Svensk författningssamling

Cybersäkerhetsförordning

SFS 2025:1507
Publicerad
den 17 december 2025

Utfärdad den 11 december 2025

Regeringen föreskriver[1] följande.

Inledande bestämmelser

1 § Denna förordning innehåller kompletterande bestämmelser till cybersäkerhetslagen (2025:1506).

2 § Denna förordning är meddelad med stöd av
– 1 kap. 8 § cybersäkerhetslagen (2025:1506) i fråga om 4 §,
– 1 kap. 15 § första stycket samma lag i fråga om 38 § 1 och 2,
– 1 kap. 15 § andra stycket samma lag i fråga om 38 § 3,
– 1 kap. 16 § 2 samma lag i fråga om 17 §,
– 2 kap. 14 § samma lag i fråga om 37 § första stycket 1–3, 37 § andra stycket, 38 § 5 och 6 samt 39 § 1–3,
– 3 kap. 10 § samma lag i fråga om 38 § 7,
– 8 kap. 11 § regeringsformen i fråga om 37 § första stycket 4 och 38 § 4, och
– 8 kap. 7 § regeringsformen i fråga om övriga bestämmelser.

3 § Uttryck som används i förordningen har samma innebörd som i cybersäkerhetslagen (2025:1506).

Utpekande av statliga myndigheter

4 § De myndigheter som omfattas av bilaga 1 till förordningen (2022:524) om statliga myndigheters beredskap ska, om de inte är undantagna med stöd av 1 kap. 12 § cybersäkerhetslagen (2025:1506), omfattas av cybersäkerhetslagen.

Anmälningsskyldighet och incidentrapportering

5 § En anmälan enligt 2 kap. 2 § cybersäkerhetslagen (2025:1506) ska göras till den gemensamma kontaktpunkten enligt 23 §.

6 § Incidentrapportering enligt 2 kap. 5–8 §§ cybersäkerhetslagen (2025:1506) ska göras till CSIRT-enheten enligt 31 §.

[1] Jfr Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet), i den ursprungliga lydelsen.

7 § Följande myndigheter är tillsynsmyndigheter enligt cybersäkerhetslagen (2025:1506) för verksamhetsutövare inom angivna sektorer.

Tillsynsmyndighet	Sektor
Statens energimyndighet	Energi
Transportstyrelsen	Transporter Tillverkning av motorfordon, släpfordon och påhängsvagnar Tillverkning av andra transportmedel
Finansinspektionen	Bankverksamhet Finansmarknadsinfrastruktur
Inspektionen för vård och omsorg	Vårdgivare i Hälso- och sjukvårdssektorn
Läkemedelsverket	Hälso- och sjukvårdssektorn, med undantag för vårdgivare Tillverkning av medicintekniska produkter och medicintekniska produkter för in vitro-diagnostik
Livsmedelsverket	Avloppsvatten Dricksvatten Produktion, bearbetning och distribution av livsmedel
Post- och telestyrelsen	Digital infrastruktur Digitala leverantörer Förvaltning av IKT-tjänster (mellan företag) Post- och budtjänster Rymden
Länsstyrelserna i Norrbottens, Skåne, Stockholms, Västra Götalands, Örebro och Östergötlands län	Avfallshantering Forskning Offentlig förvaltning, med undantag för länsstyrelserna Tillverkning, produktion och distribution av kemikalier Tillverkning av datorer, elektronikvaror och optik Tillverkning av elapparatur Tillverkning av övriga maskiner

8 § Post- och telestyrelsen är också tillsynsmyndighet för

1. länsstyrelserna, och
2. verksamhetsutövare som erbjuder domännamnsregistreringstjänster.

9 § Länsstyrelserna i Norrbottens, Skåne, Stockholms, Västra Götalands, Örebro och Östergötlands län är också tillsynsmyndigheter för

1. enskilda utbildningsanordnare med tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina, och
2. sådana myndigheter som avses i 4 §, med undantag för länsstyrelserna.

10 § Länsstyrelsen i Norrbottens län är med stöd av 7 och 9 §§ tillsynsmyndighet för kommuner och regioner som hör till Jämtlands, Norrbottens,

Västerbottens eller Västernorrlands län och verksamhetsutövare som har sitt säte i något av dessa län.

11 § Länsstyrelsen i Skåne län är med stöd av 7 och 9 §§ tillsynsmyndighet för kommuner och regioner som hör till Blekinge, Kronobergs eller Skåne län och verksamhetsutövare som har sitt säte i något av dessa län.

12 § Länsstyrelsen i Stockholms län är med stöd av 7 och 9 §§ tillsynsmyndighet för kommuner och regioner som hör till Gotlands eller Stockholms län och verksamhetsutövare som har sitt säte i något av dessa län.

13 § Länsstyrelsen i Västra Götalands län är med stöd av 7 och 9 §§ tillsynsmyndighet för kommuner och regioner som hör till Hallands eller Västra Götalands län och verksamhetsutövare som har sitt säte i något av dessa län.

14 § Länsstyrelsen i Örebro län är med stöd av 7 och 9 §§ tillsynsmyndighet för kommuner och regioner som hör till Dalarnas, Gävleborgs, Södermanlands, Uppsala, Värmlands, Västmanlands eller Örebro län och verksamhetsutövare som har sitt säte i något av dessa län.

