utredningen anser att det finns skäl att införa en möjlighet för tillsynsmyndigheten att avstå från att ingripa i särskilda fall. Enligt utredningens mening ska det dock råda stark presumtion

för ingripande. Det är tillsynsmyndigheten som prövar om förutsättningarna för att avstå från ingripande är uppfyllda i det enskilda fallet.

Ett exempel på sådana rättssäkerhetsintressen är det så kallade dubbelprövningsförbudet som följer av artikel 4 i Europakonventionens sjunde tilläggsprotokoll. Det innebär en rätt att inte bli lagförd eller straffas två gånger för samma brott (gärning). Liksom var fallet med NIS2-verksamhet så kan även en kritisk verksamhetsutövare enligt den nu föreslagna lagen tillhandahålla flera samhällsviktiga tjänster som kan falla under olika tillsynsmyndigheters ansvarsområden. Detta medför en risk för att en överträdelse kan angripas av flera tillsynsmyndigheter parallellt. Om någon annan tillsynsmyndighet ingriper mot samma överträdelse riskerar agerandet att bryta mot dubbelprövningsförbudet och en ventil är därför motiverad redan på denna grund. Det bör dock noteras att det är möjligt att ingripa även om en annan myndighet ingripit, så länge dubbelprövningsförbudet inte överträds. Detta kan enligt utredningen motivera att ventilen kan tillämpas även i andra situationer när det skulle medföra oskäliga konsekvenser för verksamhetsutövaren, exempelvis om samma incident redan lett till kännbara sanktioner enligt något annat regelverk utan att dubbelprövningsförbudet aktualiserats.

Utformningen av undantaget från ingripande bör enligt utredningens mening göras på liknande sätt som vad som gäller på finansmarknadsområdet[4], vilket medför att det får ske om en överträdelse är ringa, ursäktlig, eller om det vore oskäligt att besluta om en sanktion. Det bör särskilt framhållas att oskälighet eller ursäktlighet inte kan anses föreligga om överträdelsen uppstått till följd av omständigheter som ligger inom verksamhetsutövarens kontrollsfär, exempelvis hänförligt till rutiner, tid och prioriteringar. En ringa eller ursäktlig överträdelse skulle kunna föreligga om överträdelsen berott på någon omständighet som verksamhetsutövaren varken kunnat eller borde ha förutsett eller kunnat påverka.

[4] Se exempelvis 15 kap. 1 b § andra stycket lagen (2004:297) om bank- och finansieringsrörelse.

11.6 Vilka överträdelser ska kunna leda till sanktioner?

Utredningens förslag: Överträdelser av följande bestämmelser, eller föreskrifter som har meddelats med stöd av dem, ska leda till att tillsynsmyndigheten ingriper.

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 §.

Av artikel 21.3 framgår att medlemsstaterna ska säkerställa att tillsynsmyndigheterna har möjlighet att vidta de åtgärder som är nödvändiga och proportionella för att avhjälpa överträdelser av direktivet. Enligt artikel 22 ska medlemsstaterna också införa effektiva, proportionella och avskräckande sanktioner vid överträdelser av de nationella reglerna som antagits. Sådana överträdelser avser reglerna om anmälningsskyldighet för vissa kritiska verksamhetsutövare, att genomföra riskbedömning, genomföra åtgärder för motståndskraft, upprätta och tillämpa en plan för motståndskraft, rapportera vissa incidenter, föra en befattningsanalys, genomföra bakgrundskontroll, att anteckna att identitetshandling och registerutdrag har visats upp vid bakgrundskontrollen samt att bevara sådana anteckningar i två år.

Utredningen anser inte att det framkommit några skäl till att begränsa vilka sanktioner som ska finnas tillgängliga för tillsynsmyndighetens ingripande mot överträdelser. Som följd ska samtliga sanktioner ska finnas tillgängliga för tillsynsmyndigheterna vid de angivna överträdelserna.

11.7 Vilka sanktioner ska finnas?

Utredningens bedömning: De sanktioner som ska föreslås är föreläggande vid vite, sanktionsavgift och anmärkning.

Som angetts i avsnitt 11.2.1 ovan är utredningens utgångspunkt att möjligheterna till ingripanden och sanktioner åtminstone bör motsvara vad som gäller enligt NIS-lagen, och eftersträva likformighet med de förslagna bestämmelserna i cybersäkerhetslagen där det är möjligt. Utredningen bedömer att detta som minimum bör innebära att föreläggande som kan förenas med vite och sanktionsavgifter föreslås. För att ingripandesystemet ska kunna utformas på ett sätt som liknar det som föreslagits avseende cybersäkerhetslagen anser utredningen även att ingripande genom anmärkning bör införas. Utredningen har övervägt införande av ytterligare sanktioner som föreslagits i cybersäkerhetslagen, såsom förbud att utöva ledningsfunktion, men har inte kunnat identifiera ett tydligt behov av ytterligare sanktioner än de som nu föreslås. Övervägandena för de sanktioner som föreslås kommer att redovisas i det följande.

11.7.1 Föreläggande som kan förenas med vite

Utredningens förslag: Tillsynsmyndigheten får besluta att förelägga den kritiska verksamhetsutövaren att vidta åtgärder för att uppfylla skyldigheterna som följer av 8 kap. 1 § i den föreslagna lagen.

Ett föreläggande får förenas med vite.

I likhet med utredningens bedömning avseende NIS2[5] anser utredningen att föreläggande med vitesmöjlighet är ett centralt verktyg för att tillsynsmyndigheten ska kunna framtvinga regelefterlevnad och därmed att CER-direktivets syfte uppnås. Föreläggandet kan användas för att den som står under tillsyn ska agera, eller avstå ifrån att agera, på ett visst sätt. För att öka incitamenten för en kritisk verksamhetsutövare att följa föreläggandet bör det kunna förenas med vite, om tillsynsmyndigheten bedömer att det är nödvändigt.

[5] Se SOU 2024:18 avsnitt 9.5.2.

Detta ökar även sannolikheten för att föreläggandet får avsedd effekt. Om föreläggandet förenas med vite är lagen (1985:206) om viten tillämplig. Lagen innehåller inte några absoluta beloppsbegränsningar för vitet, men ställer däremot krav på proportionalitet vid fastställande av vitets storlek. Detta skapar således stor handlingsfrihet för tillsynsmyndigheten att avgöra vilken nivå på vite som är lämplig, ändamålsenlig och proportionerlig för att uppnå den avsedda effekten i det enskilda fallet.

Utredningen bedömer att föreläggande med vite ska kunna riktas mot både enskilda och offentliga kritiska verksamhetsutövare. Upptäcker tillsynsmyndigheten bristande regelefterlevnad behöver åtgärder kunna vidtas för att snabbt komma till rätta med överträdelsen. Ett föreläggande bör därför även kunna gälla omedelbart, se vidare avsnitt 11.8.

11.7.2 Sanktionsavgift

Förutsättningarna för att ta ut sanktionsavgift

Utredningens förslag: Tillsynsmyndigheten får besluta att en kritisk verksamhetsutövare ska betala en sanktionsavgift till följd av en överträdelse enligt 8 kap. 1 § i den föreslagna lagen.

Till skillnad från NIS2-direktivet innehåller CER-direktivet inte några bestämmelser om vilka överträdda skyldigheter som ska leda till sanktionsavgift. Utredningens uppfattning är att även sanktionsavgifter som verktyg är centralt för att regelefterlevnad ska kunna uppnås. Liksom i fråga om NIS2 anser utredningen att ett system bör bygga på strikt ansvar, vilket innebär att en sanktionsavgift ska kunna tas ut oavsett om överträdelsen skett uppsåtligen eller av oaktsamhet. Utredningen anser däremot inte att det ska vara obligatoriskt för tillsynsmyndigheten att ta ut sanktionsavgift, utan den ska i varje enskilt fall bedöma om ett sådant ingripande är påkallat och därtill rättsligt grundat. Innebörden av detta är att tillsynsmyndigheten inte måste besluta om sanktionsavgift, men om den gör det räcker det med att konstatera att en överträdelse objektivt har skett, oaktat graden av vållande, för att sanktionsavgift ska kunna beslutas. I sammanhanget bör dock poängteras att graden av vållande i stället kan

vägas in vid beräkningen av sanktionsavgiftens storlek, samt om överträdelsen är ringa eller ursäktlig – möjligheten för tillsynsmyndigheten att avstå från ingripande (se avsnitt 11.5).

Genom att sanktionsavgiften inte görs obligatorisk finns risk för att olika tillsynsmyndigheter kommer att agera på olika sätt i likartade situationer, och därmed minska graden av likabehandling. Utredningen väger denna risk mot de rättssäkerhetsintressen som ska beaktas, och anser att de senare intressena väger tyngre. En sådan lösning medför också att det saknas skäl att införa bestämmelser om eftergift av sanktionsavgiften, utan eventuella förmildrande omständigheter ska vägas in av tillsynsmyndigheten redan vid bedömningen om sanktionsavgift ska tas ut över huvud taget.

En förutsättning för sanktionsavgift är att överträdelsen ska vara lätt att konstatera både för tillsynsmyndighet och den kritiska verksamhetsutövaren. Detta leder enligt utredningen till att ju högre precision på kraven som kommer att återfinnas i tillsynsmyndigheternas föreskrifter, desto lättare blir det att bedöma om en viss situation utgör en överträdelse. I vissa fall kommer överträdelser vara enklare att konstatera, exempelvis i fråga om incidentrapportering har skett i tid.

Sanktionsavgiftens storlek

Utredningens förslag: 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.

Sanktionsavgiften ska för offentliga kritiska verksamhetsutövare bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor.

Som nämnt saknar CER-direktivet angivelser om sanktionsavgifternas storlek. Detta leder utredningen till att jämföra nivåerna på sanktionsavgifter med liknande regelverk. Det ligger nära till hands att överväga de höga nivåer som följer av NIS2-direktivet även för överträdelser mot den nu föreslagna lagen. Utredningen anser dock

att en viss skillnad bör uppmärksammas. För att CER-direktivets syfte ska kunna uppnås kommer dess tillämpning enligt utredningens mening präglas av en betydligt högre grad av förtroende och samarbete mellan tillsynsmyndighet och tillsynsobjekt än vad som är fallet i fråga om NIS2. Detta till följd av att genomförandet av CER-direktivet kommer att utgöra ny lagstiftning för flertalet av de sektorer som omfattas, och att de kritiska verksamhetsutövarna kommer att ha ett stort behov av vägledning och stöd från tillsynsmyndigheterna för att kunna uppnå adekvat skydd. Dessa faktorer talar enligt utredningens mening med viss styrka för att sanktionsbeloppen bör hållas lägre än i fråga om lagen om cybersäkerhet.[6]

Å andra sidan ska det poängteras att det inte finns någon automatik i att det högsta sanktionsbeloppet i spannet alltid ska väljas. Tvärt om anser utredningen att det är omständigheterna i det enskilda fallet som avgör sanktionsavgiftens storlek, och där den kritiska verksamhetsutövarens ekonomiska styrka spelar in. Utredningen har avseende cybersäkerhetslagen föreslagit att maximal sanktionsavgift för väsentliga verksamhetsutövare ska vara det högsta av tio miljoner euro eller två procent global årsomsättning föregående räkenskapsår. Utredningen föreslår att motsvarande beräkningsgrund ska införas avseende sanktionsavgifter enligt säkerhetsskyddsregleringen, se kapitel 14. Eftersom den som blir identifierad som kritisk verksamhetsutövare enligt CER-direktivet också blir väsentlig verksamhetsutövare enligt cybersäkerhetslagen anser utredningen att motsvarande maximibelopp för sanktioner bör föreslås för överträdelser av CER-direktivet. Att använda samma beräkningsgrund och maxbelopp för sanktionsavgifter enligt lagen om motståndskraft hos kritiska verksamhetsutövare skulle enligt utredningen även kunna bidra till att praxis mellan systemen kan bli likartade. Detta talar med styrka för att samma beräkningsgrund för maxbeloppet bör väljas. Utredningen anser dock att fortsatt differentiering är motiverad mellan enskilda och offentliga kritiska verksamhetsutövare. Taket för sanktionsavgifter bör därför i sin helhet följa den föreslagna cybersäker-

[6] Utredningen har även noterat att finska regeringen i sitt utkast till proposition avseende CER har föreslagit mycket låga sanktionsavgifter (minst 2 000, högst 20 000 euro) i jämförelse med NIS2-direktivet, se 5 kap. 23 § och s. 111 i *Utkast till regeringens proposition med förslag om skydd av samhällets kritiska infrastruktur och om stärkande av samhällets motståndskraft samt till vissa andra lagar (CER-direktivet)*, hämtad 2024-05-11 från https://www.lausuntopalvelu.fi/SV/Proposal/Participation?proposalId=67962948-2e20-43d7-a9e5-e43c99b60a8c.

hetslagen där 10 miljoner kr är max för offentliga kritiska verksamhetsutövare.

Vad som ska beaktas särskilt vid bestämmande av sanktionsavgiftens storlek

Utredningens förslag: 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.

CER-direktivet saknar, till skillnad från NIS2-direktivet, bestämmelser om vad som ska beaktas vid bestämmande av sanktionsavgiftens storlek. Utredningen anser att när en sanktionsavgifts storlek ska bestämmas i det enskilda fallet bör samtliga relevanta omständigheter beaktas. Detta bör dock inte anges i förslaget till lag. I stället anser utredningen att vissa relevanta omständigheter som ska beaktas i försvårande riktning särskilt ska anges. Enligt utredningens bedömning finns det skäl att särskilt ange skada/risk för skada till följd av överträdelsen, tidigare överträdelser och undvikna kostnader till följd av överträdelsen som sådana omständigheter som särskilt ska beaktas. Motsvarande utformning av bestämmelse återfinns i 31 § NIS-lagen. Det bör noteras att uppräkningen inte är uttömmande, utan flera av de omständigheter som redogjorts för i utredningens delbetänkande avseende NIS2[7] kan vara av relevans för bedömning, exempelvis hur lång tid en överträdelse har pågått.

Hinder mot att ta ut sanktionsavgift

Utredningens förslag: 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] Se SOU 2024:18 avsnitt 9.4.2.

Att ta ut sanktionsavgift kan i vissa fall anses strida mot dubbelprövningsförbudet (se avsnitt 11.5). Det behöver därför finnas en ventil mot vissa sådana situationer som tydligt kan förutses, nämligen om en överträdelse redan omfattas av ett föreläggande om vite, eller utdömande av det. I dessa fall ska tillsynsmyndigheten därför inte ha befogenhet att besluta om sanktionsavgift. Ett sådant undantag överensstämmer med vad som i dag gäller enligt exempelvis 33 § NIS-lagen.

Betalning, verkställighet och preskription

Utredningens förslag: 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.

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.

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.

Bestämmelser kring förfarandet vid beslut om sanktionsavgift återfinns i flera av de författningar där sanktionsavgift återfinns som sanktion, exempelvis NIS-lagen och säkerhetsskyddslagen (2018:585), samt utredningens förslag till cybersäkerhetslag. Sådana regler kompletterar de allmänna reglerna i förvaltningslagen (2017:900). Utredningen anser att motsvarande bestämmelser bör föreslås i den nya lagen.

11.7.3 Anmärkning

Utredningens förslag: Om tillsynsmyndigheten inte finner skäl att besluta om andra sanktioner ska den i stället besluta om en anmärkning.

I utredningens delbetänkande har ett system med anmärkning föreslagits. CER-direktivet saknar krav på att en motsvarande sanktion ska införas. Utredningen bedömer dock att den systematik för ingripande som föreslagits i cybersäkerhetslagen även bör gälla avseende den nu föreslagna lagen. Det innebär att en tillsynsmyndighet är skyldig att ingripa mot alla överträdelser av lagen och besluta om någon form av sanktion, om inte undantaget om att avstå från ingripande är tillämpligt. Skulle utredningen föreslå ett system utan anmärkning skulle det medföra att tillsynsmyndigheten var tvungen att meddela föreläggande eller sanktionsavgift i varje enskilt fall. Det vore en olämplig lösning, eftersom utredningen bedömer att tillsynsmyndigheten är bäst lämpad att avgöra om och i sådana fall vilken av dessa sanktioner som ska tillgripas. Genom att införa ett system med anmärkning även i lagen om motståndskraft hos kritiska verksamhetsutövare skapas ett system där en överträdelse alltid ska få minst anmärkning som påföljd, men där tillsynsmyndigheten även har möjlighet att ingripa med något av de andra verktygen om den bedömer att det är lämpligt, ändamålsenligt, proportionerligt, med mera. Utredningen anser mot denna bakgrund att anmärkning ska finnas även inom ramen för den nu föreslagna lagen och lämpligen utformas på samma sätt som utredningen föreslagit i lagen om cybersäkerhet. Det ska därför införas en möjlighet för tillsynsmyndigheten att meddela anmärkningar mot kritiska verksamhetsutövare som har överträtt den föreslagna lagen eller föreskrifter som har meddelats med stöd av den lagen.

En anmärkning i sig innebär att tillsynsmyndigheten noterar att en överträdelse skett. Eftersom den kritiska verksamhetsutövaren inte nödvändigtvis delar uppfattningen att en överträdelse har skett ska även en tillsynsmyndighets beslut om anmärkning kunna överklagas.

11.8 Omedelbar verkställighet av beslut om förelägganden

Utredningens bedömning: Tillsynsmyndigheten får bestämma att ett beslut om föreläggande enligt den föreslagna lagen ska gälla omedelbart.

Myndigheters generella möjlighet att besluta om att ett föreläggande ska gälla omedelbart återfinns i 35 § tredje stycket förvaltningslagen (2017:900). Det kan även regleras särskilt, såsom i 38 § NIS-lagen och i utredningens förslag till cybersäkerhetslag. Utredningen bedömer att omedelbar verkställighet ska vara möjlig även inom ramen för CER, och hänvisar i denna del till argumentationen som framförts i delbetänkandet.[8]

11.9 Överklagande

Utredningens förslag: Beslut enligt den föreslagna lagen eller anslutande föreskrifter får överklagas till allmän förvaltningsdomstol. När tillsynsmyndighetens beslut överklagas är tillsynsmyndigheten motpart i domstolen.

Prövningstillstånd krävs vid överklagande till kammarrätten.

De beslut som tillsynsmyndigheten kan fatta enligt denna lag kan som huvudregel antas påverka tillsynsobjektets civila rättigheter och skyldigheter enligt artikel 6 i Europakonventionen. Sådana beslut behöver därför kunna bli föremål för domstolsprövning. Att beslut som kan antas påverka någons situation på ett inte obetydligt sätt är överklagbara följer även av 41 § förvaltningslagen. Detta gäller exempelvis beslut om att en verksamhetsutövare har identifierats som kritisk. Ett sådant beslut medför skyldigheter (se avsnitt 6.5 och 8.1) som börjar gälla efter viss tid. Utredningen anser att beslut bör kunna överklagas till allmän förvaltningsdomstol, och omfatta alla typer av verksamhetsutövare som kan bli föremål för en tillsynsmyndighets beslut. Den beslutsfattande tillsynsmyndigheten ska anses vara motpart till den klagande.[9]

[8] SOU 2024:18 avsnitt 9.7.
[9] Se SOU 2024:18 avsnitt 9.8, jfr 7 a § förvaltningsprocesslagen (1971:291).

12 Gemensam kontaktpunkt

12.1 Inledning

Av artikel 9.2 framgår att varje medlemsstat ska utse eller inrätta en gemensam kontaktpunkt. Den gemensamma kontaktpunkten ska ha en sambandsfunktion för att säkerställa gränsöverskridande samarbete. Av skäl 23 framgår att den gemensamma kontaktpunkten bör ha ansvar för samordningen av frågor angående kritiska entiteters motståndskraft och gränsöverskridande samarbete på unionsnivå. 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.

12.2 Gemensam kontaktpunkt i Sverige

Utredningens bedömning: Myndigheten för samhällsskydd och beredskap ska vara gemensam kontaktpunkt.

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

Utredningen har inte funnit skäl att göra någon annan bedömning och föreslår därför att MSB ska vara gemensam kontaktpunkt i Sverige.

12.3 Gemensamma kontaktpunktens uppgifter

Utredningens bedömning: Den gemensamma kontaktpunkten ska ha en sambandsfunktion för att säkerställa gränsöverskridande samarbete med gemensamma kontaktpunkter i andra medlemsstater och kommissionen.

Den gemensamma kontaktpunkten ska senast den 17 juli 2028 och därefter vartannat år lämna den rapport som avses i artikel 9.3 i CER-direktivet.

Den gemensamma kontaktpunkten ska i samverkan med tillsynsmyndigheten delta i de samråd som avses i artikel 11 i CER-direktivet.

Enligt artikel 9.2 ska den gemensamma kontaktpunkten 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. En medlemsstat får även föreskriva att dess gemensamma kontaktpunkt ska ha en sambandsfunktion med kommissionen och säkerställa samarbete med tredjeländer.

Enligt artikel 9.3 ska den gemensamma kontaktpunkten 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 incidentrapporter som mottagits, inklusive antal, art och om andra medlemsstater informerats enligt artikel 15.3.

Enligt artikel 15.3 ska den myndighet som tar emot en incidentanmälan via den gemensamma kontaktpunkten informera gemensamma kontaktpunkter i andra medlemsstater som påverkas av incidenten. När den gemensamma kontaktpunkten skickar sådan information ska den behandla informationen på ett sätt som respekterar dess konfidentialitet och skyddar den berörda verksamhetsutövarens säkerhet och kommersiella intressen. Utredningen föreslår i avsnitt 8.3 att MSB ska vara den myndighet som tar emot incidentrapporter. I det avsnittet föreslår utredningen även att MSB ska informera kontaktpunkter i andra medlemsstater.

Enligt artikel 11 ska medlemsstaterna när så är lämpligt samråda med varandra om kritiska verksamhetsutövare i syfte att säkerställa

att direktivet tillämpas på ett konsekvent sätt. Sådana samråd ska äga rum i synnerhet med avseende på kritiska verksamhetsutövare 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 verksamhetsutövare i andra medlemsstater,

c) har identifierats som kritiska verksamhetsutövare i en medlemsstat och tillhandahåller samhällsviktiga tjänster för eller i andra medlemsstater.

Samråden ska enligt artikeln syfta till att stärka kritiska verksamhetsutövares motståndskraft och, om möjligt, minska deras administrativa börda. Av skäl 26 framgår att samråden bör inledas på begäran av en berörd behörig myndighet. Utredningen föreslår att MSB i egenskap av gemensam kontaktpunkt bör vara den myndighet som ansvarar för samråd med andra medlemsstater enligt artikeln. I dessa samråd kan det dock vara tillsynsmyndigheten som har expertkunskap rörande den aktuella sektorn och samråden bör därför ske i samverkan mellan MSB och berörd tillsynsmyndighet.

Bestämmelsen om samråd enligt artikel 11 ska enligt artikel 8 inte tillämpas avseende kritiska verksamhetsutövare inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur.

Samarbetsgrupp

Utredningens bedömning: Regeringen ska företräda Sverige i den samarbetsgrupp som inrättats enligt artikel 19 i CER-direktivet.

Tillsynsmyndigheterna och Myndigheten för samhällsskydd och beredskap ska lämna stöd till Sveriges deltagande i samarbetsgruppen.

Genom artikel 19 inrättas en samarbetsgrupp på EU-nivå (gruppen för kritiska entiteters motståndskraft) som ska ge kommissionen stöd och underlätta samarbete och informationsutbyte mellan medlemsstaterna. Det engelska namnet på gruppen är *Critical Entities Resilience Group* som förkortas CERG. Gruppen ska bestå av före-

trädare för medlemsstaterna och kommissionen men kan bjuda in andra berörda parter att delta i arbetet. Gruppens uppgifter listas i artikel 19.3 a–j. Dessa består till exempel av utbyte av bästa praxis i frågor som identifiering och incidentrapportering. Senast den 17 januari 2025 ska gruppen ta fram ett arbetsprogram med de åtgärder som ska vidtas.

På EU-nivå har det funnits en samarbetsgrupp inom ramen för det europeiska programmet för skydd av kritisk infrastruktur (EPCIP). MSB har varit Sveriges representant i den gruppen.

CERG har redan bildats samt genomfört flera möten och Sverige har hittills representerats av Regeringskansliet (Försvarsdepartementet) och MSB. Utredningen föreslår att MSB ska vara gemensam kontaktpunkt i Sverige. Myndigheten kommer också att ha en bred och samordnande roll och utredningen föreslår därför att MSB även fortsatt ska lämna stöd till Sveriges representant i samarbetsgruppen. Ansvaret att företräda Sverige i CERG bör dock ligga på regeringen. Det bör därför vara regeringen som företräder Sverige i samarbetsgruppen vilket därmed inte behöver någon särskild reglering. Avseende säkerhetsgodkännande som nämns i artikel 19.2 behandlar utredningen detta i avsnitt 9.4. För det fall att gruppen kommer att bilda sektorsspecifika arbetsgrupper på samma sätt som gjorts i samarbetsgruppen som inrättats enligt NIS-direktivet bör det även vara möjligt för tillsynsmyndigheterna att delta i arbetet. Även i övrigt kan det finnas skäl för tillsynsmyndigheterna att lämna stöd när sektorsspecifika frågor diskuteras. Det bör därför införas en bestämmelse i förordningen om att tillsynsmyndigheterna och MSB ska lämna stöd till Sveriges deltagande i CERG.

13 Sekretess

13.1 Inledning

Utredningen ska ta ställning till om bestämmelserna i offentlighets- och sekretesslagen (2009:400), OSL, innebär ett tillräckligt skydd för sådana uppgifter som kan komma att behandlas i NIS2- och CER-direktiven. Det behöver bland annat övervägas om sekretessen enligt 18 kap. 8 § OSL är tillräckligt stark. Utredningen behöver även analysera om befintliga bestämmelser i OSL tillgodoser NIS2- och CER-direktivens krav på utlämnande av uppgifter till andra medlemsstater samt till kommissionen och Europeiska unionens cybersäkerhetsbyrå (Enisa). Detsamma gäller för uppgifter som har tagits emot. Vid behov ska utredningen lämna förslag till författningsändringar.

Utredningen har i sitt delbetänkande[1] lämnat förslag om incidentrapportering enligt NIS2-direktivet. Vidare har utredningen i kapitel 8 lämnat förslag om incidentrapportering enligt CER-direktivet. Incidentrapporter som följer av förslagen till lagen om cybersäkerhet och lagen om motståndskraft hos kritiska verksamhetsutövare innehåller normalt sett uppgifter om sårbarheter, säkerhets- och bevakningsåtgärder samt om hot mot eller andra risker för verksamheten. Även en rapports förekomst kan ge upplysningar till en antagonist om att till exempel ett it-angrepp kan ha lyckats eller åtminstone identifierats.

I detta kapitel behandlas sekretessfrågan för uppgifter som rör incidentrapporter, uppgifter som lämnas vid tillsyn och uppgifter i verksamhetsutövarnas riskanalyser och riskbedömningar samt förteckningar över verksamhetsutövare. I kapitlet berörs även frågan om sekretess för uppgifter som förekommer i en bakgrundskontroll och som om de röjs kan skada enskilda intressen. I kapitlet behandlas också frågan om tystnadsplikt i enskild verksamhet som omfattas av

[1] Kapitel 7 i SOU 2024:18.

lagen om motståndskraft hos kritiska verksamhetsutövare. Slutligen behandlas frågan om sekretess för uppgifter som ska lämnas till andra medlemsstater, kommissionen och Europeiska unionens cybersäkerhetsbyrå (Enisa) samt för uppgifter som delges svenska myndigheter inom ramen för det informationsutbyte som regleras i direktiven.

Offentlighetsprincipen

Offentlighetsprincipen har olika beståndsdelar. Bestämmelserna i regeringsformen (RF) om yttrande- och informationsfrihet gäller för de som är verksamma hos det allmänna – de så kallade offentliga funktionärerna – likaväl som för medborgarna i allmänhet. I RF slås också principen om domstolsförhandlingars offentlighet fast.

Tryckfrihetsförordningen (TF) innehåller å sin sida bestämmelse om – förutom tryckfriheten – allmänna handlingars offentlighet samt om den så kallade meddelarfriheten, som innebär stora möjligheter att lämna information för publicering i tidningar och andra tryckta skrifter. Såvitt gäller andra grundlagsskyddade medier än tryckta skrifter finns bestämmelser om meddelarfrihet i yttrandefrihetsgrundlagen (YGL).

Med handling förstås enligt 2 kap. 3 § första stycket TF en framställning i skrift eller bild eller en upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel. En handling är allmän om den förvaras hos en myndighet och enligt 2 kap. 6 eller 7 §§ TF är att anse som inkommen till eller upprättad hos en myndighet.

Bestämmelserna om allmänna handlingars offentlighet finns i 2 kap. TF. Enligt 2 kap. 2 § andra stycket TF ska varje begränsning i rätten att ta del av allmänna handlingar anges i en särskild lag eller i en annan lag som den förstnämnda lagen hänvisar till. Den särskilda lag som åsyftas är OSL.

Bestämmelser om sekretess

Rätten att ta del av allmänna handlingar får enligt 2 kap. 2 § TF begränsas endast när det är påkallat med hänsyn till sju olika uppräknade intressen. Flertalet punkter avser det allmännas intressen, bland annat det allmännas ekonomiska intresse (punkten 5). Punkten 6 avser en-

skildas intressen, nämligen skyddet för enskilds personliga eller ekonomiska förhållanden.

Sekretess innebär ett förbud att röja en uppgift, oavsett om det sker genom utlämnande av en handling eller genom att röja uppgiften muntligen eller på något annat sätt (3 kap. 1 § OSL). Sekretessen innebär dels handlingssekretess, dels tystnadsplikt. Till den del sekretessen innebär tystnadsplikt innebär den en begränsning av yttrandefriheten enligt regeringsformen, och den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna. Förbudet att röja eller utnyttja en uppgift enligt OSL eller annan lagstiftning som OSL hänvisar till gäller för myndigheter. Det finns dock kompletterande bestämmelser om tystnadsplikt i enskilda verksamheter, till exempel 8 kap. 1 och 2 §§ säkerhetsskyddslagen (2018:585) och 6 kap. 12 § patientsäkerhetslagen (2010:659).

Sekretess gäller som huvudregel inte bara i förhållande till enskilda utan också mellan myndigheter och inom en myndighet, om det där finns olika verksamhetsgrenar som är att betrakta som självständiga i förhållande till varandra (8 kap. 1 och 2 §§ OSL). I vissa fall måste dock myndigheter kunna utbyta uppgifter för att kunna utföra sina uppgifter. Sekretessregleringen innehåller därför särskilda sekretessbrytande bestämmelser (10 kap. OSL). Dessa har utformats efter en intresseavvägning mellan myndigheternas behov av att utbyta uppgifter och det intresse som den aktuella sekretessbestämmelsen avser att skydda.

Sekretessens styrka bestäms i regel med hjälp av så kallade skaderekvisit. Man skiljer mellan raka och omvända skaderekvisit. Vid raka skaderekvisit är utgångspunkten att uppgifterna är offentliga och att sekretess bara gäller om det kan antas att en viss skada uppkommer om uppgiften röjs. Det omvända skaderekvisitet har den omvända utgångspunkten, och uppställer sekretess som huvudregel. Vid ett omvänt skaderekvisit gäller således sekretess om det inte står klart att uppgiften kan röjas utan att viss skada uppstår. En del bestämmelser innehåller ett kvalificerat rakt skaderekvisit, vilket innebär att det krävs särskilt mycket för att sekretess ska gälla. Sekretessen enligt en bestämmelse kan även vara absolut. Vid absolut sekretess ska uppgifter som omfattas av bestämmelsen hemlighållas oavsett skada. Någon skadeprövning ska inte göras i dessa fall.

Utbyte av uppgifter med krav på bevarande av konfidentialiteten enligt NIS2- och CER-direktiven

I NIS2- och CER-direktiven finns bestämmelser om att vissa uppgifter ska ha ett sekretesskydd. Utredningen har analyserat de krav där direktiven föreskriver att konfidentialiteten ska bevaras.

Av artikel 1.4 i CER-direktivet framgår följande. 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. Bestämmelsen motsvaras i NIS2-direktivet av artikel 2.13.

Ytterligare bestämmelser om konfidentialitet finns i artikel 15.3 andra stycket CER-direktivet där det anges att gemensamma kontaktpunkter som skickar eller tar emot information enligt första stycket (incidentanmälan) 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 finns bestämmelser om konfidentialitet och kommersiell känslighet när det gäller rådgivande uppdrag.

Enligt artikel 23.6 NIS2-direktivet ska, när så är lämpligt, och särskilt om den betydande incidenten berör två eller flera medlemsstater, CSIRT-enheten, den behöriga myndigheten eller den gemensamma kontaktpunkten utan onödigt dröjsmål informera andra berörda medlemsstater och Enisa om den betydande incidenten. Sådan information ska åtminstone inbegripa den typ av information som mottagits i enlighet med artikel 23.4. Därvid ska CSIRT-enheten, den behöriga myndigheten eller den gemensamma kontaktpunkten, i enlighet med unionsrätten eller nationell rätt, bevara entitetens säkerhets- och affärsintressen samt den tillhandahållna informationens konfidentialitet. I artikel 30.2 i NIS2-direktivet avseende frivillig underrättelse om relevant information anges att CSIRT-enheterna

eller i tillämpliga fall de behöriga myndigheterna ska säkerställa att informationen förblir konfidentiell och skyddas på lämpligt sätt. Detta sammantaget innebär att frågan om sekretess för ovanstående uppgifter behöver bedömas.

Frågan om sekretess för uppgifter som rör incidentrapportering, med mera

Utredningens bedömning: En ny sekretessbestämmelse bör införas i 18 kap. offentlighets- och sekretesslagen (2009:400). Syftet med bestämmelsen är att ge ett skydd för uppgift i incidentrapporter som följer av kravet på incidentrapportering enligt lagen (2025:000) om cybersäkerhet och lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare samt uppgift om åtgärd som följer av en sådan incident. Bestämmelsen bör ha ett omvänt skaderekvisit som syftar till att uppfylla kraven på konfidentialitet i NIS2- och CER-direktiven.

Utredningen ska i enlighet med kommittédirektiven ta ställning till om det behövs ett starkare och mer omfattande sekretesskydd för uppgifter som kan komma att behandlas med stöd av direktiven. Bindande bestämmelser som rör konfidentialitet för uppgifter som rör incidentrapportering finns i NIS2- och CER-direktiven, se ovan.

Den sekretessbestämmelse som är av intresse avseende incidentrapportering enligt lagen om cybersäkerhet är främst sekretessen för säkerhets- eller bevakningsåtgärd i 18 kap. 8 § OSL och specifikt punkten 3 som rör ”telekommunikation eller system för automatiserad behandling av information”[2]. Med telekommunikation avses överföring av meddelande med tråd, radio eller en liknande metod. Med automatiserad behandling av information avses system där datorer, telekommunikation eller annan teknisk utrustning samverkar för att insamla, ordna, bearbeta, söka eller distribuera information. Som exempel på säkerhets- eller bevakningsåtgärder som bestäm-

[2] I detta sammanhang är det snarast ledet ”system för automatiserad behandling av information. I prop. 2003/04:93 beskrivs föremålet för sekretessen på ett sådant sätt att det i stora delar sannolikt är relevant även i dag. Den tekniska utvecklingen och utvecklingen på informationsteknikområdet har emellertid varit så omfattande sedan bestämmelsen infördes att den inte kan anses täcka dagens tillämning av informationstekniken.

melsen avser att skydda är enligt förarbetena[3] 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. Vad som faller utanför sekretessens räckvidd är beskrivningar av hur ett program fungerar i stora drag och vilka typer av uppgifter som bearbetas i ett program[4]. För rapportering enligt lagen om motståndskraft hos kritiska verksamhetsutövare torde det snarast vara punkten 1 i samma sekretessbestämmelse som är relevant i sammanhanget som rör byggnader eller andra anläggningar, lokaler och inventarier.[5] Även frågor kring behov av sekretessbrytande bestämmelser, överföring av sekretess och tystnadsplikt behöver utredas.

Utredningens analys

Utredningen gav de organisationer som bidrar med experter och deltagare i referensgruppen i utredningen möjlighet att inkomma med synpunkter på sekretessfrågan där frågorna rörde behovet av en ny eller ändrad sekretessbestämmelse i OSL och skälen till ett sådant behov. Resultatet visade att flertalet av svaren innehöll betänkligheter om nuvarande sekretessbestämmelser, främst 18 kap. 8 § OSL, ger ett tillräckligt skydd för incidentrapporter. De synpunkter som angavs kan sammanfattas till en osäkerhet om incidentrapportering alltid kan antas rymmas inom begreppet ”säkerhets- eller bevakningsåtgärd”, om lydelsen i punkten 3 kan antas relevant i ett modernt språkbruk och dessutom heltäckande för de uppgifter som det är fråga om[6], samt om ett rakt skaderekvisit (dvs. presumtion för offentlighet) kan vara begränsande för viljan hos verksamhetsutövare att rapportera incidenter. Vidare framförs frågan om de analyser som CSIRT-verksamheten ska utföra kan omfattas av bestämmelsen. Sådana analyser är till exempel risk- och incidentanalyser.

Utredningen konstaterar inledningsvis att det finns viss (men begränsad) praxis avseende tillämpningen av 18 kap 8 § 3 OSL. Ett belysande exempel är Kammarrätten i Göteborgs dom av den 29 juni

[3] Prop. 2003/04:93 s. 82 och s. 88.
[4] Prop. 2003/04:93, bet. 2003/04:KU17.
[5] Sekretess kan gälla bland annat för uppgifter om instruktioner och tjänstgöringslistor som rör bevakningen av en byggnad.
[6] Till exempel uppgifter om vem som har gjort rapporteringen, hur allvarlig en incident är och dess konsekvenser.

2021 i mål nummer 2144-24 där frågan om sekretess för incidentrapporter prövades. Kammarrätten gjorde där samma bedömning som Myndigheten för samhällsskydd och beredskap hade gjort i det överklagade beslutet avseende sekretess enligt nämnda bestämmelse för incidentrapportering enligt den då gällande förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Kammarrätten ansåg vidare att redan en uppgift om huruvida det har gjorts en sådan incidentrapportering som avsågs i begäran omfattas av sekretess enligt 18 kap. 8 § 3 OSL. Detta skulle kunna leda till slutsatsen att något behov av en ny sekretessbestämmelse inte föreligger. Det finns dock exempel på avgöranden från kammarrätt som ger en divergerad bild av skyddets omfattning.[7] Exempelvis har det i praxis avgjorts att en upplysning som avslöjar att inga särskilda säkerhetsåtgärder har vidtagits faller utanför bestämmelsens tillämpningsområde, även om en sådan upplysning i sig skulle kunna vara en säkerhetsbrist och visa på en fortsatt sårbarhet. Vidare har uppgifter som av domstolarna bedömts harmlösa lämnats ut.

Ett incidentrapporteringssystem bygger på att de aktörer som ska genomföra incidentrapportering har en hög tilltro till systemet och att deras känsliga uppgifter ges ett fullgott skydd. Om tilltron minskar kan aktörerna överväga att inte genomföra rapporteringen eller utelämna uppgifter som aktörerna anser är känsliga. En sådan utveckling riskerar att motverka ändamålet med rapporteringen, vilket i slutändan kan leda till mer omfattande sårbarheter i samhället. Av detta skäl bör sekretessfrågan för uppgifterna i en incidentrapport tas på allvar. Incidentrapporteringen kan innefatta uppgifter som vid en första anblick kan verka harmlösa, men som i ett större perspektiv kan får stora konsekvenser om uppgifterna röjs. Exempel på sådana uppgifter är uppgifter som kan framkomma i ett tidigt skede under ett it-angrepp där omfattningen av angreppet ännu inte blivit känd. På samma sätt kan uppgifter om att några säkerhetsåtgärder inte har vidtagits ge en antagonist en god bild om kvarvarande sårbarheter i ett system. Vidare råder det en osäkerhet om identiteten på ingivaren av incidentrapporten kan ges ett skydd med

[7] Se till exempel Kammarrätten i Stockholms dom av den 4 augusti 2005 i mål nr 4966-05, Kammarrätten i Jönköpings dom av den 12 januari 2011 i mål nr 2954-10 och Kammarrätten i Jönköpings dom av den 14 februari 2012 i mål nr 1322-11.

stöd av nämnda sekretessbestämmelse, liksom de åtgärder som kan följa av en incidentrapport.

Utredningen anser därför att det är osäkert om sekretessens omfattning när det gäller den incidentrapportering som det nu är fråga om är tillräcklig och delar därför experternas oro över att den något ålderdomliga lydelsen[8] i kombination med viss praxis från kammarrätterna kan leda till att känsliga uppgifter som enligt utredningen bör omfattas av sekretess i stället blir offentliga.

Sedan 18 kap. 8 § OSL trädde i kraft har utvecklingen på it-området varit omfattande. Tjänster och funktionalitet i dagens informationssystem har utvecklats på ett sådant sätt som inte var möjligt att förutsäga vid bestämmelsens tillkomst. Dessutom har nya metoder att både angripa och skydda informationen tillkommit liksom att hoten mot informationssystemen har ökat och förändrats. Ett exempel på det sistnämnda är så kallat ransomware som innebär att en verksamhetsutövare kan få sin information eller sina system gjorda otillgängliga genom att en antagonist angriper tillgångarna och krypterar dem. Antagonisten kräver därefter betalning, dvs utpressning, från verksamhetsutövaren för att tillgångarna ska låsas upp. Uppgiften om vem som är ingivare av en incidentrapport kan i vissa fall vara mycket känslig – dels kan en sådan uppgift om den röjs vara börspåverkande för en enskild verksamhetsutövare, dels kan rapporten ge information till en antagonist om ett angrepp har lyckats eller blivit upptäckt. Det kan därför inte uteslutas att det kan finnas uppgifter i en incidentrapportering som, även om uppgifterna är mycket känsliga, inte skulle omfattas av sekretess enligt aktuell bestämmelse. Denna ordning är inte tillfredsställande. Särskilt hos CSIRT-enheten, där en större mängd information som härrör från incidentrapporter, är sekretessfrågan viktig. Viss av denna information skulle sannolikt kunna hänföras till 18 kap. 8 § 3 OSL medan annan information inte nödvändigtvis har ett givet sekretesskydd, Utredningen bedömer därför att en ny bestämmelse om sekretess behövs.

[8] Begreppet ”automatisk behandling av information” är ett begrepp som i dag får anses utmönstrat i det dagliga språkbruket.

En ny sekretessbestämmelse i 18 kap. OSL

Utredningen konstaterar att även om en uppgift i en incidentrapport inte nödvändigtvis behöver röra en bevaknings- eller säkerhetsåtgärd eller kan förutses innehålla en uppgift som rör en bevaknings- eller säkerhetsåtgärd torde en ny sekretessbestämmelse ändå systematiskt kunna placeras i anslutning till 18 kap. 8 § OSL.

I 18 kap. 8 a § OSL finns en bestämmelse som rör incidentrapportering i domstolar, med mera. Regeringen konstaterade i propositionen till bestämmelsen[9] att sekretesskyddet för incidentrapporter inte var heltäckande enligt dåvarande ordning och att en ny sekretessbestämmelse därför behövde införas. Skälen som anfördes överensstämmer i stort med de farhågor om sekretessens begränsning avseende de incidentrapporter som det nu är frågan om.

Frågan om skaderekvisitet

När det gäller skaderekvisitet konstaterar utredningen att utformningen av skaderekvisitet kan ha stor betydelse för en verksamhetsutövares tilltro till incidentrapporteringssystemet. Aktörerna ska lämna in en betydande mängd information vid incidenter. Om sådan informationen blir offentlig kan det orsaka skada på verksamheten och tillhandahållandet av den samhällsviktiga tjänsten samt orsaka negativa kommersiella effekter, vilket kan påverka den enskilda verksamhetsutövaren och ytterst samhällets funktionalitet. Den nuvarande sekretessregleringen för säkerhets- och bevakningsåtgärder är, i nu relevanta delar, begränsad till ”telekommunikation eller system för automatiserad behandling av information” (18 kap. 8 § 3 OSL) och är utformade med ett rakt skaderekvisit. När det gäller andra uppgifter som kan finnas i en incidentrapport finns det inte någon tillämplig bestämmelse om sekretess.

Behovet av en skärpt sekretess måste vägas mot att det kan finnas ett insynsintresse avseende incidenter som har drabbat verksamhetsutövare inom det allmänna som omfattas av lagen om cybersäkerhet och lagen om motståndskraft hos kritiska verksamhetsutövare. Allmänhetens intresse av uppgifter som rör skatte- och avgiftsfinansierad verksamhet och annan verksamhet som är av betydelse för allmänheten måste anses vara stort. När det gäller sådana upp-

[9] Prop. 2018/19:81.

gifter som om de röjs kan medföra att sårbarheter blir offentliga i det slag av verksamhet som de rör sig om anser dock utredningen att skälen för sekretess väger tyngre. Allmänhetens tillgång till uppgifter om tekniska frågor kring informationssäkerhet i en incidentrapport måste därför stå tillbaka i relation till den skada som kan uppstå genom ett röjande av uppgifterna.

It-incidentrapportering är en viktig del för att skapa kunskap och lärdom om samhället sårbarheter även för de aktörer som inte är direkt inblandade men också för allmänheten. Varje år sammanställer MSB trender och slutsatser om samhällets informations- och cybersäkerhet utifrån inkommen it-incidentrapportering[10]. Genom denna årliga redovisning får allmänheten insyn i omständigheter som rör it-incidenter under det gångna året. Vidare finns det i 5 kap. 7 § i förslaget till lagen om cybersäkerhet en bestämmelse om att en tillsynsmyndighet får förelägga en verksamhetsutövare att i vissa fall offentliggöra information rörande incidenter. Utredningen anser därför att offentlighetsintresset för detta slag av uppgifter är väl tillgodosett.

Utredningen bedömer att en ny sekretessbestämmelse bör utformas med ett omvänt skaderekvisit. Detta innebär inte att rätten att ta del av information i ärenden som rör incidentrapportering är utesluten. Det omvända skaderekvisitet innebär att om det inte kan antas att det föreligger någon skada i det enskilda fallet så ska uppgiften lämnas ut. Detta får särskild betydelse för uppgifter från verksamhetsutövare inom det allmänna där det sällan finns kommersiella aspekter och där skyddsintresset i många gånger får anses väga svagare än offentlighetsintresset.

13.2 En ny sekretessbestämmelse för uppgift i incidentrapporter

Utredningens förslag: En ny bestämmelse om sekretess förs in i 18 kap. offentlighets- och sekretesslagen (2009:400) med följande lydelse.

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

[10] I senaste utgåva MSB2341, ISBN 978-91-7927-494-8, 2024.

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

Rätten att meddela och offentliggöra uppgifter ska inte ha företräde framför den tystnadsplikt som följer av den nya sekretessbestämmelsen.

Utredningen föreslår en ny bestämmelse i OSL som explicit tar sikte på uppgift i incidentrapporter som följer av lagen om cybersäkerhet och lagen om motståndskraft hos kritiska verksamhetsutövare samt på uppgift om åtgärder som följer av sådana incidenter. Detta i syfte att motverka de negativa effekter i den rapporterande verksamhetsutövarens verksamhet som har beskrivits ovan och som är hänförliga till att sekretessen för uppgift i incidentrapporter inte är heltäckande. Detta avser till exempel negativa konsekvenser för verksamhetsutövarens pågående och framtida säkerhetsarbete, negativa ekonomiska effekter för enskilda verksamhetsutövare och bristande rapporteringsvilja. Bestämmelsen täcker incidentrapporter från såväl enskilda som från verksamhetsutövare i det allmännas verksamhet. Även om insynsintresset avseende viss verksamhet som har betydelse för viktiga samhällsfunktioner kan anses vara betydande, torde de uppgifter som det är frågan om ha ett relativt lågt informationsvärde hos allmänheten. Genom skaderekvisitet kan sekretessen göras mindre långtgående i det allmännas verksamhet där det kan finnas ett större intresse av offentlighet. Mot bakgrund av att behovet av tilltro till systemet är avgörande, att innehållet i en incidentrapport kan orsaka en stor skada om den röjs samt att konsekvenserna av ett röjande kan få betydande negativa effekter i verksamheten hos den aktör som genomför rapporteringen bör sekretessbestämmelsen som ovan nämnts utformas med ett så kallat omvänt skaderekvisit Det gäller även för de åtgärder som vidtas med anledning av en incident. Sådana åtgärder kan motverkas om en antagonist får reda på vilka åtgärder som har vidtagits (och därigenom också kan utläsa vilka åtgärder som inte har vidtagits). Även en uppgift om att inga åtgärder har vidtagits bör omfattas av sekretess om det inte står klart att en sådan uppgift kan lämnas ut. Skaderekvisitet innebär att uppgifter i rapporten, eller åtgärder som har vidtagits, ändå oftast kan

lämnas ut relativt tidigt efter en incident när åtgärder för att minska incidentens effekt har vidtagits. Exempel på sådana åtgärder är så kallade *patchningar*, som innebär att en sårbarhet minskas eller försvinner. Sekretessen bedöms därför i många fall gälla enbart för en kortare tid. För vissa uppgifter kan dock sekretessen behöva kvarstå en längre tid. Utredningen har dock valt att föreslå en begränsning till att sekretessen enbart gäller i 40 år, vilket är samma sekretesstid som gäller för incidentrapporter i domstolar, med mera.

Rätten att meddela och offentliggöra uppgifter bör begränsas

Sekretess innebär ett förbud att röja en uppgift, vare sig det sker genom utlämnande av allmän handling, muntligt eller på annat sätt (3 kap. 1 § OSL). Den rätt att meddela och offentliggöra uppgifter som följer av yttrandefrihetsgrundlagarna har som huvudregel företräde framför tystnadsplikten. Stor återhållsamhet bör iakttas vid prövningen av om det bör göras undantag från rätten att meddela och offentliggöra uppgifter i ett särskilt fall. Enligt utredningens bedömning finns det tillräckliga skäl att göra undantag för den nu aktuella typen av uppgifter. Det rör sig här bland annat om sekretess med ett omvänt skaderekvisit och där ett offentliggörande skulle kunna orsaka skada för tillhandahållandet av samhällsviktiga tjänster[11]. Som utredningen anfört ovan tillgodoses intresset av insyn bland annat genom sekretessbedömningen, att sekretessen i vissa fall endast kommer gälla under en kortare tid samt att information om incidenter finns att tillgå i MSB:s publikationer. En inskränkning av meddelarfriheten är mot den bakgrunden motiverad. Rätten att meddela och offentliggöra uppgifter bör därför inte ha företräde framför den tystnadsplikt som följer av den föreslagna bestämmelsen i 18 kap. OSL. Detta gäller redan i dag för bestämmelsen i 18 kap. 8 §. Av bestämmelsen i 18 kap. 19 § OSL framgår i vilka fall den tystnadsplikt som följer av en bestämmelse om sekretess i 18 kap. OSL inskränker rätten att meddela och offentliggöra uppgifter. Den föreslagna bestämmelsen bör därför läggs till i uppräkningen i 18 kap. 19 § OSL.

[11] Jfr prop. 1979/80:2 Del A s. 111 f.

13.3 En ny sekretessbrytande bestämmelse

Utredningens förslag: En ny sekretessbrytande bestämmelse införs i 15 kap. offentlighets- och sekretesslagen (2009:400) med följande lydelse.

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.

I 15 kap. 1 a § OSL regleras skyddet för uppgifter som en myndighet har fått från ett utländskt organ på grund av bland annat en bindande EU-rättsakt, om det kan antas att Sveriges möjlighet att delta i det internationella samarbete som avses i rättsakten försämras om uppgiften röjs. Sekretessen gäller hos den myndighet som tar emot uppgiften. Bestämmelsen är tillämplig på sådana uppgifter som regleras i NIS2- och CER-direktiven. Utredningen har konstaterat att det är nödvändigt att sådana uppgifter även kan hanteras av andra myndigheter i Sverige än den myndighet som är primär mottagare. För att kunna fullgöra sina uppgifter behöver såväl Myndigheten för samhällsskydd och beredskap liksom tillsynsmyndigheterna enligt lagen om cybersäkerhet och lagen om motståndskraft hos kritiska verksamhetsutövare ömsesidigt kunna utbyta sådana uppgifter som härrör från andra EU-medlemsstater och EU:s institutioner oberoende av vilken myndighet som har fått uppgiften. Det rör sig till exempel om uppgifter i incidentrapporter, uppgifter inom det rådgivande uppdraget enligt CER-direktivet och uppgifter som delges i samverkan med andra medlemsstaters tillsynsmyndigheter enligt NIS2-direktivet. Som redogjorts för i avsnitt 13.1 ställs krav på bevarande av konfidentialitet i båda direktiven. Utredningens bedömning är att uppgifterna i allt väsentligt kommer att vara sekretessbelagda. Av det

skälet behövs en sekretessbrytande bestämmelse som möjliggör ett sådant informationsutbyte.

När det gäller överföring av sekretess anges i förarbetena till 15 kap. 1 a § OSL anges att sekretessen primärt gäller endast hos den myndighet som fått eller inhämtat uppgiften och inte hos den mottagande myndigheten.[12] I propositionen Skydd av Sveriges säkerhet vid radioanvändning uppges att sekretess enligt denna bestämmelse gäller oavsett hos vilken myndighet informationen finns.[13] Samma ställningstagande gör regeringen i propositionen Ett granskningssystem för utländska direktinvesteringar till skydd för svenska intressen.[14] Utredningen gör inte någon annan bedömning än den som regeringen gjort i de två sistnämnda propositionerna. Slutsatsen är därmed att sekretess enligt 15 kap. 1 a § OSL gäller avsett hos vilken myndighet uppgifterna finns. Om uppgifter som är sekretessbelagda enligt denna bestämmelse lämnas till tillsynsmyndigheten, kommer de därför att ha samma sekretesskydd som hos de myndigheter som lämnat uppgifterna.

13.4 Behov av ytterligare bestämmelser om sekretess, med mera

Utredningens bedömning:

1. Bestämmelserna om sekretessbrytande och överföring av sekretess i 10 kap. 17 §, 10 kap. 28 § och 11 kap. 1 § offentlighets- och sekretesslagen (2009:400) tillgodoser behovet när det gäller överföring av uppgifter från verksamhetsutövare till tillsynsmyndigheter,
2. Bestämmelsen om sekretess för uppgifter om enskildas affärs- eller driftsförhållanden vid tillsyn och utredning i 30 kap. 23 § offentlighets- och sekretesslagen (2009:400) görs tillämplig genom att en ny punkt om utredning och tillsyn enligt lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare införs i bilagan till offentlighets- och sekretessförordningen (2009:641).

[12] Prop. 2012/13:192 s. 30.
[13] Prop. 2019/20:15 s. 37.
[14] Prop. 2022/23:116 s. 146.

3. Bestämmelsen om risk- och sårbarhetsanalyser i 18 kap. 13 § offentlighets- och sekretesslagen (2009:400) tillgodoser behovet av sekretess för riskanalyser och riskbedömningar.
4. Bestämmelsen i 18 kap. 8 § offentlighets- och sekretesslagen (2009:400) ger ett tillräckligt skydd för förteckningar av verksamhetsutövare.
5. Bestämmelsen i 8 kap. 3 § offentlighets- och sekretesslagen (2009:400) tillgodoser kraven på utlämnande av uppgifter till andra medlemsstater och till kommissionen.
6. Bestämmelserna i 15 kap. 1 § offentlighets- och sekretesslagen (2009:400) tillgodoser delvis kraven på skydd av uppgifter som mottagits från andra medlemsstater.

Utredningen har analyserat om det behövs ytterligare förändringar i OSL och där beaktat behoven av ytterligare bestämmelser om överföring av sekretess och därmed sammanhängande sekretessbrytande bestämmelser, om skyddet för enskildas affärs- eller driftsförhållande i samband med tillsyn, om skyddet för uppgifter i riskanalyser och om behovet av sekretessreglering för uppgifter som lämnas och tas emot i samarbetet med kommissionen och med medlemsstater i Europeiska unionen.

I 10 kap. 17 § OSL finns en sekretessbrytande bestämmelse som innebär att en uppgift utan hinder av sekretess får lämnas till en myndighet om uppgiften behövs för tillsyn eller revision. Vidare finns en bestämmelse i 10 kap. 28 § OSL om att sekretess inte hindrar att en uppgift lämnas till en annan myndighet, om uppgiftsskyldighet följer av lag eller förordning. Sådana bestämmelser har föreslagits i både cybersäkerhetsförordningen och förordningen om motståndskraft hos kritiska verksamhetsutövare. Bestämmelserna i 10 kap. OSL bedöms därför gälla för de uppgifter som finns hos verksamhetsutövare och som rapporteras till MSB och till tillsynsmyndigheter enligt lagen om cybersäkerhet och lagen om motståndskraft hos kritiska verksamhetsutövare. För de fallen behövs därför inte någon ytterligare sekretessbrytande bestämmelse.

I 11 kap. 1 § OSL finns en bestämmelse om överföring av sekretess som innebär att när en myndighet i verksamhet som avser tillsyn eller revision, från en annan myndighet får en sekretessreglerad uppgift,

blir sekretessbestämmelsen tillämplig på uppgiften även hos den mottagande myndigheten. Det behövs därför inte någon ytterligare bestämmelse om överföring av sekretess inom ramen för den tillsyn som ska bedrivas.

I 30 kap. 23 § OSL finns en bestämmelse som gäller, i den utsträckning regeringen meddelar föreskrifter om det, i en statlig myndighetsverksamhet som består i utredning, planering, prisreglering, tillståndsgivning, tillsyn eller stödverksamhet med avseende på produktion, handel, transportverksamhet eller näringslivet i övrigt för uppgift om en enskilds affärs- eller driftförhållanden, uppfinningar eller forskningsresultat, om det kan antas att den enskilde lider skada om uppgiften röjs. Bestämmelsen är tillämplig på uppgifter hos enskilda verksamhetsutövare under förutsättning att regeringen har meddelat föreskrifter om detta. Sådana föreskrifter finns i bilagan till OSF och utredningen föreslår därför att det där införs en ny punkt som avser utredning och tillsyn enligt lagen om motståndskraft hos kritiska verksamhetsutövare. Utöver att tillhandahålla uppgifter i tillsyn ska verksamhetsutövare enligt lagen om motståndskraft hos kritiska verksamhetsutövare även tillhandahålla uppgifter som behövs för den nationella riskbedömningen. Bestämmelsen ska inte gälla beslut i ärenden. I utredningens delbetänkande[15] lämnades motsvarande förslag när det gäller tillsyn enligt lagen om cybersäkerhet. Detta förslag bör enligt utredningens mening kompletteras med att även gälla utredning.

I 18 kap. 13 § OSL finns en sekretessbestämmelse som föreskriver sekretess för uppgift som hänför sig till en myndighetsverksamhet 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. Det har till utredningen framförts att det möjligen kan vara osäkert om sekretessen i denna bestämmelse tar sikte även på riskanalyser och riskbedömningar enligt lagen om cybersäkerhet och lagen om motståndskraft hos kritiska verksamhetsutövare. Utredningen har dock konstaterat att bestämmelsen i praxis har tillämpats för skilda slag av analyser.[16] Denna praxis följer även av

[15] SOU 2024:18 s. 68.
[16] Exempelvis har delar av en pandemiplan ansetts omfattas av sekretess enligt 18 kap. 13 § OSL, se Kammarrätten i Göteborgs dom av den 21 juli 2021 i mål nr 1727-21.

motiven i propositionen Vårt framtida försvar (2004/05:5) som införde bestämmelsen i 18 kap. 13 § OSL och som anger att begreppet "verksamhet som består i risk- och sårbarhetsanalyser avseende fredstida krissituationer eller planering och förberedelser för hantering av sådana situationer" även innefattar ett insamlande av sådana uppgifter som behövs i verksamheten när detta insamlande utförs av andra handläggare inom myndigheten än de som primärt arbetar med analys-, planerings- och förberedelsearbetet.[17] Genom att bestämmelsen berör ett flertal olika analyser torde den riskanalys respektive riskbedömning som föreslås därför ges ett tillräckligt sekretesskydd enligt denna bestämmelse.

En fråga som har analyserats är sekretessens räckvidd när det gäller förteckningar över verksamhetsutövare som till exempel ska föras av tillsynsmyndigheterna och av Myndigheten för samhällsskydd och beredskap. Utredningen konstaterar att sådana förteckningar i praxis har ansetts omfattas av sekretess enligt 18 kap. 8 §[18]. Någon ny bestämmelse om sekretess för förteckningar över verksamhetsutövare föreslås därför inte.

När det gäller det informationsutbyte som föreskrivs i NIS2- och CER-direktiven behöver det vara möjligt att överföra uppgifter som omfattas av sekretess till en utländsk myndighet eller en mellanfolklig organisation (till exempel kommissionen och medlemsstater i Europeiska unionen). I 8 kap. 3 § OSL finns en bestämmelse om att en uppgift för vilken sekretess gäller enligt denna lag får inte röjas för en utländsk myndighet eller en mellanfolklig organisation, om inte utlämnandet sker i enlighet med särskild föreskrift i lag eller förordning. Genom att skyldigheten följer av 21, 23–27 §§ i förslaget till förordning om cybersäkerhet och 7, 11–14, 19–20, 28 samt 38–40 §§ i förordningen om motståndskraft hos kritiska verksamhetsutövare är detta krav uppfyllt.

Frågan om sekretess för uppgifter från kommissionen eller från andra länder har behandlats i avsnitt 13.3. Den så kallade utrikessekretessen reglerar sekretess för en uppgift som rör Sveriges förbindelser med en annan stat eller i övrigt rör annan stat, mellanfolklig organisation, myndighet, medborgare eller juridisk person i annan stat eller statslös, om det kan antas att det stör Sveriges

[17] Prop. 2004/05:5 s. 263.
[18] Se Kammarrätten i Jönköpings avgöranden den 5 maj 2020 i mål nr 998-20 respektive den 3 december 2020 i mål nr 3039-20, som rör sammanställningar av leverantörer av samhällsviktiga tjänster.

mellanfolkliga förbindelser eller på annat sätt skadar landet om uppgiften röjs. Denna bestämmelse bedöms kunna tillämpas för det fall att uppgifter från kommissionen och andra länder skulle förekomma hos sådana myndigheter som inte har fått uppgifterna direkt, utan som ett led i samarbetet mellan olika myndigheter i Sverige.

13.5 En ny sekretessbestämmelse för diarier för incidentrapporter

Utredningens bedömning: En ny bestämmelse införs i 3 § offentlighets- och sekretessförordningen (2009:641) som gäller diarium över incidentrapporter vid Myndigheten för samhällsskydd och beredskap, tillsynsmyndighet samt myndighet som rapporterar incidenter enligt lagen (2025:00) om cybersäkerhet och lagen (2025:00) om motståndskraft hos kritiska verksamhetsutövare.

Utredningen har konstaterat att en uppgift om förekomsten av en incidentrapport som rör eller kommer från en aktör i sig kan motverka syftet med incidentrapporteringen om uppgiften om aktören röjs. Om till exempel en aktör inom elförsörjningen rapporterar en incident skulle, även om sekretess gäller för uppgifterna i rapporteringen, ärendemening och avsändare bli offentliga i det diarium som mottagaren registrerar incidentrapporterna i. Förekomsten av den aktuella elproducenten i kombination med uppgiften om att det rör en incidentrapportering ger information till en antagonist som har genomfört ett angrepp mot den aktuella elproducenten som skulle visa att angreppet har blivit upptäckt. Vidare kan uppgifterna påverka elproducenten negativt genom att uppgifterna skulle kunna påverka marknaden och tilltron till den aktuella elproducentens förmåga att motstå angrepp. Detta skulle i sin tur kunna medföra en minskad vilja hos aktörer att rapportera incidenter. Diarier över ärenden och allmänna handlingar är normalt sett offentliga hos myndigheter. I 3 § OSF finns det undantag från den principen genom att vissa diarier hos vissa myndigheter i sin helhet får omfattas av sekretess. Utredningen anser att diarier som innehåller uppgifter om incidentrapportering enligt lagen om cybersäkerhet och lagen om motståndskraft hos kritiska verksamhetsutövare bör kunna omfattas av sekretess och att därmed dessa uppgifter skyddas från de negativa

effekter som offentlighet för uppgifterna kan medföra. Bestämmelsen bör gälla diarier hos MSB, rapporterande myndigheter och tillsynsmyndigheterna eftersom det är dessa myndigheter som kommer att hantera incidentrapporter. MSB är mottagare av incidentrapporter och ska tillgängliggöra informationen till respektive tillsynsmyndighet. Varje rapporterande myndighet kan komma att upprätta en eller flera incidentrapporter.

13.6 En ny sekretessbestämmelse för uppgift i bakgrundskontroll

Utredningens förslag: En bestämmelse om sekretess för uppgifter i en bakgrundskontroll införs i en ny punkt (10) i 35 kap. 1 § OSL som 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 angelägenhet som rör bakgrundskontroll enligt lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare.

En bakgrundskontroll kan innebära att för den enskilde synnerligen känsliga uppgifter lämnas över till arbetsgivaren eller den som annars ska göra bakgrundskontrollen. Det är därför viktigt att det finns ett skydd för att uppgifterna inte används för annat ändamål än det avsedda.

I 35 kap. 1 § OSL finns en bestämmelse som tar sikte på att skydda uppgifter av liknande slag. Ett exempel i nämnda paragraf är skyddet för uppgifter som rör en säkerhetsprövning enligt säkerhetsskyddslagen (2018:585). Utredningens bedömning är därför att uppgifter av detta slag systematiskt passar väl in i paragrafen (som en ny punkt). Det medför en tydlighet i fråga om skyddet för uppgifter som kommer fram vid bakgrundskontrollen. Underlaget i den delen kan innebära tillgång till uppgifter som från integritetssynpunkt kan vara minst lika känsliga som uppgifter ur belastningsregistret, vilket visas upp för arbetsgivaren av den som prövningen avser. Den aktuella bestämmelsen i offentlighets- och sekretesslagen bör därför ändras så att den avser även en angelägenhet som rör bakgrundskontroll enligt den föreslagna lagen.

13.7 Tystnadsplikt för uppgifter som rör bakgrundskontroller hos enskilda

Utredningens förslag: En bestämmelse om tystnadsplikt införs i lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare som innebär att den som med stöd av denna lag har fått del av uppgifter som förekommer i angelägenhet som avser bakgrundskontroller inte obehörigen får röja eller utnyttja dessa uppgifter.

I det allmännas verksamhet tillämpas i stället bestämmelserna i offentlighets- och sekretesslagen (2009:400).

Bestämmelser om sekretess i offentlighets- och sekretesslagen gäller endast i det allmännas verksamhet. Bakgrundskontroller och underlag för sådana kontroller kan dock vara en uppgift som utförs även i enskilda verksamhetsutövare. Uppgifter av de slag som kan förekomma i bedömningarna bör ha samma skydd oavsett i vilken verksamhet som uppgifterna finns. Bestämmelser om tystnadsplikt i enskild verksamhet finns även i flera andra regleringar. En till OSL kompletterande bestämmelse om tystnadsplikt finns till exempel i 8 kap. 1 § säkerhetsskyddslagen (2018:585) där den som med stöd av säkerhetsskyddslagen har fått del av uppgifter som förekommer i angelägenhet som avser säkerhetsprövning inte får obehörigen röja eller utnyttja dessa uppgifter. Mot den bakgrunden anser utredningen att det behövs en till offentlighets- och sekretesslagen kompletterande bestämmelse om tystnadsplikt även för uppgifter som kommer fram om enskildas personliga förhållanden i bakgrundskontroller. Utredningen föreslår att en bestämmelse med sådant innehåll ska föras in i lagen om motståndskraft hos kritiska verksamhetsutövare.

14 Ändringar i säkerhetsskyddsregleringen

14.1 Inledning

Utredningens uppdrag är även att föreslå ändringar som behövs för att uppnå en mer sammanhållen systematik mellan NIS2- och CER-direktiven och säkerhetsskyddsregelverket, särskilt vad gäller tillsynsmyndigheternas befogenheter och sanktionsavgifternas storlek, samt lämna nödvändiga författningsförslag (dir. 2023:30 s. 19).[1] Utredningen kommer i detta kapitel att redogöra för sina förslag om förändringar i säkerhetsskyddsregleringen avseende tillsynsmyndighetens befogenheter och sanktionsavgiftens storlek.

I avsnitt 5.3.4 finns förslag till förändringar i säkerhetsskyddslagen för att uppnå en sammanhållen systematik mellan CER-direktivet och säkerhetsskyddslagen. Vidare finns förslag till undantag från uppgiftsskyldighet avseende säkerhetsskyddsklassificerade uppgifter samt tillträde till säkerhetskänslig verksamhet i avsnitt 5.3.5 och 5.3.6.

14.2 Utgångspunkter för utredningens bedömningar

Sveriges säkerhet kan sammanfattas som skyddet för Sveriges oberoende och bestånd. Skyddet av Sveriges säkerhet är därmed grundläggande för vår säkerhet som nation. Säkerhetsskyddslagen (2018:585) är central för skyddet av dessa intressen. Säkerhetsskyddslagens verktyg för att ingripa mot överträdelser av lagen behöver till sin art och omfattning vara mycket ingripande för att lagens skyddsintressen ska kunna uppnås. Sanktionerna och utformningen av dem

[1] Utredningen har noterat den pågående utredningen om förbättrade möjligheter att skydda Sveriges säkerhet (Ju 2023:23, dir. 2023:152).

ska innebära att det är avskräckande mot att bryta mot lagen, och att inträffade överträdelser snabbt och effektivt ska kunna åtgärdas.

Regeringen har den 15 februari 2024 gett tillsynsmyndigheterna enligt säkerhetsskyddslagen i uppdrag att redovisa hur tillsynsarbete enligt säkerhetsskyddslagstiftningen har bedrivits och fungerat under perioden 1 januari 2021–31 december 2023. Redovisningen ska avse tillsynsärenden eller tillsynsaktiviteter och bland annat innehålla uppgifter om

- antal inledda tillsynsärenden eller tillsynsaktiviteter, med en översiktlig beskrivning av hur dessa handläggs,
- antal utfärdade förelägganden och om dessa förenats med vite samt i förekommande fall uppgift om att beslutet därefter prövats i domstol och om beslutet då fastställts, ändrats eller undanröjts (6 kap. 4 och 6 §§ säkerhetsskyddslagen [2018:585]),
- antal beslut om handräckning inklusive uppgift om vilken åtgärd som handräckningen avsett (6 kap. 5 §) och
- antal beslut om sanktionsavgift inklusive uppgift om vilken bestämmelse som överträdelsen avsett samt i förekommande fall uppgift om att beslutet därefter prövats i domstol och om beslutet då fastställts, ändrats eller undanröjts (7 kap. 1 och 2 §§).

Uppdraget ska redovisas senast den 1 oktober 2024.

Bestämmelserna om sanktioner och ingripande infördes den 1 december 2021 och har således inte varit i kraft under någon längre tid. Det finns inte heller någon utvärdering av hur sanktioner och ingripanden har tillämpats och i vilken effekt dessa har haft på säkerhetsskyddsarbetet. Utredningen har övervägt om det mot bakgrund av regeringens uppdrag till tillsynsmyndigheterna finns anledning att avvakta denna utvärdering. Mot bakgrund av vad regeringen anför i uppdraget avseende det säkerhetspolitiska läget samt hotbilden mot Sverige och svenska intressen är utredningens bedömning att det inte finns anledning att avvakta denna utvärdering när det gäller undersökningsbefogenheter och sanktioner.

14.3 Gällande rätt avseende undersökningsbefogenheter och sanktioner

Genom en ändring i säkerhetsskyddslagen (2018:585) den 1 december 2021 infördes undersökningsbefogenheter för tillsyn samt möjlighet att besluta om åtgärdsföreläggande och sanktionsavgifter.

Tillsynsmyndigheten får enligt 6 kap. 4 § säkerhetsskyddslagen besluta att förelägga den som står under tillsyn att tillhandahålla information och ge tillträde till lokaler och andra utrymmen. Ett sådant beslut får förenas med vite. Av 6 kap. 5 § samma lag framgår att tillsynsmyndigheten får begära handräckning av Kronofogdemyndigheten för att genomföra tillsynsåtgärder.

Enligt 6 kap. 6 § säkerhetsskyddslagen får tillsynsmyndigheten besluta om åtgärdsföreläggande. Ett sådant beslut får förenas med vite.

Tillsynsmyndigheten får enligt 7 kap. säkerhetsskyddslagen besluta om sanktionsavgift vid vissa i lagen angivna överträdelser. Sanktionsavgift enligt säkerhetsskyddslagen får beslutas av tillsynsmyndigheten. Det är sålunda inte obligatoriskt att besluta om en sanktionsavgift vid en överträdelse. I de fall en sanktionsavgift tas ut ska den enligt 7 kap. 3 § samma lag bestämmas till lägst 25 000 kronor och högst 50 miljoner kronor. Sanktionsavgiften för en statlig myndighet, region eller kommun ska dock bestämmas till högst 10 miljoner kronor.

14.4 Tillsynsmyndighetens undersökningsbefogenheter ändras inte

Utredningens bedömning: Det finns inte något behov av att ändra bestämmelserna om tillsynsmyndighetens undersökningsbefogenhet i säkerhetsskyddslagen.

Utredningen konstaterar att de undersökningsbefogenheter som tillsynsmyndigheterna föreslås få i den föreslagna cybersäkerhetslagen (4 kap. 6–7 §§) och lagen om motståndskraft hos kritiska verksamhetsutövare (7 kap. 5–6 §§) är likalydande med de befogenheter tillsynsmyndigheten har i säkerhetsskyddslagen.

Utredningens bedömning är därför att det inte finns något behov av att ändra bestämmelserna om tillsynsmyndighetens undersökningsbefogenhet i säkerhetsskyddslagen.

14.5 Tillsynsmyndighetens möjlighet att ingripa med åtgärdsföreläggande med mera ändras inte

Utredningens bedömning: Det finns inget behov av ändring i säkerhetsskyddslagen avseende bestämmelserna om åtgärdsföreläggande.

Det bör inte införas någon möjlighet att förelägga en verksamhetsutövare att offentliggöra information rörande överträdelser i säkerhetsskyddslagen.

Det bör inte införas någon möjlighet att förelägga verksamhetsutövare att informera användare som kan påverkas av ett betydande cyberhot med mera i säkerhetsskyddslagen.

Utredningen har i förslaget till cybersäkerhetslag och lagen om motståndskraft hos kritiska verksamhetsutövare infört bestämmelser om åtgärdsföreläggande. Vidare har utredningen föreslagit att tillsynsmyndigheten ska få förelägga en verksamhetsutövare enligt cybersäkerhetslagen att offentliggöra information rörande överträdelser samt att informera användare som kan påverkas av ett betydande cyberhot och vilka skydds- eller motåtgärder de kan vidta (5 kap. 7 §).

När det gäller åtgärdsföreläggande överensstämmer bestämmelsen i säkerhetsskyddslagen med de bestämmelser utredningen föreslår i cybersäkerhetslagen och lagen om motståndskraft hos kritiska verksamhetsutövare. Något behov av ändring i säkerhetsskyddslagen avseende åtgärdsföreläggande finns därmed inte.

Utredningens förslag om beslut att förelägga en verksamhetsutövare att offentliggöra information rörande överträdelser i cybersäkerhetslagen bör enligt utredningens bedömning inte införas i säkerhetsskyddslagen. Överträdelser av bestämmelserna i säkerhetsskyddslagen innebär att det i de flesta fall finns en sårbarhet i säkerhetsskyddet och att offentliggöra en sårbarhet är enligt utredningens mening olämpligt.

Förslaget i cybersäkerhetslagen om beslut att förelägga en verksamhetsutövare att informera användare som kan påverkas av ett

betydande cyberhot med mera är utredningens bedömning att ett sådant ingripande inte bör införas i säkerhetsskyddslagen. Detta grundar sig huvudsakligen på att de hot och sårbarheter som kan upptäckas inom denna kontext är av sådan karaktär att de ofta behöver skyddas snarare än offentliggöras. Vidare finns redan en etablerad rapporteringskedja för säkerhetshotande händelser.[2]

14.6 Sanktionsavgiften för enskilda verksamhetsutövare ska höjas

Utredningens förslag: Sanktionsavgiften för enskilda verksamhetsutövare 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.

Utredningens bedömning: Bestämmelsen om sanktionsavgiften för en statlig myndighet, kommun eller region i säkerhetsskyddslagen ska inte ändras.

Sanktionsavgift infördes i säkerhetsskyddslagen den 1 december 2021 för att säkerställa säkerhetsskyddslagstiftningens efterlevnad. Sanktionsavgift ska enligt förarbetena (prop. 2020/21:194 s. 92 f.) i första hand komma i fråga vid åsidosättande av de mest centrala skyldigheterna enligt säkerhetsskyddslagstiftningen. 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 bör beloppsintervallet enligt regeringen vara mycket stort. Regeringen anförde vidare att vid bedömning av sanktionsavgiftens storlek kan den avgiftsskyldiges finansiella ställning ha betydelse.[3] Maximibeloppet

[2] 2 kap. 15–18 §§ Säkerhetspolisens föreskrifter om säkerhetsskydd (PMFS 2022:1).
[3] Prop. 2020/21:194 s. 106 och 140.

bestämdes därför till 50 miljoner kronor. 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 miljoner kronor. Minimibeloppet bestämdes till 25 000 kronor.

Sanktionsavgifter i cybersäkerhetslagen och lagen om motståndskraft hos kritiska verksamhetsutövare

Utredningens förslag avseende sanktionsavgiftens storlek i 5 kap. 13–15 §§ i förslaget till cybersäkerhetslag är följande.

- Sanktionsavgift om minst 5 000 kronor och högst
  - 10 000 000 kronor för offentliga verksamhetsutövare
  - det högsta av 10 000 000 euro eller 2 procent av verksamhetsutövarens totala globala årsomsättning under föregående räkenskapsår för väsentliga verksamhetsutövare,
  - det högsta av 7 000 000 euro eller 1,4 procent av verksamhetsutövarens totala globala årsomsättning under föregående räkenskapsår för viktiga verksamhetsutövare.

Utredningens förslag avseende sanktionsavgift i 8 kap. 6–7 §§ i förslaget till lag om motståndskraft hos kritiska verksamhetsutövare är följande.

- Sanktionsavgift om lägst 5 000 kronor och högst
  - 10 000 000 för offentliga kritiska verksamhetsutövare
  - det högsta av 10 000 000 euro eller 2 procent av den enskilda kritiska verksamhetsutövarens totala globala årsomsättning under föregående räkenskapsår.

Behov av ändring i säkerhetsskyddslagen

TechSverige har anfört att reglerna i säkerhetsskyddslagen är otydliga och att det kan vara svårt för enskilda verksamhetsutövare att bedöma vad som utgör fara för Sveriges säkerhet. Vidare anförs att det inte har gått så lång tid sedan bestämmelserna om sanktionsavgift infördes. Sanktionsavgifterna bör därför inte höjas.

När det gäller behovet av ändring av beloppsintervallet för sanktionsavgiften i säkerhetsskyddslagen ansluter sig utredningen till vad regeringen anfört i kommittédirektivet att det inte är önskvärt att brister i en verksamhetsutövares säkerhetsskydd leder till mindre ingripande åtgärder än brister i andra delar av verksamhetsutövarens verksamhet som inte rör säkerhetskänslig verksamhet.

Utredningen föreslår därför att maximibeloppet för sanktionsavgiftens storlek i säkerhetsskyddslagen ska höjas för enskilda verksamhetsutövare till att motsvara beloppen för väsentliga verksamhetsutövare enligt cybersäkerhetslagen, vilket innebär 120 miljoner kronor eller 2 procent av verksamhetsutövarens totala globala årsomsättning under föregående räkenskapsår. Dock ska minimibeloppet fortsatt vara 25 000 kronor. Den föreslagna höjningen innebär enligt utredningens mening att regeringens ambitioner om att sanktionsavgiftens storlek ska kunna vara avskräckande för alla verksamhetsutövare upprätthålls. Kopplingen av sanktionsavgiftens storlek till verksamhetsutövarens omsättning innebär också att den avgiftsskyldiges finansiella ställning får en större betydelse vid bedömning av avgiftens storlek.

När det gäller offentliga verksamhetsutövare är utredningens bedömning att det inte ska göras någon förändring av avgiftens storlek. Utredningen delar den tidigare bedömningen att den nuvarande avgiften om 10 miljoner kronor är en effektiv, proportionell och avskräckande sanktion också för allvarliga överträdelser av en statlig myndighet, kommun eller region.[4]

[4] Prop. 2020/21:194 s. 103.

14.7 Sanktionen förbud att utöva ledningsfunktion

Utredningens bedömning: Det bör inte införas ett förbud mot att utöva ledningsfunktion i säkerhetsskyddslagen.

Genom bestämmelserna i 5 kap. 8–11 §§ förslaget till cybersäkerhetslag införs sanktionen förbud att utöva ledningsfunktion för att införliva artikel 32.5 b NIS2-direktivet. Sanktionen innebär ett tillfälligt förbud att utöva ledningsfunktion och riktar sig mot varje fysisk person som på nivån för verkställande direktör eller juridiskt ombud har ledningsansvar i en väsentlig verksamhet.[5]

I prop. 2020/21:194 s. 87 konstateras, när det gäller bedömningen av vilka ytterligare administrativa sanktioner och andra möjligheter till ingripande som bör införas i säkerhetsskyddslagen, att förbud mot att bedriva en viss verksamhet inte är en framkomlig väg bland annat eftersom det i många fall är viktigt att en säkerhetskänslig verksamhet fortsätter att bedrivas och att det i vissa fall även finns en skyldighet att bedriva en sådan verksamhet.

Utredningen menar att det finns mindre enskilda verksamhetsutövare där ledningsfunktionen är kritisk för den säkerhetskänsliga verksamhetens bedrivande. Att ingripa mot ledningsfunktionen hos sådana verksamhetsutövare skulle därmed kunna leda till att den säkerhetskänsliga verksamheten lamslås, vilket i sig kan innebära risk för skada för Sveriges säkerhet. Det finns också en risk att en sådan ingripande sanktion får till följd att verksamhetsutövare tvekar att vända sig till tillsynsmyndigheten för att få nödvändig vägledning. Det kan även övervägas om en sådan sanktion enbart ska kunna riktas mot enskilda verksamhetsutövare, eller även offentliga sådana. Den senare gruppen kräver omfattande utredning där konstitutionella frågor behöver belysas, bland annat under vilka förutsättningar det skulle vara möjligt att rikta ett förbud mot en förtroendevald. Utredningen anser att det eventuella behovet och utformningen av en sådan sanktion, inklusive de intresseavvägningar det kan föranleda behöver utredas ytterligare och mer ingående än vad som är möjligt för denna utredning. Som följd ska sanktionen inte föreslås.

[5] SOU 2024:18 s. 272 ff.

14.8 Sanktionen anmärkning

Utredningens bedömning: Det bör inte införas en sanktion om anmärkning i säkerhetsskyddslagen.

Enligt 5 kap. 2 § andra stycket förslaget till cybersäkerhetslag ska tillsynsmyndigheten om den inte finner skäl att ingripa med någon annan sanktion meddela verksamhetsutövaren en anmärkning. Bestämmelsen genomför artikel 32.4 a och 33.4 a NIS2-direktivet.

En motsvarande bestämmelse föreslås införas i 8 kap. 2 § andra stycket lagen om motståndskraft hos kritiska verksamhetsutövare.

Mot bakgrund av att det är obligatoriskt för tillsynsmyndigheten att ingripa om en verksamhetsutövare har åsidosatt vissa angivna skyldigheter enligt cybersäkerhetslagen och lagen om motståndskraft hos kritiska verksamhetsutövare har införts sanktionen anmärkning. Anmärkning kan meddelas om något annat ingripande inte görs.

När det gäller säkerhetsskyddslagen är det inte obligatoriskt att meddela åtgärdsföreläggande eller besluta om administrativ sanktionsavgift. Tillsynsmyndigheten får alltså avstå från att besluta om sanktion. Utredningen bedömer därför att det inte finns något behov av att införa sanktionen anmärkning i säkerhetsskyddslagen.

15 Konsekvensanalys

15.1 Inledning

En utredning ska beskriva konsekvenserna av sina förslag och kraven är angivna i kommittéförordningen (1998:1474). I förordningens 14 § föreskrivs att om förslagen i ett betänkande påverkar kostnaderna eller intäkterna för staten, kommuner, regioner, företag eller andra enskilda, ska en beräkning av dessa konsekvenser redovisas i betänkandet.

Om förslagen innebär samhällsekonomiska konsekvenser i övrigt ska dessa redovisas. När det gäller kostnadsökningar och intäktsminskningar för det allmänna ska utredningen föreslå en finansiering.

Vidare ska enligt 15 § i förordningen eventuella konsekvenser för den kommunala självstyrelsen redovisas. Detsamma gäller eventuella konsekvenser för brottsligheten och det brottsförebyggande arbetet, för sysselsättning och offentlig service i olika delar av landet, för små företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt i förhållande till större företags, för jämställdheten mellan kvinnor och män eller för möjligheterna att nå de integrationspolitiska målen. Därutöver gäller enligt 15 a § i förordningen särskilda krav för förslag till nya eller ändrade regler. För dem ska konsekvenserna även anges på ett sätt som motsvarar kraven i 6 och 7 §§ förordningen (2007:1244) om konsekvensutredning vid regelgivning. Av 6 § i förordningen följer att en konsekvensutredning för förslag till nya eller ändrade regler ska innehålla följande:

1. en beskrivning av problemet och vad man vill uppnå,
2. en beskrivning av alternativa lösningar samt effekterna av att en reglering inte föreslås,
3. uppgifter om vem som berörs av regleringen,
4. uppgifter om kostnadsmässiga samt andra konsekvenser regleringen skulle medföra och en jämförelse av konsekvenserna,

5. en bedömning av om regleringen överensstämmer med eller går utöver de skyldigheter som följer av Sveriges anslutning till Europeiska unionen (EU), och
6. en bedömning av om särskilda hänsyn behöver tas när det gäller tidpunkten för ikraftträdande och om det finns behov av speciella informationsinsatser.

Av 7 § samma förordning följer att om regleringen kan få effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt ska konsekvensutredningen, utöver vad som följer av 6 § och i den omfattning som är möjlig, innehålla en beskrivning av följande:

1. antalet företag som berörs, vilka branscher företagen är verksamma i samt storleken på företagen,
2. tidsåtgången regleringen kan föra med sig för företagen och vad regleringen innebär för företagens administrativa kostnader,
3. andra kostnader den föreslagna regleringen medför för företagen och vilka förändringar i verksamheten som företagen kan behöva vidta till följd av den,
4. i vilken utsträckning regleringen kan komma att påverka konkurrensförhållandena för företagen,
5. hur regleringen i andra avseenden kan komma att påverka företagen, och
6. om särskilda hänsyn behöver tas till små företag vid reglernas utformning.

Av regeringens direktiv följer också därutöver särskilt att utredarens förslag ska utformas så att reglerna blir tydliga och ger så låga administrativa och andra kostnader som möjligt för de kritiska verksamhetsutövarna. I detta ingår enligt regeringen att bedöma de ekonomiska konsekvenserna av förslagen för de behöriga myndigheterna. Det följer också av direktivet att det 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 kom-

munala självstyrelsen ska utöver dess konsekvenser, också de särskilda avvägningar som lett fram till förslaget särskilt redovisas.

I detta kapitel ska konsekvenserna av utredningens förslag redovisas. Nedan kommer konsekvenserna för förslagen som hänför sig till införlivandet av CER-direktivet i svensk rätt att redovisas.

15.2 Regleringsalternativ och beskrivning av uppdraget

Utredningens uppdrag har i huvudsak varit att lämna förslag om hur CER-direktivet kan införlivas i svensk rätt. Syftet med CER-direktivet är att stärka motståndskraften hos kritiska verksamhetsutövare för att upprätthålla motståndskraft i samhällsviktiga tjänster inom sektorerna energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, dricksvatten, avloppsvatten, digital infrastruktur, offentlig förvaltning, rymden och produktion samt bearbetning och distribution av livsmedel (bilaga 1 till CER-direktivet). Det är ett bindande minimidirektiv med innebörd att medlemsstaten får anta bestämmelser i nationell rätt som syftar till att uppnå en högre grad av motståndskraft för kritiska verksamhetsutövare. Förslagen innehåller inga krav som syftar till att uppnå en högre grad av motståndskraft än de som följer av direktivet. Det betyder att den föreslagna regleringen uteslutande är en konsekvens av Sveriges medlemskap i EU och går inte utöver dessa skyldigheter. Effekten av att någon reglering inte kommer till stånd skulle således vara att Sverige inte följer skyldigheterna enligt EU-rätten. I uppdraget har vidare ingått att vid behov lämna förslag på ändring i säkerhetsskyddslagen (2018:585) och offentlighets- och sekretesslagen (2009:400).

15.3 Vem berörs av förslagen?

Lagen om motståndskraft hos kritiska verksamhetsutövare med tillhörande förordning kommer att omfatta kritiska verksamhetsutövare, både offentliga och enskilda sådana. När det gäller offentliga verksamhetsutövare omfattas statliga myndigheter, regioner och kommuner. Enskilda verksamhetsutövare omfattas oavsett i vilken form verksamheten bedrivs. Statliga, regionala och kommunala bolag är enskilda verksamhetsutövare. Det finns inget krav på att en kritisk

verksamhetsutövare ska uppfylla något storlekskrav vilket innebär att även små företag kan komma att omfattas.

Enligt CER-direktivet ska medlemsstaterna identifiera vilka verksamhetsutövare som erbjuder samhällsviktiga tjänster inom sektorerna enligt bilaga 1 till direktivet. För att omfattas av regleringen krävs att verksamhetsutövaren tillhandhåller en sådan samhällsviktig tjänst i eller till Sverige. Vidare krävs att verksamhetsutövaren har en kritisk infrastruktur belägen i Sverige och att en incident skulle få betydande störande effekt på verksamhetsutövarens tillhandahållande av den samhällsviktiga tjänsten. När det gäller tröskelvärdenas nivå se avsnitt 6.4. Dessa verksamhetsutövare benämns som kritiska verksamhetsutövare. De krav som ställs för att bli identifierad som en kritisk verksamhetsutövare medför enligt utredningens mening att antalet identifierade kritiska verksamhetsutövare kommer att vara betydligt färre än det totala antalet verksamhetsutövare i respektive sektor.

15.4 Skyldigheter för dem som omfattas av förslagen

De identifierade kritiska verksamhetsutövarna har särskilda skyldigheter. De ska göra en riskbedömning, vidta åtgärder för att öka motståndskraften, inklusive bakgrundskontroller, och rapportera incidenter, se kapitel 8–9.

CER-direktivet innehåller också bestämmelser om att kritiska verksamhetsutövare av särskild europeisk betydelse har en anmälningsskyldighet och att de under vissa omständigheter ska delta i samråd och rådgivande uppdrag, se kapitel 7.

Enligt lagen om motståndskraft hos kritiska verksamhetsutövare har även vissa myndigheter uppgifter. Det handlar om tillsynsmyndigheter och MSB. Även Polismyndigheten kommer att få uppgifter när det gäller kravet på bakgrundskontroll, se kapitel 9. Enligt utredningens förslag är tillsynen delad mellan olika tillsynsmyndigheter. Innebörden är att det finns olika tillsynsmyndigheter för de olika sektorerna på samma sätt som i cybersäkerhetslagen och NIS-lagen. Såväl MSB som merparten av tillsynsmyndigheterna har redan liknande uppgifter enligt nu gällande NIS-lagen. De föreslås också få motsvarande uppgifter i cybersäkerhetslagen.

Utredningen har i kapitel 8 föreslagit att regeringen ska ge MSB ett uppdrag att tillsammans med tillsynsmyndigheterna se över om och hur MSB:s redan framtagna verktygslådor för arbetet med att öka motståndskraft och annat befintligt stöd behöver anpassa och kompletteras för att kunna användas av kritiska verksamhetsutövare. Vidare har utredningen föreslagit att regeringen ska ge Försvarshögskolan ett uppdrag att tillhandahålla utbildning för kritiska verksamhetsutövares säkerhetsansvariga som ett led i att öka kompetensen att utbilda den egna personalen.

15.5 Ekonomiska konsekvenser

Medlemsstaterna ska enligt artikel 9.4 CER-direktivet säkerställa att dess behöriga myndighet och gemensamma kontaktpunkt har de befogenheter och resurser som krävs för att på ett effektivt och ändamålsenligt sätt fullgöra uppgifterna.

Enligt artikel 10 i direktivet ska medlemsstaterna stödja kritiska verksamhetsutövare för att stärka deras motståndskraft, till exempel genom vägledning och utbildning. Utan att det påverkar regler för statligt stöd får medlemsstaterna även erbjuda ekonomiska resurser om det är nödvändigt och motiverat av allmänt intresse.

Av artikel 18.5 framgår att kommissionen täcker kostnaderna för rådgivande uppdrag avseende kritiska verksamhetsutövare av särskild europeisk betydelse.

Enligt kommittédirektivet ska utredningen bedöma de ekonomiska konsekvenserna av förslagen för det allmänna och för företag eller andra enskilda. Vidare ska utredningen bedöma de ekonomiska konsekvenserna för de behöriga myndigheterna. Leder förslagen till kostnadsökningar för det allmänna ska utredningen föreslå hur dessa ska finansieras.

15.5.1 Utgångspunkter

Samhällsviktiga tjänster, inbegripet kritisk infrastruktur, spelar en oumbärlig roll för att upprätthålla viktiga samhällsfunktioner eller central ekonomisk verksamhet både på den inre marknaden och i Sverige. Att stärka motståndskraften i sådana tjänster är centralt för att förebygga, motstå och hantera incidenter som kan ge allvarliga stör-

ningar. Incidenter kan hindra genomförande av ekonomisk verksamhet, generera omfattande ekonomiska förluster, undergräva förtroende för tjänsternas tillhandahållande och medföra allvarliga konsekvenser för Sveriges och unionens ekonomi. Incidenter kan också medföra allvarliga konsekvenser för invånarna i Sverige.

De samhällsviktiga tjänster som avses i detta förslag tillhandahålls inte bara i Sverige utan även i andra medlemsstater. Störningar och incidenter kan därför vare sig de är avsiktliga eller oavsiktliga och oberoende av var de förekommer påverka enskilda medlemsstater och unionen som helhet. Motståndskraft i sådan kritisk infrastruktur som tillhandhåller samhällsviktiga tjänster är därför viktigt för att den inre marknaden och den svenska marknaden ska fungera väl.

Som framgår av kapitel 6 i betänkandet utgår bestämmelserna om identifiering av kritiska verksamhetsutövare från att det finns en strategi för kritiska verksamhetsutövares motståndskraft samt en nationell riskbedömning. Strategin ska enligt artikel 4 i CER-direktivet antas av varje medlemsstat senast den 17 januari 2026 och samtidigt ska även den nationella riskbedömningen vara genomförd. Identifieringen av de kritiska verksamhetsutövarna ska göras senast den 17 juli 2026. Därefter ska verksamhetsutövarna underrättas om att de identifierats. En riskbedömning ska göras nio månader efter att verksamhetsutövaren har identifierats och tio månader efter dagen för underrättelse om identifiering blir bestämmelserna om krav på åtgärder för motståndskraft tillämpliga, senast i början av 2027.

Uppskattning av antalet verksamhetsutövare

Utredningen har av samtliga föreslagna tillsynsmyndigheter efterfrågat uppgift om antalet statliga myndigheter, regioner, kommuner, företag eller andra enskilda som omfattas av definitionen i respektive kategori av verksamhetsutövare i bilagan till CER-direktivet[1]. Utredningen frågade vidare om antalet statliga myndigheter, regioner, kommuner, företag eller andra enskilda som har identifierats i motsvarande kategori enligt NIS-lagen enligt den lagens tillämpningsområde. De föreslagna tillsynsmyndigheterna har lämnat följande svar.

[1] Statens energimyndighet och Transportstyrelsen har i stället uppskattat hur många aktörer som skulle kunna omfattas inom respektive kategori.

Energi

Statens energimyndighet har uppgett att det är svårt att kartlägga CER-aktörer utifrån den information de har i dag. Statens energimyndighet har inte angett antalet aktörer i respektive sektor utan har i stället gjort en egen uppskattning av vilka aktörer som skulle kunna omfattas inom respektive kategori. För elektricitet cirka 260 aktörer, fjärrvärme cirka 100–200 aktörer, olja/drivmedel cirka 30 aktörer, gas inkl. vätgas cirka 85 aktörer varav cirka 10 aktörer är vätgas.

Antalet aktörer som i dag är anmälda enligt NIS-lagen inom respektive kategori är elektricitet 241 aktörer, olja/drivmedel 16 aktörer och gas 7 aktörer.

Transport

Transportstyrelsen har uppgett att det är svårt att kartlägga CER-aktörer utifrån den information de har i dag. Transportstyrelsen har gjort en initial bedömning av vilka aktörer som skulle kunna omfattas inom respektive undersektor. För luftfart 22 aktörer, järnväg 24 aktörer, vatten 136 aktörer, väg 6 aktörer och kollektivtrafik 22 aktörer, totalt 200 aktörer.

Transportstyrelsen har tidigare uppgett till utredningen att man har 130 tillsynsobjekt enligt NIS-lagen.

Bankverksamhet och finansmarknadsinfrastruktur

Finansinspektionen har uppgett att inom kategorin kreditinstitut finns 125 aktörer, kategorin operatörer av handelsplatser 3 aktörer och kategorin centrala motparter 1 aktör.

Antalet aktörer som i dag är anmälda inom NIS-regleringen är kreditinstitut 10 aktörer, operatör av handelsplatser 1 aktör och central motpart 1 aktör.

Hälso- och sjukvård

Inspektionen för vård och omsorg (kategorin vårdgivare) har uppgett att antalet aktiva organisationer i Vårdgivarregistret är 18 367.

Antalet aktörer som i dag är anmälda enligt NIS-lagen är cirka 250 aktörer.

Läkemedelsverket har uppgett att inom kategorin EU-referenslaboratorier finns 1 aktör, för entiteter som bedriver forskning och utveckling avseende läkemedel saknas uppgift hos Läkemedelsverket om antal aktörer, för entiteter som tillverkar farmaceutiska basprodukter och läkemedel finns 134 aktörer, för entiteter som tillverkar medicintekniska produkter saknas uppgifter men uppskattas finnas högst 1 000 aktörer, för entiteter med tillstånd att bedriva partihandel finns 231 aktörer. Läkemedelsverket har pekat på att det finns svårigheter att utifrån definitionerna i bilagan ange vilka aktörer som kan komma att omfattas.

Dessa aktörer omfattas inte av nuvarande NIS-lag.

Dricksvatten

Livsmedelsverket har uppgivit att det inom kategorin leverantörer och distributörer av dricksvatten finns maximalt 290 aktörer.

Antalet aktörer som i dag är anmälda enligt NIS-lagen är 100.

Avloppsvatten

Livsmedelsverket har uppgivit att det inom kategorin verksamhet som samlar ihop, släpper ut och renar avloppsvatten från tät bebyggelse, hushållsspillvatten eller industrispillvatten finns maximalt 290 aktörer.

Dessa aktörer omfattas inte av nuvarande NIS-lag.

Digital infrastruktur

Post- och telestyrelsen har uppgivit att det finns 704 tillhandahållare av allmänna elektroniska kommunikationsnät och 314 övriga aktörer inom digital infrastruktur.

Antalet aktörer som i dag är anmälda enligt NIS-lagen är 9. Vidare har PTS tillsyn över 40–50 leverantörer av digitala tjänster. Leverantörer av elektroniska kommunikationstjänster omfattas inte av nuvarande NIS-lag.

Rymden

Post- och telestyrelsen har uppgivit att det finns 15 aktörer inom rymdsektorn.

Dessa aktörer omfattas inte av nuvarande NIS-lag.

Produktion, bearbetning och distribution av livsmedel

Livsmedelsverket har uppgivit att när det gäller kategorin livsmedelsföretag som uteslutande bedriver logistikverksamhet och grossisthandel samt storskalig industriell produktion och bearbetning finns ingen direkt motsvarighet i exempelvis livsmedelslagstiftningen eller SNI-systemet vilket bidrar till oklarheter och svårigheter att bedöma vem som träffas av regleringen och därmed hur många. Vidare finns frågetecken kring begreppen och vad som inbegrips.

Dessa aktörer omfattas inte av nuvarande NIS-lag.

Offentlig förvaltning

När det gäller sektorn offentlig förvaltning fanns det den 1 januari 2024 367 myndigheter under regeringen[2]. Här ska också noteras att det finns flera undantag i den föreslagna regleringen som rör statliga myndigheter.

Utredningens bedömning är att det i dag inte går att göra någon tillförlitlig beräkning av hur många av aktörer som anges ovan inom respektive sektor som faktiskt kommer att omfattas av det nya regelverket. Som utredningen konstaterat avsnitt 6.3–4 kommer dock inte samtliga aktörer i sektorn omfattas eftersom en förutsättning är att aktören tillhandahåller en samhällsviktig tjänst. Ett kriterium för att bli identifierad som kritisk verksamhetsutövare är också att en incident skulle få en betydande störande effekt på verksamhetsutövarens

[2] Statskontorets webbplats, inhämtat 2024-06-24

tillhandhållande av den samhällsviktiga tjänsten. En viss vägledning kan dock antalet aktörer som omfattas av den nu gällande NIS-lagen ge.

Utredningen har också noterat regeringens skrivelse Nationell säkerhetsstrategi (skr. 2023/24:168), och vad som framgår i den avseende bland annat fokusområdet Ett motstånds- och konkurrenskraftigt Sverige om att skyddet av samhällsviktig verksamhet ska stärkas (s. 25 ff.).

15.5.2 Ekonomiska konsekvenser för tillsynsmyndigheterna

Utredningens förslag: Regeringen bör för år 2025 och 2026 ge Statens energimyndighet, Transportstyrelsen, Inspektionen för vård och omsorg, Läkemedelsverket, Livsmedelsverket, Post- och telestyrelsen, länsstyrelserna i Norrbottens, Skåne, Stockholms och Västra Götalands län ett förstärkt anslag med en miljon kronor per år.

Utredningens bedömning: De kostnader som förslagen medför för Finansinspektionen bör finansieras inom ramen för befintliga anslag.

Kostnader för löpande tillsyn bör beräknas först när identifieringen av kritiska verksamhetsutövare är genomförd.

Av nedanstående tabell följer vilken myndighet som är tillsynsmyndighet enligt utredningens förslag och tillsynsmyndighetens tillsynsområde.

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

Det handlar alltså om elva myndigheter. Tillsynsmyndigheternas uppgift är att utöva tillsyn över att kritiska verksamhetsutövare uppfyller sina skyldigheter, utföra rådgivande uppdrag inom ramen för tillsyn samt besluta om sanktioner.

Tillsynsmyndigheterna ska också identifiera de kritiska verksamhetsutövare som bedriver verksamhet inom tillsynsområdet, underrätta verksamhetsutövaren och upprätta en förteckning över dessa. Förteckningen ska vidarebefordras till MSB.

Varje tillsynsmyndighet ska meddela föreskrifter om riskbedömning samt om åtgärder och planer för motståndskraft, se kapitel 8.

Flera av de elva tillsynsmyndigheterna bedriver redan tillsyn enligt 17 § förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster. Vidare har utredningen i sitt delbetänkande[4] föreslagit samma myndigheter som tillsynsmyndigheter i 8 § förordningen (2025:000) om cybersäkerhet.

Utredningen föreslog i sitt delbetänkande utökade resurser för 2025 för att tillsynsmyndigheterna ska kunna identifiera vilka verksamhetsutövare som omfattas av cybersäkerhetslagen samt utfärda nya föreskrifter och nya vägledningar utan att samtidigt behöva minska

[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.
[4] SOU 2024:18 s. 334 ff.

ambitionen med tillsyn. De fem nya tillsynsmyndigheterna Läkemedelsverket, länsstyrelserna i Skåne, Stockholms, Västra Götalands och Norrbottens län föreslogs även få medel för att kunna starta upp tillsynsverksamheten.

Kritiska verksamhetsutövare inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur ska inte tillämpa artikel 11 och inte heller kapitlen III, IV och VI i CER-direktivet. Dock ska tillsynsmyndigheten identifiera kritiska verksamhetsutövare, underrätta verksamhetsutövaren och upprätta en förteckning över dessa samt vidarebefordra förteckningen till MSB. Någon tillsyn eller efterlevnadskontroll ska inte bedrivas hos dessa kritiska verksamhetsutövare.

Utredningens bedömning är att det i dag inte är möjligt att dra några tillförlitliga slutsatser om de löpande kostnaderna för tillsynsmyndigheterna eftersom antalet tillsynsobjekt inte är känt och, som det visat sig, är svårt att uppskatta. Det är inte heller nödvändigt att göra någon uppskattning nu eftersom tillsyn inte kommer bedrivas förrän tidigast 2027. Utredningens bedömning är att den löpande kostnaden i stället ska beräknas när samtliga tillsynsmyndigheter har upprättat en förteckning över kritiska verksamhetsutövare.

Tillsynsmyndigheterna måste dock redan när lagen och tillhörande förordning träder i kraft meddela föreskrifter, ta fram en metod för identifiering samt ge vägledning. Både Läkemedelsverket och Livsmedelsverket har också uppgett att definitionerna enligt bilaga 1 i direktivet är oklara. I vissa fall saknar definitionerna motsvarighet i svensk lagstiftning, de förteckningar man hänvisar till är inte konstanta och vissa begrepp är otydliga. Utredningens bedömning är därför att tillsynsmyndigheterna behöver utökade resurser för 2025 och 2026.

När det gäller att bygga upp en tillsynsverksamhet menar utredningen att de föreslagna myndigheterna redan har en tillsynsorganisation eller har fått medel för detta genom förslaget till en ny cybersäkerhetsreglering.

När det gäller tillsynsmyndigheten Finansinspektionen ska endast bestämmelserna om identifiering och att upprätta en förteckning tillämpas för sektorerna bankverksamhet, finansmarknadsinfrastruktur. Utredningen drar för Finansinspektionen slutsatsen att identifiering och upprättande av en förteckning kan komma att medföra ökade kostnader men i så fall endast i en begränsad omfattning. Dessa kostnadsökningar bör därför finansieras inom ramen för befintligt anslag.

När det gäller tillsynsmyndigheten PTS ska endast bestämmelserna om identifiering och att upprätta en förteckning tillämpas för sektorn digital infrastruktur. PTS föreslås i den nya lagen även som tillsynsmyndighet för sektorn rymden. Utredningen drar för PTS slutsatsen att identifiering och upprättande av en förteckning avseende sektorn digital infrastruktur kan komma att medföra ökade kostnader men endast i begränsad omfattning. Dessa kostnadsökningar bör därför finansieras inom ramen för befintligt anslag. Däremot ska samtliga uppgifter utföras när det gäller sektorn rymden. Utredningens bedömning är därför att PTS behöver utökade resurser för 2025 och 2026 för sektorn rymden.

När det gäller bedömningen avseende frågan om avgiftsfinansierad tillsyn hänvisar utredningen till den bedömning som gjordes i delbetänkandet.[5]

15.5.3 Ekonomiska konsekvenser för Myndigheten för samhällsskydd och beredskap

Utredningens förslag: Regeringen bör för år 2025 och 2026 ge Myndigheten för samhällsskydd och beredskap ett förstärkt anslag med en miljon kronor per år.

Utredningens bedömning: Kostnader för stöd vid incidenter får klarläggas av regeringen när identifieringen av kritiska verksamhetsutövare är genomförd.

I detta avsnitt ska de ekonomiska konsekvenserna för MSB analyseras samt förslag till finansiering lämnas.

MSB har redan i dag uppgifter till följd av rådets direktiv 2008/114/EG[6]. Dessa är till viss del likartade dem som föreslås och avser följande. MSB är Sveriges kontaktpunkt och samordnar frågor kring skydd av kritisk infrastruktur (samhällsviktig verksamhet) i Sverige, med relevanta aktörer inom Sverige, med andra medlemsstater och med kommissionen. MSB bistår i arbetet med att identi-

[5] SOU 2024:18 s. 354 f.
[6] Rådets direktiv 2008/114/EG av den 8 december 2008 om identifiering av och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet av att stärka skyddet av denna.

fiera eventuell europeisk kritisk infrastruktur inom de svenska energi- och transportsektorerna.

MSB är vidare kontaktpunkt gentemot EU:s civilskyddsmekanism.

Enligt 2 § förordningen (2008:1002) med instruktion för MSB ska myndigheten senast vid utgången av april månad varje udda årtal lämna en nationell risk- och sårbarhetsbedömning till regeringen. I arbetet ska myndigheten beakta de risk- och sårbarhetsbedömningar som beredskapsmyndigheter lämnar enligt 19 § förordningen (2022:524) om statliga myndigheters beredskap. Myndigheten ska genomföra bedömningen såväl på en övergripande samhällsnivå som beredskapssektorsvis. Av bedömningen ska särskilt allvarliga hot, risker och sårbarheter samt vidtagna och planerade åtgärder framgå.

MSB stödjer också både offentliga och privata aktörer i att identifiera samhällsviktig verksamhet, både inom den egna organisationen, i ett geografiskt område eller för ett ansvarsområde. MSB erbjuder även stöd för att upprätthålla samhällsviktig verksamhet genom att skapa en grundläggande förmåga och uthållighet, bland annat genom arbete med kontinuitetshantering. Stödet finns i form av metod, utbildning, rådgivning och föreläsningar.

MSB har således redan i dag ett omfattande uppdrag när det handlar om samhällets förmåga att förebygga och hantera kriser. Därutöver har myndigheten tagit fram en rad olika verktygslådor för att arbeta med att öka motståndskraften i samhällsviktig verksamhet. Stöden i verktygslådorna bygger på internationella standarder och andra vedertagna vägledningar. MSB har också inom ramen för sitt uppdrag bland annat tagit fram en vägledning[7] som är ett stöd för offentliga aktörer att identifiera samhällsviktig verksamhet som är nödvändig för totalförsvaret, stöd i identifiering av samhällsviktig verksamhet,[8] vägledning för identifiering av samhällsviktig verksamhet[9] samt en sammanställning av de viktiga samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet i vardagen, krisen och kriget.[10]

MSB har likartade uppgifter till följd av regelverket för informationssäkerhets för samhällsviktiga och digitala tjänster samt föreslås

[7] Vägledning för att identifiera samhällsviktig verksamhet som är nödvändig för totalförsvaret, MSB2275, 2023.
[8] Bildspel, MSB1857, 2023
[9] Metod för identifiering av samhällsviktig verksamhet, MSB1408, 2023
[10] Lista med viktiga samhällsfunktioner – Utgångspunkt för att stärka samhällets beredskap, MSB 1844, 2023

få likartade uppgifter i förslaget till ny cybersäkerhetsreglering, se delbetänkandet.[11]

Enligt utredningens förslag ska MSB vara gemensam kontaktpunkt, ta fram medlemsstaternas riskbedömning och meddela föreskrifter med mera.

Sammantaget ska MSB enligt utredningens förslag ha följande uppgifter:

1. Göra den nationella riskbedömningen (se avsnitt 6.1)
2. Upprätta en samlad förteckning över samtliga kritiska verksamhetsutövare utifrån uppgifter från tillsynsmyndigheterna samt vidarebefordra vissa uppgifter till kommissionen (avsnitt 6.7)
3. Meddela föreskrifter om vad som avses med betydande störande effekt (avsnitt 6.4) och om incidentrapportering (avsnitt 8.3)
4. Meddela föreskrifter om åtgärder och planer för motståndskraft för sektorn offentlig förvaltning (avsnitt 8.2)
5. Leda ett samarbetsforum där tillsynsmyndigheterna ingår (avsnitt 10.6)
6. Ta emot incidentrapporter och vidta åtgärder och lämna information (avsnitt 8.3)
7. Vara gemensam kontaktpunkt (kapitel 12)
8. Delta i samråd och rådgivande uppdrag (avsnitt 7.2–3)
9. Delge kommissionen information

Utredningens bedömning är att vissa uppdrag i anslutning till identifieringsförfarandet innebär att MSB kommer att få nya uppgifter när bestämmelserna träder i kraft. Dessa är att ta fram nya föreskrifter, göra en samlad förteckning över kritiska verksamhetsutövare samt att delge information till kommissionen. När det gäller föreskriftsarbetet har MSB inom ramen för sitt befintliga uppdrag gjort en stor del av de förberedande delarna i samverkan med bland annat de myndigheter som nu föreslås vara tillsynsmyndigheter. Utredningens bedömning är dock att MSB bör få en budgetförstärkning med en miljon kronor för att ta fram föreskrifter om vad som avses med en betydande störande effekt.

[11] SOU 2024:18 s. 336 ff.

MSB föreslås vara den myndighet till vilken incidentrapportering ska ske. Myndigheten har motsvarande uppdrag enligt NIS-lagen och föreslås vara CSIRT-enhet enligt cybersäkerhetslagen. Det medför att MSB kan nyttja det digitala rapporteringsverktyg som myndigheten redan har tagit fram för rapportering enligt NIS-lagen och det föreskriftsarbete som gjorts enligt den lagen. I MSB:s befintliga uppdrag ingår operativ hantering av samhällsstörningar vid olyckor, kriser och krig. Incidentrapporter enligt den föreslagna lagen kommer bli en viktig informationskälla i det arbetet och därmed bidra positivt till den hanteringen. När det gäller uppdragen avseende incidentrapportering är det enligt utredningens mening i dag inte möjligt att beräkna vilka kostnader som kommer uppstå. Det saknas uppgift om antalet kritiska verksamhetsutövare som skulle kunna komma att rapportera och därmed också hur många som skulle behöva information. Dessutom kommer kravet på incidentrapportering tillämpas tidigast 2027. Utredningens bedömning är att MSB bör kunna använda det digitala rapporteringsverktyg som myndigheten redan har tagit fram. Föreskriftsarbetet kommer medföra vissa kostnader för MSB men även här bör man kunna utgå från de föreskrifter som redan finns på plats och som kommer tas fram för incidentrapportering enligt cybersäkerhetslagen. Incidentrapporterna kommer som nämnts ovan även att bidra i MSB:s nuvarande uppdrag. Utredningen anser därför att detta föreskriftsarbete ryms inom befintligt anslag. De kostnader som kan komma att uppstå för administration av incidentrapporter och att lämna information vid incidenter kan beräknas översiktligt först när antalet kritiska verksamhetsutövare är känt, dvs. i juli 2026.

Kostnader för det rådgivande uppdraget enligt kapitel 7 täcks av kommissionen. Kostnaden för att delta i samråd enligt kapitel 7 får anses ingå MSB:s ordinarie uppdrag och bör finansieras inom ramen för befintligt anslag.

Uppdraget att göra den nationella riskbedömningen får anses ingå i det uppdrag som MSB har avseende nationell risk- och sårbarhetsbedömning enligt 2 § förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap och i det befintliga anslaget.

15.5.4 Ekonomiska konsekvenser för Polismyndigheten

Utredningens bedömning: Polismyndighetens kostnader för att anpassa it-system för det utdrag ur belastningsregistret som följer av den föreslagna bakgrundkontrollen bör finansieras inom befintligt anslag.

Kostnaden för den löpande hanteringen av utdrag ur belastningsregistret till följd av bakgrundskontroll bör beräknas när identifieringen av kritiska verksamhetsutövare är genomförd och när dessa har gjort den föreskrivna befattningsanalysen.

De löpande kostnaderna bör följas upp i syfte att kunna göra eventuella anpassningar av finansieringen efter de volymer av registerutdrag som den nya lagen föranleder.

Polismyndigheten kommer få ett utökat uppdrag med anledning av förslaget om bakgrundskontroll, genom att de kommer ansvara för att behandla och lämna ut registerutdrag (se kapitel 9). Utredningens förslag innebär att utdrag ur belastningsregistret får begäras för ett nytt ändamål vilket enligt Polismyndigheten bland annat får till följd att ansöknings- och e-tjänsten måste utvecklas anpassas samt att nya blanketter måste tas fram. Utredningens bedömning är att sådana åtgärder bör finansieras inom befintligt anslag.

Som utredningen tidigare konstaterat går det i dag inte att beräkna antalet kritiska verksamhetsutövare på ett tillförlitligt sätt eller hur många befattningar som kommer vara föremål för bakgrundskontroll. Följaktligen är det därför inte heller möjligt att beräkna hur många utdrag ur belastningsregistret som kan bli aktuellt. Utredningens bedömning är att kostnaden för Polismyndigheten för hantering av ansökningarna – som både avser sådana som görs av enskilda individer i Sverige samt tillsynsmyndigheter i andra medlemsstater är helt beroende på hur många sådana utdrag som begärs. En teoretisk bedömning av kostnaden kan därför göras först när samtliga tillsynsmyndigheter har identifierat de kritiska verksamhetsutövarna och när dessa har gjort befattningsanalysen. Denna bedömning bör även följas upp för att se vad det faktiska utfallet blivit. Utredningen noterar särskilt att eftersom utredningens förslag att det aktuella utdraget ur belastningsregistret ska kunna ske kostnadsfritt finns det en risk att fler begär ett sådant utdrag än vad som är avsett, i syfte att de ska slippa betala för liknande typer av utdrag. Det är vidare oklart i vilken

mån kostnaderna kommer att påverkas av att ytterligare slagningar mot Ecris-TCN kommer att behöva göras när de systemen tagits i bruk inom EU. Volymerna bör därför följas upp och Polismyndighetens finansiering anpassas i den mån det behövs.

15.5.5 Ekonomiska konsekvenser för domstolar

Tillsynsmyndighetens beslut om identifiering och beslut om sanktioner får överklagas till allmän förvaltningsdomstol vilket kan medföra en ökning av antalet mål där. Det bedöms dock i så fall endast bli fråga om ett fåtal ytterligare beslut som kommer under prövning i domstol. De ekonomiska konsekvenserna för domstolarna bedöms därför kunna hanteras inom befintliga budgetramar, men den faktiska måltillströmningen bör följas upp.

15.5.6 Ekonomiska konsekvenser för offentliga kritiska verksamhetsutövare

Utredningens bedömning: Kostnaderna för offentliga kritiska verksamhetsutövare som inte finansieras på annat sätt bör finansieras inom befintlig budgetram.

Som framgått tidigare omfattas delar av den offentliga sektorn av regleringens krav. När det gäller statliga myndigheter ingår dessa i en egen sektor, offentlig förvaltning, enligt bilagan till CER-direktivet. För kommuner och regioner krävs däremot för att omfattas av regleringens krav att man ingår i någon av de övriga sektorerna i bilagan.

Detta medför att endast vissa offentliga verksamhetsutövare kommer att omfattas. Vilka dessa är och hur många som kommer att omfattas går inte att beräkna på ett tillförlitligt sätt i nuläget. Det är först när tillsynsmyndigheterna har identifierat de kritiska verksamhetsutövarna och upprättat en förteckning över dessa som antalet kan beräknas. Som framgått tidigare ska identifieringen vara genomförd senast den 17 juli 2026.

SKR har hänvisat till finansieringsprincipen. Den principen innebär att kommuner och regioner inte ska behöva höja skatten eller prioritera om sin verksamhet för att finansiera nya statliga uppgifter.

Den innebär enligt SKR att inga nya obligatoriska uppgifter från staten får införas utan medföljande finansiering till kommuner och regioner.[12] PTS har anfört att kravet på incidentrapportering inte endast medför kostnader när en incident inträffar. Verksamhetsutövaren måste ta fram en process och kanske systemstöd för att övervaka och kunna upptäcka incidenter. Vidare krävs att det finns utbildad personal som kan hantera incidenter när de uppstår.

En kritisk verksamhetsutövare har enligt förslaget skyldigheter. Det handlar bland annat om att göra en riskbedömning, vidta åtgärder för motståndskraft inklusive bakgrundskontroller och att rapportera incidenter. För verksamhetsutövare av särskild europeisk betydelse förslås en anmälningsskyldighet till tillsynsmyndigheten, se kapitel 7. Bestämmelserna om riskbedömning och om skyldigheterna för de kritiska verksamhetsutövarna ska dock tillämpas först nio respektive tio månader efter att tillsynsmyndigheten har underrättat verksamhetsutövaren om att den är en kritisk verksamhetsutövare. Den föreslagna regleringen kommer innebära nya krav för vissa kritiska verksamhetsutövare medan andra redan i dag uppfyller kraven.

Utredningen bedömer att kraven inte kan beskrivas som omfattande, men samtidigt kan de för vissa kritiska verksamhetsutövare vara tillräckligt ingripande och kostnadskrävande för att verksamhetsutövaren kan komma att behöva avsätta resurser. Det är i första hand kravet på att vidta åtgärder för motståndskraft som kan medföra kostnader, eftersom incidenthanteringen aktualiseras ju bara vid problem. Kostnader och tidsåtgång kommer också att vara beroende av befintligt skydd hos verksamheten samt av verksamhetens storlek.

Utredningen menar 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. Vidare ingår att ha en process och system för att hantera, upptäcka och rapportera incidenter. Åtgärderna för att förebygga incidenter kan också förhindra eller begränsa incidenter och medför därmed att kostnader för att hantera incidenter inte uppkommer. Av direktivet framgår också 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).

[12] https://skr.se/skr/ekonomijuridik/ekonomi/finansieringsprincipen.1709.html, inhämtat 2024-01-30.

I sektorn dricksvatten finns redan i dag föreskrifter om fysiskt skydd[13]. Vissa anläggningar i de nu aktuella sektorerna är också redan i dag skyddsobjekt och har genom detta ett förstärkt tillträdesskydd. Detta innebär att flertalet kritiska verksamhetsutövare har vidtagit, i vart fall vissa, åtgärder som krävs enligt utredningens förslag.

På samma sätt som anfördes redan i betänkandet *Informationssäkerhet för samhällsviktiga och digitala tjänster*[14] och utredningens delbetänkande[15] kommer enhetliga regler, tillsyn och möjligheten att få vägledning av tillsynsmyndigheten och MSB bidra till minskade kostnader för verksamhetsutövaren.

Utredningens konstaterade i kapitel 2 att kritiska verksamhetsutövare till allt väsentligt kommer finnas inom det området som benämns samhällsviktig verksamhet och dessa kan redan i dag kan erhålla resurser för att finansiera sådana åtgärder det är fråga om här bland annat inom ramen för befintlig finansiering av krisberedskapsåtgärder. Vidare görs det i arbetet med att stärka det civila försvaret en mängd åtgärder och satsningar för ökad motståndskraft inom de sektorer som nu är i fråga.

Varje år ger också regeringen MSB i uppdrag att fördela cirka en miljard kronor genom anslag 2:4 Krisberedskap för att stärka samhällets krisberedskap och försvarsförmåga. För kommuner och regioner finns *Överenskommelse om kommunernas arbete med krisberedskap och civilt försvar (MSB 2023-17351) och Överenskommelse om regionernas arbete med krisberedskap och civilt försvar (MSB 2023-17352)* som reglerar hur ersättningen som utgör en del av anslag 2:4 Krisberedskap får användas. Ersättningen betalas årligen ut av MSB.

När det gäller den kommunala finansieringsprincipen menar utredningen att förslagen inte är direkt riktade mot kommuner och regioner utan i deras egenskap av tillhandahållare av en samhällsviktig tjänst. Den behöver därför inte tillämpas.

Sammantaget bedömer utredningen att förslagen i vissa fall kan medföra kostnader för offentliga kritiska verksamhetsutövare, men övergripande för hela offentliga sektorn även besparingar. Vidare görs som nämnts redan stora satsningar på områdena krisberedskap och totalförsvar bland annat för att stärka motståndskraften. Det anges också i artikel 20 att det kan komma att finnas ekonomiska resurser på

[13] Livsmedelsverkets föreskrifter (LIVSFS 2008:13) om åtgärder mot sabotage och annan skadegörelse riktad mot dricksvattenanläggningar.
[14] SOU 2017:36 s. 276.
[15] SOU 2024:18.

unionsnivå tillgängliga för att stärka kritiska verksamhetsutövares motståndskraft. De ekonomiska konsekvenserna för offentliga kritiska verksamhetsutövare som inte kan finansieras på annat sätt bedöms inte vara omfattande och föreslås därför finansieras inom verksamhetsutövarens befintliga budgetram.

15.5.7 Ekonomiska konsekvenser för enskilda kritiska verksamhetsutövare

Utredningens bedömning: Förslagen innebär för närvarande inte några ekonomiska konsekvenser för enskilda kritiska verksamhetsutövare. När antalet kritiska verksamhetsutövare har identifierats och riskbedömningar har genomförts kan det dock finnas anledning att överväga om det finns behov av att införa statligt stöd för dem.

Utredningen bedömer att regleringen inte får effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt.

Med enskilda verksamhetsutövare avses fysiska och juridiska personer som bedriver verksamhet och inte är en statlig myndighet, region eller kommun. Det ställs inte krav på viss storlek av verksamhetsutövaren vilket innebär att även små företag kan komma att omfattas.

Kraven för att bli identifierad som en kritisk verksamhetsutövare, se avsnitt 6.3, medför att endast vissa enskilda verksamhetsutövare kommer att omfattas. Vilka dessa är och hur många som kommer att omfattas av utredningens förslag är svårt att ange i nuläget.

Den föreslagna regleringen kommer att innebära nya krav för vissa kritiska verksamhetsutövare medan andra redan i dag uppfyller kraven. Utredningen bedömer att kraven inte kan beskrivas som omfattande, men samtidigt är de tillräckligt ingripande och kostnadskrävande för att vissa kritiska verksamhetsutövare kan komma att behöva avsätta resurser. Det är i första hand kravet på att vidta åtgärder för motståndskraft, eftersom incidenthanteringen bara aktualiseras vid problem. Tidsåtgången kommer också att vara beroende av verksamhetens storlek.

PTS har anfört att kravet på incidentrapportering inte endast medför kostnader när en incident inträffar. Verksamhetsutövaren måste

ta fram en process och kanske systemstöd för att övervaka och kunna upptäcka incidenter. Vidare krävs att det finns utbildad personal kan hantera incidenter när de uppstår.

Utredningen menar på samma sätt som för offentliga verksamhetsutövare att det i uppdraget att tillhandahålla en samhällsviktig tjänst även 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. Vidare ingår att ha en process och system för att hantera, upptäcka och rapportera incidenter. Åtgärderna för att förebygga incidenter kan också förhindra eller begränsa incidenter och medför därmed att kostnader för att hantera incidenter inte uppkommer. Av direktivet framgår också 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[16]. 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 utredningens förslag.

Vissa verksamhetsutövare kan också ha fått ersättning för säkerhetsåtgärder som även kan främja motståndskraften i kritisk infrastruktur enligt till exempel elberedskapslagen (1997:288) för att vidta beredskapsåtgärder och förordningen (2022:511) om elektronisk kommunikation för att beakta totalförsvarets behov. I förordningen (2018:1300) om statligt stöd för driftsäkra och robusta elektroniska kommunikationer finns bestämmelser om statligt stöd till företag för att genomföra vissa åtgärder för driftsäkra och robusta elektroniska kommunikationer i syfte att skydda kommunikationerna mot allvarliga hot och påfrestningar i fredstid och vid höjd beredskap. PTS tilldelades 130 miljoner kronor för budgetåret 2024.

På samma sätt som anfördes redan i betänkandet *Informationssäkerhet för samhällsviktiga och digitala tjänster*[17] och utredningens delbetänkande[18] kommer enhetliga regler, tillsyn och möjligheten att få

[16] Livsmedelsverkets föreskrifter (LIVSFS 2008:13) om åtgärder mot sabotage och annan skadegörelse riktad mot dricksvattenanläggningar.
[17] SOU 2017:36 s. 276.
[18] SOU 2024:18.

vägledning av tillsynsmyndigheten att bidra till minskade kostnader för verksamhetsutövaren.

Det anges också i artikel 20 att det kan komma att finnas ekonomiska resurser på unionsnivå tillgängliga för att stärka kritiska verksamhetsutövares motståndskraft.

Utredningens bedömning i nuläget är att förslagen inte kommer innebära några ekonomiska konsekvenser för enskilda kritiska verksamhetsutövare. När antalet kritiska verksamhetsutövare har identifierats och riskbedömningar har genomförts kan det dock finnas anledning att överväga om det finns behov av att införa statligt stöd. Det bör då beaktas i vilken utsträckning sådant stöd har införts i andra medlemsstater.

Det ska vidare beaktas att kraven kommer att gälla samtliga enskilda verksamhetsutövare inom sektorn, inte bara i Sverige utan även inom hela EES. Den föreslagna regleringen innebär därför att reglerna om motståndskraft i samhällsviktiga tjänster blir enhetliga i Sverige och hela unionen. Förslaget bör därför underlätta för alla typer av företag som vill verka på den inre marknaden och därmed förbättra konkurrensen. Genom gruppen för kritiska entiteters motståndskraft som inrättats enligt artikel 19 underlättas samarbetet mellan medlemsstaterna och informationsutbytet om frågor som rör CER-direktivet. Utredningen bedömer därför att regleringen inte får effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt.

15.5.8 Ekonomiska konsekvenser för konsumenter och andra användare

Förslagen innebär krav på kritiska verksamhetsutövare inom vissa angivna sektorer. Utredningen har konstaterat att det måste anses ingå i uppdraget att tillhandahålla en samhällsviktig tjänst att också vidta grundläggande säkerhetsåtgärder. I de fall sådana åtgärder inte har vidtagits kan det inte uteslutas att kostnader för sådana åtgärder kan avspegla sig i priset. Detta ska dock vägas mot de kostnader som kan uppkomma för konsumenter och andra användare på grund av brister i motståndskraften i den samhällsviktiga tjänsten.

15.6 Övriga konsekvenser

15.6.1 Konsekvenser för det kommunala självstyret

Utredningens bedömning: Förslagen innebär en viss inskränkning i självstyrelsen. Med hänsyn till det stora intresset av att stärka motståndskraften hos kritiska verksamhetsutövare är inskränkningen nödvändig.

När det gäller förslagens konsekvenser för det kommunala självstyret ansluter sig utredningen till den bedömning som gjordes av regeringen i propositionen med förslag till NIS-lag och som utredningen gjort i sitt delbetänkande.[19]

I betänkandet om införlivning av NIS-direktivet anfördes att det finns ett antal värden som kan tillgodoses genom kommunal självstyrelse, som demokrativärden och effektivitetsvärden.

Vid analysen av konsekvenser för kommunalt självstyre kunde enligt den utredningen följande frågor användas:

1. Har förslaget betydelse för den lokala demokratin – återverkar det på kommunalpolitikernas handlingsutrymme eller medborgarnas möjlighet att utöva inflytande i systemet?
2. Påverkar förslaget uppgiftsfördelningen mellan staten och kommunerna?
3. Innebär förslaget statlig regelstyrning eller tillsyn över kommunal verksamhet?
4. Innebär förslaget att man inom någon del av den kommunala verksamheten inför nya rättigheter för medborgarna? Föreslås domstolskontroll av den kommunala verksamheten?

Utredningen anför vidare att det finns lagstiftning som inte påverkar den kommunala självstyrelsen på det sätt som avses. Det anges att kommuner och regioner ska kunna omfattas av säkerhetsföreskrifter med mera av produktionsmässig karaktär. I de situationerna blir det enligt den utredningen inte aktuellt att göra en prövning av den föreslagna lagstiftningen utifrån de värden som den kommunala självstyrelsen är satt att värna.

[19] SOU 2024:18 s. 358 f.

I betänkandet gjordes därför bedömningen att förslagen inte påverkade den kommunala självstyrelsen på sätt som avses i 15 § kommittéförordningen (1998:1474). Det hänvisades till att förslagen avsåg krav på säkerhetsåtgärder och incidentrapportering som omfattar kommuner och regioner i deras egenskap av tillhandahållare av en samhällsviktig tjänst på samma sätt som andra leverantörer av samhällsviktiga tjänster.

I propositionen om förslag till NIS-lag anförde regeringen att förslagen innebar att kommuner och landsting kan bli skyldiga att vidta säkerhetsåtgärder och att rapportera incidenter. Dessa nya åligganden för kommuner och landsting innebar enligt regeringens bedömning en viss inskränkning i självstyrelsen. Regeringen bedömde dock med hänsyn till det stora intresset av att öka säkerheten i nätverks- och informationssystem att inskränkningen var nödvändig. Utredningen ansluter sig till detta synsätt.

15.6.2 Konsekvenser för brottsligheten och det brottsförebyggande arbetet

Utredningens förslag om krav på riskbedömning och åtgärder för motståndskraft samt incidentrapportering förebygger både avsiktliga angrepp och så kallade handhavandefel. Förslagen bör enligt utredningens mening leda till att brott som riktas mot samhällsviktiga tjänster förebyggs, upptäcks, förhindras och beivras.

15.6.3 Konsekvenser för jämställdheten och de integrationspolitiska målen

Utredningen bedömer att förslagen inte berör jämställdheten mellan kvinnor och män eller möjligheterna att nå de integrationspolitiska målen.

15.6.4 Särskild hänsyn till små företag

Utredningens bedömning: Mot bakgrund av syftet i lagen om motståndskraft hos kritiska verksamhetsutövare är utredningens bedömning att det inte ska tas någon särskild hänsyn till små företag vid utformning av regleringen. Dock bör små företags behov av stöd särskilt identifieras.

När det gäller utformningen av regleringen i lagen om cybersäkerhet är utredningens bedömning att det, mot bakgrund av regleringens syfte, inte bör tas någon annan särskild hänsyn än att bestämmelserna ska tillämpas först tio månader efter att beslutet om identifiering delgetts den kritiska verksamhetsutövaren.

Som utredningen konstaterat ovan kan även små företag komma att omfattas av förslagen under förutsättning att de identifieras som kritiska verksamhetsutövare. Utredningens bedömning är dock att kravet på att en incident ska få betydande störande effekt på tillhandahållandet av tjänsten kommer medföra att endast ett begränsat antal små företag kommer att omfattas. För de små företag som identifieras som kritiska verksamhetsutövare kommer ställas samma krav som på övriga kritiska verksamhetsutövare. Detta skulle kunna innebära en något större börda för små företag.

Den föreslagna regleringen kommer innebära nya krav för vissa kritiska verksamhetsutövare medan andra redan i dag uppfyller kraven. Detta gäller även små företag. Utredningen menar också att det, oavsett storlek på verksamhetsutövaren, i uppdraget att tillhandahålla en samhällsviktig tjänst även 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. Utredningen bedömer att kraven inte kan beskrivas som omfattande, men samtidigt är de tillräckligt ingripande och kostnadskrävande för att verksamhetsutövaren behöver avsätta resurser. Det är i första hand kravet på att vidta åtgärder för motståndskraft eftersom incidenthanteringen bara aktualiseras vid problem. Tidsåtgången kommer också att vara beroende av verksamhetens storlek. Se avsnitt 15.5.7 när det gäller redan gällande krav på åtgärder och befintlig finansiering.

På samma sätt som anfördes redan i betänkandet *Informationssäkerhet för samhällsviktiga och digitala tjänster*[20] och utredningens delbetänkande[21] kommer enhetliga regler, tillsyn och möjligheten att få vägledning av tillsynsmyndigheten också bidra till minskade kostnader för verksamhetsutövaren. Utredningen föreslår vidare att MSB inom ramen för sitt stödjande uppdrag särskilt ska identifiera små företags behov av stöd.

Mot bakgrund av den föreslagna regleringens syfte bedömer utredningen att det inte ska tas någon särskild hänsyn till små företag vid utformning av regleringen. Som anförs ovan bör dock små företags behov av stöd särskilt identifieras.

Genom förslaget i lagen om cybersäkerhet att kritiska verksamhetsutövare, oavsett storlek, ska omfattas av den föreslagna cybersäkerhetslagen under förutsättning att den kritiska verksamhetsutövaren dels bedriver verksamhet som omfattas av bilaga 1 eller 2 i NIS2-direktivet, dels uppfyller kravet på att vara etablerad i Sverige, kommer vissa små företag genom att de identifierats som en kritisk verksamhetsutövare omfattas av cybersäkerhetslagen. Utredningen har i avsnitt 6.6 avseende dessa verksamhetsutövare föreslagit att cybersäkerhetslagen ska börja gälla först tio månader efter att den kritiska verksamhetsutövaren delgetts beslutet om identifiering. Utredningen har noterat att regeringen i promemoria Fö2024/01285 har lämnat förslag på ny förordning om stöd till åtgärder för cybersäkerhet avseende ekonomiskt stöd för i huvudsak kapacitetsuppbyggnad inom cybersäkerhet till små och medelstora företag.

Utredningens bedömning är att det, mot bakgrund av regleringens syfte, inte bör tas någon annan särskild hänsyn vid regleringens utformning än att bestämmelserna i cybersäkerhetslagen ska tillämpas först efter tio månader efter att beslutet om identifiering delgetts den kritiska verksamhetsutövaren.

[20] SOU 2017:36 s. 276.
[21] SOU 2024:18 s. 357 f.

15.6.5 Behov av speciella informationsinsatser

Utredningens bedömning: Det finns inget behov av informationsinsatser med anledning av den föreslagna lagen med tillhörande förordning.

Myndigheten för samhällsskydd och beredskap har redan i dag en webbplats, www.msb.se/nis där även information om CER-direktivet finns. MSB har vidare uppgett att det pågår ett arbete för att ytterligare förbättra tillgången till information. Myndigheten för samhällsskydd och beredskap ska enligt utredningens förslag leda ett samarbetsforum där tillsynsmyndigheterna ingår. Syftet med forumet ska vara att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn. I detta uppdrag bör också anses ingå att samordna information om den nya regleringen. Utredningen anser därför inte att det behövs ytterligare informationsinsatser med anledning av den föreslagna lagen med tillhörande förordning.

16 Ikraftträdande med mera

I detta kapitel ska utredningen ta ställning till när lagen om motståndskraft hos kritiska verksamhetsutövare ska träda i kraft och behovet av följdändringar i annan lagstiftning. Vidare redovisas utredningens förslag på regeringsuppdrag till vissa myndigheter.

16.1 Lagen om motståndskraft hos kritiska verksamhetsutövare

Utredningens förslag: Lagen och förordningen om motståndskraft hos kritiska verksamhetsutövare ska träda i kraft den 1 augusti 2025.

Av artikel 26 följer att medlemsstaterna senast den 17 oktober 2024 ska anta och offentliggöra de bestämmelser som är nödvändiga för att följa direktivet. Bestämmelserna ska tillämpas från den 18 oktober 2024.

I direktivet anges vidare vissa andra tidsfrister för medlemsstaterna.

En strategi för kritiska verksamhetsutövare ska enligt artikel 4 antas senast den 17 januari 2026. Av artikel 5 framgår att medlemsstaternas riskbedömning ska göras senast den 17 januari 2026. Senast den 17 juli 2026 ska medlemsstaterna enligt artikel 6 identifiera de kritiska verksamhetsutövarna för de sektorer och undersektorer som anges i bilagan.

Utredningen föreslår att lag och förordning som ska innehålla direktivets krav träder i kraft den 1 augusti 2025.

16.2 Offentlighets- och sekretesslagen (2009:400) och offentlighets- och sekretessförordningen (2009:641)

Utredningens förslag: Bestämmelserna i 15 kap 3 c §, 18 kap. 8 d § och 18 kap. 9 § offentlighets- och sekretesslagen (2009:400) ska träda i kraft den 1 januari i fråga om lagen (2025:000) om cybersäkerhet och i övrigt den 1 augusti 2025.

Bestämmelsen i 35 kap. 1 § 10 offentlighets- och sekretesslagen (2009:400) ska träda i kraft den 1 augusti 2025.

Utredningens bedömning: Ändringen i 3 § offentlighets- och sekretessförordningen (2009:641) ska träda i kraft den 1 januari 2025 i fråga om diarium över incidenter enligt lagen (2025:000) om cybersäkerhet och i övrigt den 1 augusti 2025.

Ändringen i bilagan till offentlighets- och sekretessförordningen (2009:641) ska träda i kraft den 1 augusti 2025.

Utredningen har i sitt delbetänkande föreslagit att lagen om cybersäkerhet ska träda i kraft den 1 januari 2025 och föreslår i detta betänkande att lagen om motståndskraft hos kritiska verksamhetsutövare ska träda i kraft den 1 augusti 2025. Utredningens förslag när det gäller sekretessfrågor rör båda lagförslagen. Det kan därför övervägas om de ändringar i offentlighets- och sekretesslagen (2009:400) och offentlighets- och sekretessförordningen (2009:641) som gäller lagen om cybersäkerhet ska träda i kraft redan den 1 januari 2025.

Utredningens bedömning är att bestämmelserna om sekretess bör träda i kraft samtidigt som respektive lag och förordning träder i kraft. Det kan inte uteslutas att incidenter som ska rapporteras inträffar kort efter cybersäkerhetslagens ikraftträdande och det vore otillfredsställande om det under en övergångstid saknades sekretesskydd. Samma bedömning gör sig gällande avseende övriga bestämmelser.

16.3 Följdändringar i annan författning

16.3.1 Bestämmelser som upphävs

Utredningens bedömning: Genom att direktivet 2008/114/EG upphör att gälla ska hänvisningar till detta direktiv i förordning (2007:1119) med instruktion för Affärsverket svenska kraftnät, förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap, förordning (2010:185) med instruktion för Trafikverket och förordning (2014:520) med instruktion för Statens energimyndighet upphävas.

Utredningens förslag:

1. Förordningen (2007:1119) med instruktion för Affärsverket svenska kraftnät ska ändras på så sätt att 3 § 13 ska upphävas.
2. Förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap ska ändras på så sätt att 17 a § ska upphävas.
3. Förordningen (2010:185) med instruktion för Trafikverket ska ändras på så sätt att 4 § 7 ska upphävas.
4. Förordningen (2014:520) med instruktion för Statens energimyndighet ska ändras på så sätt att 3 § 3 ska upphävas.

Av artikel 27 framgår att direktivet 2008/114/EG ska upphöra gälla med verkan från och med den 18 oktober 2024.

Genom att direktivet 2008/114/EG upphör att gälla ska hänvisningar till detta direktiv i andra författningar upphävas samma dag som den nya lagen och förordningen träder i kraft, dvs. den 1 augusti 2025.

16.4 Övrigt

En förutsättning för att tillsynsmyndigheterna ska kunna identifiera kritiska verksamhetsutövare inom sitt tillsynsområde är att föreskrifterna om när en störande effekt är betydande har meddelats. Utredningen föreslår i 9 § i förordningen om motståndskraft hos kritiska verksamhetsutövare och i avsnitt 6.4 att Myndigheten för samhällsskydd och beredskap (MSB) efter att ha berett tillsynsmyndighe-

terna tillfälle att yttra sig meddelar sådana föreskrifter. Regeringen bör därför ge MSB och tillsynsmyndigheterna i uppdrag att påbörja arbetet med denna föreskrift så att identifieringen kan påbörjas när lagen och förordningen träder i kraft.

Kritiska verksamhetsutövare ska kunna få stöd (avsnitt 8.2) och enligt utredningen bör detta stöd finnas på plats när tillsynsmyndigheterna börjar identifiera kritiska verksamhetsutövare. MSB har inom ramen för sitt uppdrag tagit fram en rad olika verktygslådor för att arbeta med att öka motståndskraften i samhällsviktig verksamhet. Stöden i verktygslådorna bygger på internationella standarder och andra vedertagna vägledningar. MSB bör därför få ett uppdrag att tillsammans med tillsynsmyndigheterna se över om och hur dessa verktygslådor och annat befintligt stöd behöver anpassa och kompletteras för att kunna användas av kritiska verksamhetsutövare. MSB bör också inom ramen för sitt stödjande uppdrag särskilt identifiera små företags behov av stöd.

Utredningen föreslår också att regeringen ger Försvarshögskolan ett uppdrag att ta fram och tillhandahålla en utbildning för de befattningshavare som ansvarar för säkerheten hos kritiska verksamhetsutövare.

Utredningen föreslår i 1 kap. 6 § att regeringen i föreskrifter får ange vilka bestämmelser om riskbedömning, åtgärder för motståndskraft, bakgrundskontroller och incidentanmälan som har motsvarande verkan. Tillsynsmyndigheterna bör ges i uppdrag att utreda vilka kategorier av verksamhetsutövare inom respektive tillsynsområde som omfattas av annan lag eller andra bindande unionsrättsakter med krav på riskbedömning, åtgärder för motståndskraft, bakgrundskontroller och incidentrapportering vars verkan minst motsvarar verkan av skyldigheterna enligt lagen.

17 Författningskommentar

17.1 Förslaget till lag om motståndskraft hos kritiska verksamhetsutövare

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.

Paragrafen genomför artikel 1.1 i CER-direktivet och behandlas i avsnitt 5.1.

Första stycket anger syftet med lagen. Uttrycken motståndskraft, kritisk verksamhetsutövare och samhällsviktig tjänst definieras i 2 §.

Av *andra stycket* framgår att lagen genomför CER-direktivet utom vad gäller Sveriges skyldighet att anta en strategi för kritiska entiteters motståndskraft. Hänvisningen till direktivet är dynamisk och avser därmed den vid varje tidpunkt gällande lydelsen av direktivet. Det innebär att ändringar i direktivet får omedelbart genomslag. Det samma gäller för övriga EU-rättsakter som hänvisas till i lagen, se bland annat 2 § och 11 § samt 2 kap. 2 §.

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.

Bestämmelsen genomför artikel 2 och 17.1 i CER-direktivet och anger definitioner av ord och begrepp i lagen. Definitionerna behandlas i kapitel 5–8. Flera av definitionerna motsvarar vad som följer av artikel 2 i CER-direktivet, medan vissa har anpassats till svensk rätt och ytterligare några definitioner har tillförts utöver vad som följer av direktivet. Vissa definitioner hänvisar till andra EU-förordningar. Hänvisningarna är dynamiska och avser därmed den vid varje tidpunkt gällande lydelsen av rättsakterna. Numreringen har ändrats jämfört med den som följer av CER-direktivet.

Definitionen av *CER-direktivet* har tillförts för att möjliggöra enklare hänvisningar till direktivet i de fall det är nödvändigt.

Uttrycket *enskild verksamhetsutövare* utgör en anpassning av direktivets begrepp *privat entitet*, som inte definieras i direktivet. Definitionen träffar alla juridiska personer och fysiska personer som bedriver verksamhet, och som inte är en statlig myndighet, region eller kommun. Begreppet analyseras i avsnitt 5.2.2.

Definitionen av *incident* överensstämmer med direktivets definition (artikel 2.3). Begreppet analyseras i avsnitt 8.3.

Definitionen av *kritisk infrastruktur* överensstämmer med direktivets definition (artikel 2.4) av samma begrepp.

Uttrycket *kritisk verksamhetsutövare* är en anpassning av direktivets begrepp (artikel 2.1) *kritisk entitet*. Bakgrunden till definitionen redogörs för i avsnitt 5.2.3 och 6.2.2.

Uttrycket *kritisk verksamhetsutövare av särskild europeisk betydelse* motsvarar materiellt direktivets definition (artikel 17.1) av begreppet. Rekvisiten för att anses vara en sådan verksamhetsutövare redogörs för i avsnitt 7.2.

Uttrycket *motståndskraft* motsvarar materiellt direktivets definition (artikel 2.2) med språklig anpassning till lagens begrepp *kritisk verksamhetsutövare*.

[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)

Begreppet *NIS2-direktivet* har tillförts för att förenkla hänvisningar till det direktivets bestämmelser i den mån de behöver göras i författning. Hänvisningen till direktivet är dynamisk och avser därmed den vid varje tidpunkt gällande lydelsen av direktivet.

Med *offentlig verksamhetsutövare* avses en statlig myndighet, en region eller en kommun. I lagen undantas vissa offentliga verksamhetsutövare från lagens tillämpningsområde. Begreppet ska inte förväxlas med direktivets begrepp *offentlig förvaltning* som är en sektor i direktivets bilaga. I den sektorn ingår endast statliga myndigheter med de undantag som anges i lagen. Begreppen har redogjorts för i avsnitt 5.2.1.

Uttrycket *risk* motsvarar direktivets definition av begreppet (artikel 2.6).

Begreppet *riskbedömning* motsvarar direktivets definition (artikel 2.7).

Uttrycket *samhällsviktig tjänst* överensstämmer med samma begrepp i direktivet (artikel 2.5) och redogörs för i avsnitt 6.2.2 och 6.3. Begreppet är inte synonymt med *samhällsviktig verksamhet* som förekommer i annan författning.

Begreppet *standard* har samma definition som i direktivet (artikel 2.8).

Uttrycket *teknisk specifikation* har samma definition som i direktivet (artikel 2.9).

Lagens tillämpningsområde

3 § Lagen gäller för enskilda och offentliga verksamhetsutövare som har identifierats som kritiska enligt 2 kap. 1 §.

Paragrafen genomför artikel 1.1 och anger lagens tillämpningsområde samt förutsättningarna för att omfattas. Övervägandena behandlas i kapitel 5 och avsnitt 6.3.

4 § För kritiska verksamhetsutövare inom sektorerna bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur gäller inte 3–6 kap.

Paragrafen genomför artikel 8 i direktivet och anger att kritiska verksamhetsutövare inom vissa sektorer inte omfattas av kraven i lagen. Övervägandena behandlas i avsnitt 5.3.2. Definitionen av de aktuella sektorerna följer av bilagan till CER-direktivet. Av bestämmelsen

följer att tillsynsmyndigheten ska identifiera kritiska verksamhetsutövare i dessa sektorer men att de inte omfattas av de krav som normalt följer av ett sådant utpekande. Det innebär också att bestämmelserna om tillsyn och sanktioner inte ska tillämpas för dessa kritiska verksamhetsutövare.

Undantag från lagens tillämpningsområde

Krav i andra författningar

5 § Lagen gäller inte för sådant som regleras i lagen om cybersäkerhet (2025:000).

Paragrafen genomför artikel 1.2 i direktivet och behandlas i avsnitt 5.3.1. Innebörden är att den föreslagna lagen ska vara subsidiär till cybersäkerhetslagen, men endast i sådana frågor som är reglerade och skyddade av den lagen.

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.

Paragrafen genomför artikel 1.3 och övervägandena behandlas i avsnitt 5.3.3. Som en följd ska inte heller bestämmelserna om ingripande och sanktioner gälla avseende åsidosättande av skyldigheter.

Offentliga verksamhetsutövare

7 § Lagen gäller inte för regeringen, Regeringskansliet, utlandsmyndigheter, kommittéväsendet, Riksrevisionen, Riksdagens ombudsmän, Sveriges Riksbank, Riksdagsförvaltningen och Sveriges domstolar.

Paragrafen innehåller undantag för vissa angivna statliga myndigheter och genomför delvis artikel 2.10. Övervägandena behandlas i avsnitt 5.2.1.

Av definitionen i artikel 2.10 framgår vad som avses med en offentlig förvaltningsenhet och att undantag görs för rättsväsendet, parlament och centralbank.

I begreppet Sveriges domstolar ingår specialdomstolarna Arbetsdomstolen och Försvarsunderrättelsedomstolen. Däremot ska aktörer med funktioner kopplade till rättsväsendet ändå kunna omfattas av lagen.

Riksdagen är ingen myndighet utan en beslutande församling. Detsamma gäller region- och kommunfullmäktige.

Att även Regeringskansliet, utlandsmyndigheterna och kommittéväsendet är undantagna från lagen utvecklas i avsnitt 5.2.1.

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.

Paragrafen som innehåller flera typer av undantag från lagens tillämpningsområde genomför artikel 1.5–7 och övervägandena behandlas i avsnitt 5.3.4.

Av *första stycket* följer att lagen inte gäller för statliga myndigheter som *till övervägande del* bedriver brottsbekämpning eller säkerhetskänslig verksamhet. Regeringen bemyndigas i *tredje stycket* att i förordning ange vilka som ska anses vara sådana myndigheter.

Av *andra stycket* följer en begränsning i lagens tillämpningsområde avseende offentliga verksamhetsutövare som förvisso bedriver säkerhetskänslig verksamhet eller brottsbekämpning, men inte gör det till övervägande del (jfr första stycket). Sådana aktörer ska som utgångspunkt tillämpa bestämmelserna. Om den samhällsviktiga tjänsten till någon del omfattas av säkerhetsskydd ska dock inte kraven i lagen om motståndskraft hos kritiska verksamhetsutövare till-

lämpas i den delen. Den samhällsviktiga tjänsten omfattas således av lagens bestämmelser, men endast i den del som inte omfattas av säkerhetsskydd.

I *fjärde stycket* anges ett undantag för enskilda verksamhetsutövare som bedriver säkerhetskänslig verksamhet. Innebörden av undantaget är detsamma som redogjorts för avseende offentliga verksamhetsutövare i *andra stycket*.

9 § Skyldighet att lämna uppgifter enligt denna lag gäller inte uppgifter som är säkerhetsskyddsklassificerade enligt säkerhetsskyddslagen (2018:585).

Bestämmelsen genomför artikel 1.8 och övervägandena behandlas i avsnitt 5.3.5. Paragrafen medför en begränsning i den uppgiftsskyldighet som följer av lagen. Uppgiftsskyldigheten omfattar inte säkerhetsskyddsklassificerade uppgifter. Säkerhetsskyddsklassificerade uppgifter definieras i 1 kap. 2 § andra stycket säkerhetsskyddslagen (2018:585). Innebörden av bestämmelsen blir att varken enskilda eller offentliga verksamhetsutövare är skyldiga rapportera sådana uppgifter eller på annat sätt lämna sådana uppgifter till någon annan aktör. Säkerhetsskyddsklassificerade uppgifter kan avse såväl uppgifter som härrör från verksamhetsutövarens egen verksamhet som uppgifter från myndigheter och andra.

10 § Tillsynsmyndighetens undersökningsbefogenheter i denna lag omfattar inte sådana delar av områden, lokaler eller andra utrymmen där säkerhetskänslig verksamhet enligt säkerhetsskyddslagen (2018:585) bedrivs.

Paragrafen genomför artikel 1.8 och övervägandena behandlas i avsnitt 5.3.6. Bestämmelsen innebär en begränsning i tillsynsmyndighetens undersökningsbefogenheter, och medför att tillsynsmyndigheten inte har rätt att få tillgång till delar av sådana områden, lokaler med mera där säkerhetskänslig verksamhet bedrivs. Begränsningen ska dock inte uppfattas som att den träffar alla sådana utrymmen där säkerhetsskyddsåtgärder har vidtagits, utan endast till sådana platser där den säkerhetskänsliga verksamheten bedrivs och i direkt anslutning till detta. Om det finns en del av området eller byggnaden som omfattas av säkerhetsskyddsåtgärder men där säkerhetskänslig verksamhet inte bedrivs medför detta ingen begränsning av tillsynsmyndighetens undersökningsbefogenheter i denna del.

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 de andra sektorerna, 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].

Paragrafen genomför artikel 5 och övervägandena behandlas i avsnitt 6.1.

Bestämmelsen innehåller ett bemyndigande för regeringen avseende den nationella riskbedömningen som Sverige ska göra. I förordningen föreslås att Myndigheten för samhällsskydd och beredskap ska göra den nationella riskbedömningen. Den nationella riskbedömningen ska beaktas när tillsynsmyndigheterna identifierar kritiska verksamhetsutövare. Tillsynsmyndigheten måste därför få del av de delar av riskbedömningen som gäller för tillsynsområdet. Den nationella riskbedömningen ska också utgöra ett underlag för de kritiska verksamhetsutövarna när de gör sin riskbedömning enligt 4 kap. 1 §. Det innebär att de också måste få del av relevanta delar av den nationella riskbedömningen. På motsvarande sätt föreslås en skyldighet för tillsynsmyndigheter och kritiska verksamhetsutövare att lämna information till stöd för framtagandet av den nationella riskbedöm-

[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).

ningen, se vidare 7 kap. 2 och 3 §§. Hänvisningen till EU-rättsakterna är dynamiska och avser därmed den vid varje tidpunkt gällande lydelsen av respektive rättsakt.

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.

Paragrafen genomför artikel 6.1, 6.3 och 6.5 (delvis). Övervägandena behandlas i avsnitt 6.5

Identifiering som kritisk verksamhetsutövare medför att flera skyldigheter inträder för verksamhetsutövaren. Av *första stycket* framgår att den underrättelse som anges i artikel 6.3 ska ske genom ett beslut som kan överklagas. Skyldigheterna kan vid överklagande även inhiberas till dess att frågan om identifiering slutligt avgjorts av domstolen. Det är domstolen som prövar ett yrkande om inhibition.

I *andra stycket* anges de relevanta tidpunkterna när olika skyldigheter börjar gälla, samtliga beräknade från dagen efter det att verksamhetsutövaren fick del av beslutet. Skyldigheten att göra en riskbedömning börjar gälla en månad innan övriga skyldigheter inträder.

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.

Paragrafen genomför artikel 6.2 och 7.1 och övervägandena behandlas i avsnitt 6.3 samt 6.4.

Första stycket innehåller de kriterier som ska vara uppfyllda för att bli identifierad som kritisk verksamhetsutövare enligt 1 §. För att tillhandahålla en tjänst krävs att tjänsten på något sätt är tillgänglig för den svenska marknaden. Detta medför att Sverige inte kan identifiera en verksamhetsutövare som kritisk om den har kritisk infrastruktur i Sverige men den samhällsviktiga tjänsten inte tillhandahålls i Sverige, utan i en annan medlemsstat. Den som uppfyller kravet på att tillhandahålla en samhällsviktig tjänst bedriver också verksamhet. Hänvisningen till direktivet är dynamisk och avser därmed den vid varje tidpunkt gällande lydelsen av direktivet.

Kritisk infrastruktur definieras i 1 kap. 2 § 4. Definitionen är mycket bred och kan träffa byggnader, nätverks- och informationssystem, en maskin eller annat. Det saknas nedre gräns för vad som kan utses utgöra ”en del” av den kritiska infrastrukturen. Därför kan alla delar av en kritisk infrastruktur träffas hur små de än är. Ledning för bedömningen kan hämtas i vilken påverkan som en störning eller ett bortfall skulle ha på tillgängligheten hos den samhällsviktiga tjänsten.

I 8 § i den föreslagna förordningen anges vilka kriterier som ska beaktas när medlemsstaterna tar fram tröskelvärden för att fastställa om en störande effekt är betydande. Det kan till exempel avse antalet användare, andra sektorers grad av beroende, incidentens effekt, tillgången till alternativa sätt att erbjuda tjänsten med mera. Även syftet med direktivet ska beaktas vid fastställande av tröskelvärdena. Ytterligare bestämmelser om när en störande effekt är betydande får meddelas i myndighetsföreskrift. Det är alltså en betydande störning på tillhandahållande av tjänsten som avses och inte för verksamhetsutövarens verksamhet.

Begreppet betydande störande effekt som används för att identifiera kritiska verksamhetsutövare ska inte blandas ihop med begreppet betydande störning som reglerar vilka incidenter en kritisk verksamhetsutövare ska rapportera.

Av *andra stycket* framgår vad tillsynsmyndigheten ska beakta i arbetet med att identifiera kritiska verksamhetsutövare.

I *tredje stycket* har införts ett bemyndigande för att föreskrifterna kan behöva gå utöver vad som kan meddelas med stöd av 8 kap. 7 § regeringsformen (verkställighetsföreskrifter). I förordningen regleras vilka kriterier som ska beaktas vid bedömningen av när en störande effekt är betydande och att MSB får, efter att ha gett tillsynsmyndigheterna tillfälle att yttra sig, meddela ytterligare föreskrifter.

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.

Övervägandena behandlas i avsnitt 5.3, 6.5 och 6.6.

Av *första stycket* framgår att beslutet ska innehålla en upplysning om de tidsfrister inom vilka verksamhetsutövarens skyldigheter börjar gälla. Paragrafen upplyser även om bestämmelserna i cybersäkerhetslagen som medför att verksamhetsutövare som identifierats som kritiska enligt denna lag omfattas av lagen om cybersäkerhet och att de är väsentliga verksamhetsutövare enligt den lagen.

Av *andra stycket* framgår att beslutet i vissa angivna fall ska innehålla en upplysning om att vissa verksamhetsutövare endast ska identifieras, utan att skyldigheter uppstår för dem, se avsnitt 5.3.2.

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.

Övervägandena behandlas i avsnitt 5.3.4. Bestämmelsen innebär att om en verksamhetsutövare invänder att den samhällsviktiga tjänsten till någon del utgör säkerhetskänslig verksamhet ska tillsynsmyndigheten underrätta motsvarande tillsynsmyndighet enligt säkerhetsskyddsregelverket. Bestämmelsen införs tillsammans med en korresponderande bestämmelse i säkerhetsskyddslagen som tar sikte på vad den som är tillsynsmyndighet enligt säkerhetsskyddsregelverket är skyldig att göra med anledning av en sådan underrättelse.

Underrättelse om avidentifiering

5 § Om tillsynsmyndigheten beslutar att en verksamhetsutövare inte längre är kritisk ska den omedelbart underrätta verksamhetsutövaren om detta.

Paragrafen genomför artikel 6.5 delvis. Övervägandena behandlas i avsnitt 6.5. Paragrafen reglerar situationen att en verksamhetsutövare inte längre bedöms vara kritisk, och följderna det får. Om verksamhetsutövaren endast var identifierat som kritisk av den tillsynsmyndighet som nu avidentifierar den upphör också samtliga skyldigheter enligt lagen att gälla omedelbart. Om verksamhetsutövaren däremot har identifierats som kritisk av flera tillsynsmyndigheter behåller den sin status som kritisk, om än inte längre i den sektor som den nu avidentifierats från.

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.

Bestämmelsen genomför artikel 6.3 och 6.5 (delvis) och övervägandena behandlas i avsnitt 6.7. Av 34 § förordningen framgår att tillsynsmyndigheterna ska upprätta en förteckning över kritiska verksamhetsutövare för sina respektive tillsynsområde. Tillsynsmyndigheten ska lämna förteckningen till MSB som enligt 10 § förordningen ska upprätta en samlad förteckning över samtliga kritiska verksamhetsutövare.

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 för bankverksamhet, finansmarknadsinfrastruktur och digital infrastruktur.

Av anmälan ska det framgå vilken samhällsviktig tjänst som tillhandahålls och till eller i vilka medlemsstater den tillhandahålls.

Paragrafen genomför artikel 17.2 och övervägandena behandlas i avsnitt 7.2.

I *första stycket* anges en skyldighet för de kritiska verksamhetsutövare som tillhandahåller den samhällsviktiga tjänsten till eller i minst sex medlemsstater att anmäla detta till sin tillsynsmyndighet.

I *andra stycket* regleras vad en sådan anmälan ska innehålla. Dessa uppgifter är nödvändiga för att kunna identifiera kritiska verksamhetsutövare av särskild europeisk betydelse. Uppgifterna ska lämnas till kommissionen som efter ett samråd med behöriga myndigheter och den berörda kritiska verksamhetsutövaren kan fastställa att den berörda kritiska verksamhetsutövaren är en kritisk verksamhetsutövare av särskild europeisk betydelse. En definition av begreppet finns i 1 kap. 2 § 6.

Vem som är tillsynsmyndighet regleras i förordningen om motståndskraft hos kritiska verksamhetsutövare.

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.

Paragrafen genomför artikel 17.2 och övervägandena behandlas i avsnitt 7.2.

I *första* stycket ges ett bemyndigande till regeringen att bestämma vem som ska delta i samrådet. I den föreslagna förordningen föreslås att MSB ska delta i samrådet. I MSB:s uppdrag ska även ingå att, efter samråd med berörd tillsynsmyndighet, informera kommissionen om tjänsten som omfattas av samrådet bedöms vara en samhällsviktig tjänst.

Av *andra* stycket framgår att berörd kritisk verksamhetsutövare ska delta i samrådet.

Hänvisningarna till direktivet är dynamiska och avser därmed den vid varje tidpunkt gällande lydelsen av direktivet.

Underrättelse om identifiering

3 § Den myndighet regeringen bestämmer ska underrätta en kritisk verksamhetsutövare om kommissionens underrättelse om att en kritisk verksamhetsutövare är att betrakta som kritisk verksamhetsutövare av särskild europeisk betydelse.

Bestämmelsen om skyldigheter i 5 § ska tillämpas från och med dagen den kritiska verksamhetsutövaren mottagit kommissionens underrättelse.

Paragrafen genomför artikel 17.3–4 och övervägandena behandlas i avsnitt 7.2.

I *första stycket* ges ett bemyndigande till regeringen att bestämma vem som ska underrätta den kritiska verksamhetsutövaren att kommissionen fastställt att den är att betrakta som en kritisk verksamhetsutövare av särskild europisk betydelse. En definition av begreppet finns i 1 kap. 2 § 6. Närmare bestämmelser finns i förordningen om motståndskraft hos kritiska verksamhetsutövare.

I *andra stycket* anges när den kritiska verksamhetsutövarens skyldigheter med anledning av ett rådgivande uppdrag kan börja tillämpas.

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 4–6 kap.

Paragrafen genomför artikel 18.1–2 och övervägandena behandlas i avsnitt 7.3.

Av *första stycket* framgår att ett rådgivande uppdrag anordnas av kommissionen. Detta kan ske på initiativ av Sverige, en annan medlemsstat eller kommissionen. I och med att det genomförs inom ramen för en tillsyn blir bestämmelser om tillsynsmyndighetens undersökningsbefogenheter tillämpliga. Därmed är det tillsynsmyndigheten som bedömer vilken åtkomst till uppgifter, system och anläggningar som är nödvändig för utförande av det rådgivande uppdraget. När det gäller säkerhetsskyddsklassificerade uppgifter och tillträde eller åtkomst till säkerhetskänslig verksamhet finns bestämmelser i 1 kap. 9–10 §§.

Ett rådgivande uppdrag för en kritisk verksamhetsutövare av särskild europeisk betydelse i Sverige kräver samtycke. I förordningen om motståndskraft hos kritiska verksamhetsutövare regleras att MSB kan begära att kommissionen anordnar ett rådgivande uppdrag och att det är MSB som efter samråd med den berörda kritiska verksamhetsutövaren av särskild europeisk betydelse och dennas tillsynsmyndighet som samtycker till ett sådant uppdrag. MSB lämnar också förslag på experter till det rådgivande uppdraget.

Bestämmelser om säkerhetsgodkännande av den som ska delta i ett rådgivande uppdrag finns i 6 kap. 7 §. Vad som avses med ett säkerhetsgodkännande behandlas i avsnitt 9.4.

I *andra stycket* regleras syftet med ett rådgivande uppdrag.

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 §.

Paragrafen genomför artikel 18.3 och övervägandena behandlas i avsnitt 7.3.

I bestämmelsen regleras en skyldighet för dessa verksamhetsutövare att tillhandahålla information till MSB. Uppgiftsskyldigheten har sin grund i att kommissionen och medlemsstater (artikel 18.3) kan begära viss information, relevanta delar av riskbedömningen, förteckning över vidtagna relevanta åtgärder och tillsyns- eller efterlevnadskontrollåtgärder. Skyldigheten att tillhandahålla informationen skulle kunna inträffa innan den tiomånadersfrist som anges i 2 kap. 1 § har löpt ut. Om detta skulle inträffa bör MSB enligt utredningens bedömning avvakta med sin begäran. Det är MSB som ska bedöma om den begäran som har inkommit är motiverad och som ansvarar för att tillhandhålla begärda uppgifter. I 34 § 5 förordningen om motståndskraft hos kritiska verksamhetsutövare regleras skyldigheten för tillsynsmyndigheten att tillhandahålla uppgifter.

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.

Paragrafen genomför artikel 12 och behandlas i avsnitt 8.1.

Av *första* och *andra stycket* framgår att verksamhetsutövarens riskbedömning ska innehålla en redogörelse för alla relevanta risker som skulle kunna leda till en incident. Detta inkluderar risker för naturolyckor och risker orsakade av människan. CER-direktivet nämner särskilt risker av sektorsövergripande eller gränsöverskridande slag, olyckor, naturkatastrofer, hot mot folkhälsan och hybridhot samt andra antagonistiska hot, inklusive terroristbrott. En riskbedömning ska vidare beakta om andra sektorer som omfattas av direktivet är beroende av den samhällsviktiga tjänst som erbjuds av den kritiska verksamhetsutövaren och om den kritiska verksamhetsutövaren är beroende av samhällsviktiga tjänster från dessa andra sektorer. Detta gäller även om dessa tjänster levereras från angränsande medlemsstater eller tredjeländer.

I *tredje stycket* finns krav på uppdatering av riskbedömningen.

Fjärde stycket innehåller ett bemyndigande. Av förordningen framgår att tillsynsmyndigheterna och MSB kan meddela föreskrifter.

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.

Paragrafen genomför artikel 13.1–2 och behandlas i avsnitt 8.2.

I *första stycket* regleras syftet med åtgärderna som ska säkerställa verksamhetsutövarnas motståndskraft. Stycket innehåller också en uppräkning av vilka förmågor åtgärderna ska säkerställa hos verksamhetsutövaren.

Att *förhindra incidenter* innefattar åtgärder för katastrofriskreducering och klimatanpassning. *Reagera på, stå emot och begränsa konsekvenserna av incidenter* inkluderar genomförande av risk- och krishanteringsförfaranden och protokoll samt varningsrutiner. *Återhämta sig från incidenter*, innefattar åtgärder för kontinuitetshantering och identifiering av alternativa försörjningskedjor, för att återuppta tillhandahållandet av den samhällsviktiga tjänsten. *Säkerställa ett tillfredsställande fysiskt skydd av lokaler och kritisk infrastruktur*, inkluderar exempelvis stängsel, barriärer, verktyg och rutiner för övervakning av områdesgränser, detektionsutrustning och åtkomstkontroller. *Säkerställa ändamålsenlig hantering av personalsäkerhet* inkluderar till exempel 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 och fastställande av de kategorier av personer som måste genomgå sådana bakgrundskontroller samt fastställande av lämpliga utbildningskrav och kvalifikationer. Bakgrundkontroller behandlas särskilt i kapitel 6 i den föreslagna lagen. *Öka kunskapen om åtgärderna för motståndskraft hos berörd personal* inkluderar exempelvis att öka medvetenheten om åtgärderna i 1–5 hos berörd personal, med vederbörlig hänsyn till utbildningskurser, informationsmaterial och övningar.

Enligt *andra stycket* ska verksamhetsutövaren också upprätta en plan för motståndskraft.

Tredje stycket innehåller ett bemyndigande. Av förordningen framgår att tillsynsmyndigheterna och MSB kan meddela föreskrifter. Föreskriftsrätten omfattar även bakgrundskontroller enligt 6 kap. i den föreslagna lagen, eftersom de är en delmängd av åtgärderna för motståndskraft avseende personalsäkerhet enligt första stycket.

3 § Kritiska verksamhetsutövare ska utse en samverkansansvarig som utgör kontaktpunkt för berörda myndigheter.

Paragrafen genomför artikel 13.3 och behandlas i avsnitt 8.2.

Bestämmelsen innebär att verksamhetsutövaren ska upprätthålla en funktion för samverkan med myndigheter. Detta innebär att den kritiska verksamhetsutövaren kan välja mellan att peka ut en specifik individ eller en funktion för att fullgöra uppgiften.

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.

Paragrafen genomför artikel 15.1 och behandlas i avsnitt 8.3.

I bestämmelsen regleras skyldigheten att rapportera incidenter. Begreppet incident definieras i 1 kap. 2 § 3 som varje händelse som kan medföra en betydande störning, eller som medför en störning, av tillhandahållandet av en samhällsviktig tjänst. Verksamhetsutövaren ska rapportera incidenter utan onödigt dröjsmål vilket innebär att en första rapport ska lämnas senast 24 timmar från det att verksamhetsutövaren fått kännedom om incidenten. En detaljerad rapport ska sen lämnas en månad efter den första rapporten. I 24 § förordningen regleras vad som särskilt ska beaktas vid bedömningen om en incident medför en betydande störning. I 26 § förordningen regleras övergripande vad en incidentrapport ska innehålla. Vad en incidentrapport ska innehålla och vad som utgör en betydande störning bör preciseras i myndighetsföreskrifter.

2 § Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om vad som utgör en betydande störning och om incidentrapporteringen enligt 1 §.

Paragrafen behandlas i avsnitt 8.3 och innehåller ett bemyndigande. Av 25 § förordningen framgår att MSB får meddela föreskrifter om betydande störning och incidentrapporteringen.

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.

Paragrafen genomför artikel 13.1 e (delvis) och artikel 14.1 (delvis) samt behandlas i avsnitt 9.3.2. Bestämmelserna i detta kapitel ansluter till kraven i 4 kap. 2 § första stycket 5. Kapitlet om bakgrundskontroll utgör endast en delmängd av personalsäkerheten, som därutöver bland annat består av utbildning av personalen. Av 4 kap. 2 § tredje stycket följer att regeringen eller den myndighet regeringen bestämmer får föreskriva om åtgärder för motståndskraft, vilket bakgrundskontroller är en del av.

Denna bestämmelse anger syftet med bakgrundskontrollen, som är att bedöma om den enskilde är lämplig att delta i sådana befattningar där deltagandet kan orsaka skada på den samhällsviktiga tjänsten. Deltagande i befattning är mycket brett och träffar anställda, men även konsulter eller andra som på något sätt kan delta i den aktuella befattningen. Det rör sig om deltagande genom både fysisk som logisk behörighet som kan leda till skada på den samhällsviktiga tjänsten. Således omfattas även deltagande som endast sker på distans, trots att fysiskt tillträde saknas.

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.

Bestämmelsen genomför artikel 13.1 e (delvis) och 14.1 (delvis) och behandlas i avsnitt 9.3.3.

Av *första stycket* följer en skyldighet för verksamhetsutövaren att upprätta och hålla en befattningsanalys uppdaterad. Ingångsvärdena ska vara den egna riskbedömningen och utifrån den ska av befattningsanalysen åtminstone framgå vilka befattningar deltagande kan orsaka mer än ringa skada på den samhällsviktiga tjänsten. Deltagande i sådana befattningar kräver att bakgrundskontroll ska genomföras innan deltagande, samt med viss periodicitet under deltagande.

I *andra stycket* anges kraven på när befattningsanalysen ska uppdateras. Det första kravet är ”vid behov”, och det ankommer på verksamhetsutövaren att bedöma när sådant behov uppstår. Det kan exempelvis utgöras av att omfattningen av den samhällsviktiga tjänsten förändras, organisatoriska förändringar eller att it-system byts ut med förändrade processer eller behörigheter som följd. Uppdatering ska dock minst ske en gång om året.

Rätten att utfärda föreskrifter avseende bakgrundskontroller följer av den allmänna föreskriftsrätten avseende åtgärder för motståndskraft.

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.

Bestämmelsen genomför artikel 13.1 e (delvis) samt 14.1 (delvis). Paragrafen behandlas i avsnitt 9.3.4 och anger när en bakgrundskontroll ska genomföras.

Av *första stycket* följer att bedömningen tar sikte på individens lämplighet att delta i verksamhet där deltagandet kan orsaka mer än ringa skada på den samhällsviktiga tjänsten, och att det gäller för både den som redan har sådan möjlighet eller kan komma att få. Bakgrundskontrollen ger viss grundläggande information (se 5 §) som stöd för bedömningen av individens lämplighet (och huruvida den

har sårbarheter), men vid lämplighetsbedömningen bör även annan information som typiskt sett framkommer vid rekryteringar och intervjuer vägas in. Om en person farit med osanning rörande sina meriter, betyg eller genomförda utbildningar bör detta typiskt sett kunna tala emot en persons lämplighet.

Av *andra stycket* följer ett förbud för verksamhetsutövaren att låta en person som inte genomgått bakgrundskontroll och bedömts lämplig, på något sätt delta i en sådan befattning som följer av befattningsanalysen. Vid rekrytering utgör bestämmelsen inte ett hinder mot rekrytering i sig, men den rekryterade får då endast delta i sådan befattning där den kan orsaka ingen eller endast ringa skada på den samhällsviktiga tjänsten. På motsvarande sätt kan en person som under pågående anställning/deltagande bedöms olämplig (eller där bakgrundskontroll inte görs i tid) omplaceras till en befattning där motsvarande skada inte är möjlig. När kravet ska börja tillämpas för verksamhetsutövaren (jfr 2 kap. 1 §) träffar det även befintlig personal, som alltså måste ha genomgått bakgrundskontroll och bedömts lämpliga innan de får delta i sådan befattning.

I *tredje stycket* anges att en ny bakgrundskontroll och bedömning av lämplighet ska göras när det finns skäl för det, och annars senast inom två år från att den senaste bakgrundskontrollen genomfördes. Bestämmelsen ger en möjlighet att genomföra förnyade bakgrundskontroller om verksamhetsutövaren anser att det föreligger skäl för det.

Rätten att utfärda föreskrifter avseende bakgrundskontroller följer av den allmänna föreskriftsrätten avseende riskhanteringsåtgärder.

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.

Bestämmelsen genomför artikel 14.2–3. Bestämmelsen behandlas i avsnitt 9.3.5 och anger bakgrundskontrollens innehåll och omfattning.

I *paragrafen* poängteras att den kontrollen avser endast är skyldig att visa upp sådana handlingar och utdrag som följer *på förfrågan* av verksamhetsutövaren. Verksamhetsutövaren är således skyldig att be-

gära detta från den enskilde för att uppfylla kraven på att ha genomfört en bakgrundskontroll.

Av *punkten ett* följer kraven på giltig och godtagbar id-handling. Huruvida en id-handling är giltig torde vara en relativt enkel bedömning. Utredningen anser att samma typ av handlingar som godtas enligt Skatteverkets föreskrifter (SKVFS 2009:14)[6] om identitetskort ska anses utgöra godtagbara identitetshandlingar.

Enligt *punkten två* ska ett särskilt utdrag ur belastningsregistret hämtas in och visas upp. Det får vid tidpunkten för bakgrundskontrollen, dvs. vid uppvisandet, maximalt vara ett år gammalt.

Rätten att utfärda föreskrifter avseende bestämmelsen följer den allmänna föreskriftsrätten avseende åtgärder för motståndskraft.

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.

Bestämmelsen behandlas i avsnitt 9.3.5 och genomför artikel 13 (delvis). Bestämmelsen medför en skyldighet för verksamhetsutövaren att föra anteckning om att sådana handlingar som avses i 4 § har visats upp. Anteckningar får inte göras avseende innehållet i det som visas upp, utan endast att det har skett.

Av *andra stycket* följer ett bevarandekrav för verksamhetsutövaren. Offentliga verksamhetsutövare träffas i regel av andra krav på bevarande, medan stycket behövs för att ålägga enskilda verksamhetsutövare en sådan skyldighet.

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.

[6] Senaste lydelse enligt SKVFS 2021:9.

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.

Bestämmelserna genomför artikel 18.5 och 19.2 samt behandlas i avsnitt 9.4. Paragraferna hanterar det som CER-direktivet benämner säkerhetsgodkännande och innebär att de för svenskt vidkommande ska hanteras på samma sätt som bakgrundskontroller.

I *6 §* regleras regeringens rätt att utfärda sådana säkerhetsgodkännanden för deltagare i CERG.

I *7 §* ges regeringen eller den myndighet regeringen bestämmer möjlighet att genomföra och utfärda sådana godkännanden för individer som ska ingå i ett rådgivande uppdrag. MSB föreslås få ansvar för sådana säkerhetsgodkännanden.

Hänvisningarna till direktivet är dynamiska och avser därmed den vid varje tidpunkt gällande lydelsen av direktivet.

7 kap. Tillsyn

Tillsynsmyndighet

1 § Den myndighet som regeringen bestämmer ska vara tillsynsmyndighet.

Paragrafen genomför artikel 9.1 och behandlas i avsnitt 10.2.

Det ska finnas en eller flera tillsynsmyndigheter för varje sektor. I 29 § i förordningen anges vilka myndigheter som är tillsynsmyndigheter för vilken sektor.

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 §.

Paragrafen genomför artikel 9.1 och 18.1. Övervägandena behandlas i avsnitt 6.1, 7.3 och 10.4.

Syftet med tillsyn är att kunna bedöma om verksamhetsutövare uppfyller lagens krav. Resultatet av en tillsyn kan ligga till grund för ingripanden och sanktioner.

Bestämmelsen medför att tillsynsmyndighetens befogenheter blir tillämpliga vid genomförandet av ett rådgivande uppdrag. Syftet med ett rådgivande uppdrag är enligt 3 kap. 4 § att bedöma de åtgärder den kritiska verksamhetsutövaren av särskild europeisk betydelse har vidtagit för att uppfylla skyldigheterna i 4–6 kap. Kommissionen anordnar efter samtycke från MSB det rådgivande uppdraget.

Bestämmelsen innebär också en skyldighet för tillsynsmyndigheterna att ge MSB den information som behövs för att myndigheten ska kunna upprätta den nationella riskbedömningen.

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 §.

Paragrafen genomför artikel 18.7, 21.1 och 21.2 och behandlas i avsnitt 6.1 och 10.5.

Tillsynsmyndigheten kan ålägga en verksamhetsutövare att tillhandahålla sådan information som behövs för att bedöma om verksamhetsutövaren uppfyller lagens krav. Detta inkluderar bland annat information som behövs för att bedöma de åtgärder för motståndskraft som verksamhetsutövaren vidtagit, dokumenterade riskbedömningar och planer för motståndskraft.

Bestämmelsen innebär också att tillsynsmyndigheterna ges möjlighet att inhämta de uppgifter som behövs från kritiska verksamhetsutövare för att den nationella riskbedömningen ska kunna upprättas.

Vissa begränsningar i uppgiftsskyldigheten finns i 1 kap. 9 § när det gäller säkerhetsskyddsklassificerade uppgifter.

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.

Paragrafen genomför artikel 18.7, 21.1 och behandlas i avsnitt 10.5.

Paragrafen ger tillsynsmyndigheten tillträde till områden lokaler och andra utrymmen, dock inte bostäder, i den utsträckning det behövs för att kunna utöva tillsyn.

Vissa begränsningar i tillsynsmyndighetens undersökningsbefogenheter finns i 1 kap. 10 § när det gäller säkerhetskänslig verksamhet.

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.

Paragrafen genomför artikel 18.7 och 21.1. Bakgrunden till paragrafen behandlas i avsnitt 10.5.

Paragrafen ger tillsynsmyndigheten möjlighet att förelägga en verksamhetsutövare att tillhandahålla information enligt 3 § och ge tillträde enligt 4 §. Ett beslut om föreläggande får enligt andra stycket 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.

Bakgrunden till paragrafen behandlas i avsnitt 10.5.

Om en verksamhetsutövare vägrar att ge tillsynsmyndigheten information eller tillträde till en lokal kan tvångsåtgärder behöva användas. Tillsynsmyndigheten ska därför vid behov kunna begära biträde av Kronofogdemyndigheten.

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 anteckning samt bevarande av viss information vid bakgrundskontroll enligt 6 kap. 5 §.

Bestämmelsen genomför artikel 22 och behandlas i avsnitt 11.4 och 11.6. Paragrafen innebär att tillsynsmyndigheten som huvudregel ska ingripa mot överträdelser av de angivna skyldigheterna, samt sådana föreskrifter som har meddelats med stöd av dem.

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.

Paragrafen genomför artikel 22. Övervägandena behandlas i avsnitt 11.7.

Av *första och andra stycket* följer de sätt tillsynsmyndigheten kan ingripa på, nämligen föreläggande (vid vite), sanktionsavgift och anmärkning. Tillsynsmyndigheten avgör själv vilken eller vilka sanktioner som är aktuella att använda sig av i det enskilda fallet, samt utformningen av dem. Om varken föreläggande eller sanktionsavgift anses lämpliga ska tillsynsmyndigheten i stället meddela en anmärkning. Anmärkning behandlas i avsnitt 11.7.3.

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.

Paragrafen genomför artikel 22. Övervägandena behandlas i avsnitt 11.5.

Bestämmelsen utgör en möjlighet för tillsynsmyndigheten att underlåta ingripande, och är en ventil som ska tillämpas restriktivt. Den tar sikte på situationer där ett ingripande exempelvis skulle anses strida mot dubbelprövningsförbudet enligt Europakonventionens sjunde tilläggsprotokoll (ne bis in idem) eller anses oskäligt på grund av en annan myndighets ingripande mot samma överträdelse eller händelse. Det kan röra sig om såväl en svensk som utländsk tillsynsmyndighets ingripande. Tillsynsmyndigheten behöver inte fatta ett beslut om att avstå från att ingripa.

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.

Paragrafen genomför artikel 21.3 och 22. Övervägandena behandlas i avsnitt 11.7.1. Förelägganden kan riktas mot både enskilda och offentliga kritiska verksamhetsutövare, och kan beslutas att gälla omedelbart, se vidare 9 kap. 2 §.

Sanktionsavgift

5 § Tillsynsmyndigheten får besluta att en kritisk verksamhetsutövare ska betala en sanktionsavgift till följd av en överträdelse enligt 1 §.

Paragrafen genomför artikel 22. Övervägandena behandlas i avsnitt 11.7.2. Bestämmelsen ger tillsynsmyndigheten befogenhet att besluta om sanktionsavgifter enligt de uppräknade bestämmelserna. Tillsynsmyndigheten får ta ut sanktionsavgift vid överträdelser och det ska ske med tillämpning av strikt ansvar där det saknar betydelse om överträdelsen skett av misstag, oaktsamhet eller uppsåtligen. Sådana aspekter ska i stället kunna vägas in vid bestämmande av sanktionsavgiftens storlek.

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.

Övervägandena behandlas i avsnitt 11.7.2. Gemensamt för bestämmelserna i 6–7 §§ är miniminivån på 5 000 kronor. Maximinivån beror på vilken typ av verksamhetsutövare det rör sig om. Det stora spannet mellan minimi- och maximibelopp ger tillsynsmyndigheten stor handlingsfrihet kring utformningen av sanktionen. Detta gör att tillsynsmyndigheten kan anpassa sanktionen för att vara effektiv, proportionerlig och avskräckande i varje enskilt fall med beaktande av samtliga omständigheter.

7 § Sanktionsavgiften ska för offentliga kritiska verksamhetsutövare bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor.

Övervägandena behandlas i avsnitt 11.7.2.

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.

Paragrafen genomför artikel 22. Övervägandena behandlas i avsnitt 11.7.2.

Vid bestämmande av sanktionsavgiftens storlek ska alla relevanta omständigheter beaktas, men bestämmelsen anger att vissa saker ska beaktas särskilt och kan därför få större genomslag på bedömningen.

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.

Övervägandena behandlas i avsnitt 11.7.2.

Bestämmelsen utgör ett uttryck för det så kallade dubbelprövningsförbudet enligt Europakonventionen och kompletterar den allmänna ventilen mot ingripande i 3 §. Bestämmelsen medför inte någon begränsning för tillsynsmyndigheten att besluta om någon annan sanktion än just sanktionsavgift för den aktuella överträdelsen.

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.

Övervägandena behandlas i avsnitt 11.7.2 och innehåller författningsbestämmelser för sanktionsavgifter.

Första stycket innebär en preskriptionsregel för sådana sanktionsavgifter där verksamhetsutövaren inte har fått tillfälle att yttra sig inom två år från överträdelsen.

Andra stycket anger att ett beslut om sanktionsavgift ska delges. Vid delgivning är delgivningslagen (2010:1932) tillämplig.

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.

Övervägandena behandlas i avsnitt 11.7.2 och innehåller förfarandebestämmelse för sanktionsavgifter.

Första stycket fastställer när betalning ska ske, och att tillsynsmyndigheten har möjlighet att förlänga den tid som betalningen ska ske inom.

Andra stycket anger att obetalda avgifter ska få lämnas för indrivning och att sådan verkställighet får ske enligt utsökningsbalkens regler.

Av *tredje stycket* framgår att sanktionsavgiften 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.

Övervägandena behandlas i avsnitt 11.7.2 och innebär att en sanktionsavgift preskriberas om inte verkställighet av den har skett 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).

Paragrafen innehåller bestämmelser om tystnadsplikt för uppgifter som förekommer i angelägenhet som avser bakgrundskontroller. Övervägandena behandlas i avsnitt 13.7.

Första stycket innebär en tystnadsplikt för enskilda verksamhetsutövare som tar sikte på att skydda enskildas integritet vid bakgrundskontroller enligt lagen om motståndskraft hos kritiska verksamhetsutövare. Tystnadsplikten gäller såväl uppgifter som har lämnats av den prövade och sådana uppgifter som i övrigt förekommer i bakgrundskontrollen till exempel i en intervju med den prövade.

I *andra stycket* anges upplysningsvis att motsvarande tystnadsplikt gäller i det allmännas verksamhet enligt bestämmelser i offentlighets- och sekretesslagen (2009:400), OSL. Se även kommentaren till förslaget om ändring i 35 kap. 1 § 10 OSL.

Förordnande om att beslut ska gälla omedelbart

2 § Tillsynsmyndigheten får bestämma att ett beslut om föreläggande enligt denna lag ska gälla omedelbart.

Bestämmelsen behandlas i avsnitt 11.8 och möjliggör omedelbar verkställighet av förelägganden enligt denna lag. Det kan exempelvis avse sådana tillsynsåtgärder som måste vidtas omedelbart för att vara verksamma, till exempel att få tillträde till en verksamhetsutövares lokaler eller dokumentation.

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.

Paragrafen genomför artikel 21.4.

Bestämmelsen anger regler för överklagande enligt lagen och behandlas i avsnitt 11.9.

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, eller
7. *enligt bestämmelser i lagen (2025:00) 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 *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.

Ändringen i bestämmelsen genomför artikel 14.2–3 och bakgrunden till ändringen redogörs för i avsnitt 9.4.1.

En ny punkt 7 har införts i *andra stycket*. Ändringen innebär en rätt för enskilda att få begränsade utdrag ur belastningsregistret om sig själva avseende sådana utdrag som följer av 6 kap. 4 § första stycket 2 lagen om motståndskraft hos kritiska verksamhetsutövare.

Av *tredje stycket* följer att regeringen får rätt att meddela föreskrifter om innehållet i ett sådant utdrag.

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 brottmåls-

förfarande 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.

Ändringen av paragrafen genomför artikel 14.2–3 (delvis) och bakgrunden behandlas i avsnitt 9.4.2.

Tredje stycket är nytt och är avsett att hantera att reciprocitetskravet inte tillgodoses på annat sätt. Hänvisningen till direktivet är dynamisk, och avser därmed den vid varje tidpunkt gällande lydelsen av direktivet.

17.3 Förslaget till lag om ändring i offentlighets- och sekretesslagen (2009:400)

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.

Paragrafen är ny. Den innehåller en sekretessbrytande bestämmelse för Myndigheten för samhällsskydd och beredskap och tillsynsmyndigheter enligt lagen om cybersäkerhet och lagen om motståndskraft hos kritiska verksamhetsutövare när det gäller sekretess i det internationella samarbetet. Övervägandena behandlas i avsnitt 13.3.

Första stycket gör det möjligt för Myndigheten för samhällsskydd och beredskap att lämna en uppgift som avses i 15 kap. 1 a § OSL till

en tillsynsmyndighet om det behövs för att tillsynsmyndigheten ska kunna fullgöra sitt uppdrag enligt nämnda lagar. Det rör sig till exempel om uppgifter i incidentrapporter, uppgifter inom det rådgivande uppdraget enligt CER-direktivet och uppgifter som delges i samverkan med andra medlemsstaters tillsynsmyndigheter enligt NIS2-direktivet.

Andra stycket gör det möjligt för en tillsynsmyndighet att på samma sätt lämna en uppgift som avses i 15 kap. 1 a § OSL till Myndigheten för samhällsskydd och beredskap.

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 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.

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

Paragrafen är ny och innehåller bestämmelser om sekretess för uppgifter incidentrapporter enligt 3 kap. 5–7 §§ lagen om cybersäkerhet och 5 kap. 1 § lagen om motståndskraft hos kritiska verksamhetsutövare samt uppgifter om åtgärder som följer av en sådan incident. Övervägandena behandlas i avsnitt 13.2.

I *första stycket* skyddas uppgift i incidentrapporter och uppgift om åtgärder som följer av en sådan incident. Paragrafen har ett omvänt skaderekvisit vilket innebär att en uppgift ska lämnas ut enbart om det står klart att uppgiften kan röjas utan att den rapporterande verksamhetsutövarens verksamhet skadas eller de åtgärder som vidtagits motverkas. Skada för verksamheten kan till exempel vara negativa konsekvenser för verksamhetsutövarens pågående och framtida säkerhetsarbete, negativa ekonomiska effekter för enskilda verksamhetsutövare och bristande rapporteringsvilja.

Enligt *andra stycket* gäller sekretessen i högst fyrtio år.

19 §

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 13 §§ 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 §, 1–18 §§, 20 § 3 och 22 § första stycket 1 och andra stycket tryckfrihetsförordningen samt 5 kap. 1 § och 4 § första stycket 1 och andra stycket yttrandefrihetsgrundlagen.

I paragrafen regleras rätten att meddela och offentliggöra uppgifter. Övervägandena behandlas i avsnitt 13.2.

Första stycket ändras så att den nya 8 d § omfattas av uppräkningen som görs där. Rätten att meddela och offentliggöra uppgifter får därmed inte företräde framför den tystnadsplikt som följer av 8 d §.

35 kap.

1 §

10. angelägenhet som rör bakgrundskontroll enligt lagen (2025:000) om motståndskraft hos kritiska verksamhetsutövare.

Bestämmelsen ändras inte på annat sätt än att en ny punkt införs. Ändringen innebär att sekretessen utvidgas till att avse bakgrundskontroller som genomförs med stöd av lagen om motståndskraft hos kritiska verksamhetsutövare. Syftet med ändringen är att ge ett skydd

för uppgifter som kommer fram vid bakgrundskontrollen. Det kan bland annat vara fråga om uppgifter ur belastningsregistret eller om personliga och ekonomiska förhållanden som den som kontrollen avser lämnar vid en intervju. Övervägandena behandlas i avsnitt 13.6.

Sekretessen enligt *första stycket* 10 gäller hos kritiska verksamhetsutövare enligt lagen om motståndskraft hos kritiska verksamhetsutövare om det kan antas att den enskilde eller någon närstående till honom eller henne lider skada eller men om uppgiften röjs.

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 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.

Övervägandena behandlas i kapitel 14.

Paragrafen fastställer minimi- och maximibelopp för sanktionsavgift. Övervägandena behandlas i avsnitt 14.6.

Ändringen innebär att det högsta beloppet som en sanktionsavgift kan bestämmas till höjs för enskilda verksamhetsutövare. Det stora spannet mellan minimi- och maximibelopp ger tillsynsmyndigheten större handlingsfrihet kring utformningen av sanktionen och höjningen medför att sanktionen kommer vara avskräckande för alla verksamhetsutövare. Kopplingen av sanktionsavgiftens storlek till verksamhetsutövarens omsättning innebär att den avgiftsskyldiges finansiella ställning får större betydelse vid bedömningen av avgiftens storlek.

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).

En ny rubrik och en ny paragraf införs som innebär att tillsynsmyndigheten i vissa fall ska meddela tillsynsmyndigheten enligt lagen om motståndskraft hos kritiska verksamhetsutövare huruvida en verksamhetsutövare anmält att den bedriver säkerhetskänslig verksamhet.

Överväganden behandlas i avsnitt 5.3.4.

Om en verksamhetsutövare under identifieringsarbetet enligt 2 kap. 1 § lagen om motståndskraft hos kritiska verksamhetsutövare uppger att den samhällsviktiga tjänsten till någon del är säkerhetskänslig ska den tillsynsmyndigheten underrätta berörd tillsynsmyndighet enligt säkerhetsskyddslagen. På motsvarande sätt införs en skyldighet för den myndighet som är tillsynsmyndighet enligt säkerhetsskyddslagen att meddela tillsynsmyndigheten enligt lagen om motståndskraft hos kritiska verksamhetsutövare om den aktuella verksamhetsutövaren har anmält att den bedriver säkerhetskänslig verksamhet.

17.5 Förslaget om lag om ändring i lagen om cybersäkerhet

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 domännamnsregistrering *eller som beslutats vara kritiska enligt 2 kap. 1 § lagen (2025:000) om motståndskraft för 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.

Ändringen i paragrafen genomför artikel 2.3 i NIS2-direktivet.

Övervägandena behandlas i avsnitt 6.6. Ändringen innebär att den som identifierats som kritisk verksamhetsutövare enligt 2 kap. 1 § lagen om motståndskraft hos kritiska verksamhetsutövare under vissa förutsättningar omfattas av denna lag.

En förutsättning för att omfattas av cybersäkerhetslagen är att verksamhetsutövaren bedriver verksamhet som omfattas av bilaga 1 eller 2 i NIS2-direktivet samt uppfyller kravet på att vara etablerad i Sverige. Däremot behöver storlekskravet inte vara uppfyllt.

Skyldigheterna i 3 kap. cybersäkerhetslagen ska, för de kritiska verksamhetsutövare som inte uppfyller storlekskravet, börja gälla tio månader efter den dag de fått del av beslutet om identifiering enligt 2 kap. 1 § lagen om motståndskraft hos kritiska verksamhetsutövare. Skyldigheten att anmäla sig till tillsynsmyndigheten enligt 2 kap. 2 § cybersäkerhetslagen ska dock göras när den kritiska verksamhetsutövaren fått del av beslutet.

2 kap.

1 §

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 (2025:00) om motståndskraft hos kritiska verksamhetsutövare.

Ändringen i paragrafen, en ny punkt, genomför artikel 3.1 i NIS2-direktivet.

Övervägandena behandlas i avsnitt 6.6. Ändringen innebär att den som identifierats som kritisk verksamhetsutövare enligt 2 kap. 1 § lagen om motståndskraft hos kritiska verksamhetsutövare under vissa förutsättningar omfattas av denna lag och klassificeras som väsentlig verksamhetsutövare. Det innebär att bestämmelserna om tillsyn och sanktioner som gäller för väsentliga verksamhetsutövare enligt denna lag ska tillämpas för dessa kritiska verksamhetsutövare.

Kommittédirektiv 2023:30

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 tillhanda-

hålla 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 etable-

ras 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 med-

föra. 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 kommissio-

nen 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)

Kommittédirektiv 2024:3

Tilläggsdirektiv till Utredningen om genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft (Fö 2023:01)

Beslut vid regeringssammanträde den 11 januari 2024

Förlängd tid för en del av uppdraget

Regeringen beslutade den 23 februari 2023 kommittédirektiv om genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, förkortat NIS2-direktivet och EU:s direktiv om kritiska entiteters motståndskraft, förkortat CER-direktivet (dir. 2023:30).

Enligt de ursprungliga direktiven ska uppdraget redovisas senast den 23 februari 2024. Utredningstiden ligger fast för de delar av uppdraget som avser att föreslå hur NIS2-direktivet ska genomföras och frågor som är gemensamma för NIS2- och CER-direktiven i de ursprungliga kommittédirektiven i den mån dessa är hänförliga till genomförandet av NIS2-direktivet. Utredningstiden ska dock förlängas för de delar av de ursprungliga direktiven som avser att

- föreslå hur CER-direktivet ska genomföras och frågor gemensamma för NIS2- och CER-direktiven i de ursprungliga kommittédirektiven i den mån dessa är hänförliga till genomförandet av CER-direktivet eller i övrigt syftar till att uppnå en sammanhängande reglering,

- 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,
- ta ställning till om bestämmelserna i offentlighets- och sekretesslagen (2009:400) innebär ett tillräckligt skydd för sådana uppgifter som kan komma att behandlas enligt direktiven, och
- i anslutning till dessa frågor lämna nödvändiga författningsförslag.

Uppdraget ska i dessa delar redovisas senast den 16 september 2024.

Utredaren har även fortsättningsvis möjlighet att ta upp andra frågor som har samband med de frågeställningar som ska hanteras inom ramen för utredningen under förutsättning att uppdraget ändå kan redovisas i tid.

(Försvarsdepartementet)

CER-direktivet

Jämförelsetabell

Artikel i CER-direktivet	Svensk rätt[1]
1.1	1 kap. 1 och 3 §§
1.2	1 kap. 5 §
1.3	1 kap. 6 §
1.4	–
1.5	1 kap. 8 §
1.6	1 kap. 8 § första och tredje stycket och 4–5 §§ förordningen
1.7	1 kap. 8 § andra och fjärde stycket
1.8	1 kap. 9–10 §§
1.9	–
2	1 kap. 2 och 7 §§
3	–
4	–
5	1 kap. 11 §
6.1	2 kap. 1 §
6.2	2 kap. 2 §
6.3	2 kap. 1 och 6 §§
6.4	34 § 7 förordningen
6.5	2 kap. 1 § och 5–6 §§
6.6	–
7.1	8 § förordningen
7.2	11 § förordningen
7.3	–
8	1 kap. 4 § och 2 kap. 3 § andra stycket
9.1	7 kap. 1–2 §§
9.2	37-38 §§ förordningen
9.3	39 § förordningen
9.4	–
9.5	–
9.6	–
9.7	–
9.8	–
10.1–3	–
11.1–2	40 § förordningen
12.1–2	4 kap. 1 §
13.1–2	4 kap. 2 § och 6 kap.
13.3	4 kap. 3 §
13.4	17 § förordningen

Artikel i CER-direktivet	Svensk rätt[1]
13.5–6	–
14.1–3	6 kap. 1–7 §§
15.1	5 kap. 1 § och 24 § förordningen
15.2	26 § förordningen
15.3	28 § förordningen
15.4	27 § förordningen
16	–
17.1	1 kap. 2 § 6 p
17.2	3 kap. 1–2 § och 12–13 § förordningen
17.3–4	3 kap. 3 §, 14 §§ och 34 § 4 förordningen
18.1	3 kap. 4 § och 7 kap. 2 §
18.2	3 kap. 4 § och 15–16 § förordningen
18.3	3 kap. 5 § och 19 § förordningen
18.4	33 § förordningen
18.5	6 kap. 7 § och 18 § förordningen
18.6	–
18.7	7 kap. 3–5 §§
18.8	1 kap. 9–10 §§
18.9–10	–
19	6 kap. 6 § och 40 § förordningen
20	–
21.1	7 kap. 4–6 §§
21.2	7 kap. 3–6 §, 35 § förordningen
21.3	8 kap. 4 §
21.4	9 kap. 3 §
21.5	–
22	8 kap.
23	–
24	–
25	–
26	–
27	–
28	–
29	–

[1] Om inget annat anges avses utredningens förslag till lag om motståndskraft hos kritiska verksamhetsutövare. Med förordningen avses utredningens förslag till förordning om motståndskraft hos kritiska verksamhetsutövare.