15 § Länsstyrelsen i Östergötlands län är med stöd av 7 och 9 §§ tillsynsmyndighet för kommuner och regioner som hör till Jönköpings, Kalmar eller Östergötlands län och verksamhetsutövare som har sitt säte i något av dessa län.

16 § Om två eller flera tillsynsmyndigheter har tillsynsansvar för samma verksamhetsutövare ska myndigheterna komma överens om hur tillsynen ska genomföras.

Tillsynsmyndighetens uppgifter och befogenheter

17 § En tillsynsmyndighet får inom sitt tillsynsområde besluta om undantag enligt 1 kap. 16 § 2 cybersäkerhetslagen (2025:1506).

18 § Tillsynsmyndigheten ska samarbeta med Integritetsskyddsmyndigheten vid hantering av incidenter som även utgör personuppgiftsincidenter.

Om tillsynsmyndigheten, när den utövar tillsyn enligt cybersäkerhetslagen (2025:1506), får kännedom om en omständighet som kan innebära en personuppgiftsincident som ska anmälas enligt 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), ska tillsynsmyndigheten så snart det kan ske informera Integritetsskyddsmyndigheten om incidenten.

19 § Om tillsynsmyndigheten utövar tillsyn över en verksamhetsutövare som har identifierats som en kritisk tredjepartsleverantör av IKT-tjänster enligt artikel 31 i 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, ska tillsynsmyndigheten informera det tillsynsforum som har inrättats enligt artikel 32 i samma förordning.

20 § Tillsynsmyndigheten ska samarbeta med och bistå tillsynsmyndigheter i andra medlemsstater inom EES i enlighet med artikel 37 i NIS 2-direktivet, i den ursprungliga lydelsen, avseende verksamhetsutövare som erbjuder tjänster i

1. mer än en medlemsstat, eller
2. en eller flera medlemsstater och dess nätverks- och informationssystem finns i en eller flera andra medlemsstater.

21 § Tillsynsmyndigheten får avslå en begäran om bistånd enligt 20 §, om

1. myndigheten inte är behörig att tillhandahålla biståndet,
2. biståndet inte är proportionerligt i förhållande till tillsynsmyndighetens uppgifter, eller
3. begäran avser information eller omfattar verksamhet som, om den skulle lämnas ut eller utföras, skulle inverka skadligt på Sveriges säkerhetsintressen, allmänna säkerhet eller försvar.

Innan tillsynsmyndigheten avslår en begäran om bistånd ska tillsynsmyndigheten samråda med övriga berörda behöriga myndigheter samt, på begäran av en av de berörda medlemsstaterna, med Europeiska kommissionen och Europeiska unionens cybersäkerhetsbyrå (Enisa).

22 § Tillsynsmyndigheten ska lämna stöd till den gemensamma kontaktpunkten i egenskap av representant enligt 25 §.

Gemensam kontaktpunkt

23 § Myndigheten för civilt försvar ska vara gemensam kontaktpunkt enligt artikel 8.3 i NIS 2-direktivet, i den ursprungliga lydelsen.

24 § Den gemensamma kontaktpunkten ska i enlighet med artikel 8.4 i NIS 2-direktivet, i den ursprungliga lydelsen, utöva en sambandsfunktion som säkerställer ett gränsöverskridande samarbete med myndigheter i andra medlemsstater, Europeiska kommissionen och Europeiska unionens cybersäkerhetsbyrå (Enisa) samt ett sektorsövergripande samarbete med tillsynsmyndigheterna.

25 § Den gemensamma kontaktpunkten är Sveriges representant i den samarbetsgrupp som har inrättats enligt artikel 14 i NIS 2-direktivet, i den ursprungliga lydelsen.

26 § Den gemensamma kontaktpunkten ska på begäran av CSIRT-enheten enligt 31 § eller en tillsynsmyndighet vidarebefordra incidentrapporter som lämnas enligt 2 kap. 5–8 §§ cybersäkerhetslagen (2025:1506) till de gemensamma kontaktpunkterna i andra berörda medlemsstater.

27 § Den gemensamma kontaktpunkten ska i enlighet med artikel 23.9 i NIS 2-direktivet, i den ursprungliga lydelsen, var tredje månad lämna in en sammanfattande rapport till Europeiska unionens cybersäkerhetsbyrå (Enisa) med anonymiserade och aggregerade uppgifter om betydande incidenter, incidenter, cyberhot och tillbud.

28 § Den gemensamma kontaktpunkten ska i enlighet med artikel 3.5 a i NIS 2-direktivet, i den ursprungliga lydelsen, underrätta Europeiska kommissionen och samarbetsgruppen om antalet väsentliga och viktiga verksamhetsutövare som har förtecknats för varje sektor och delsektor.

29 § Den gemensamma kontaktpunkten ska i enlighet med artikel 3.5 b i NIS 2-direktivet, i den ursprungliga lydelsen, lämna relevant information till Europeiska kommissionen avseende verksamhetsutövare som omfattas av 1 kap. 5 § 1–3 cybersäkerhetslagen (2025:1506).

30 § Den gemensamma kontaktpunkten ska så snart det kan ske vidarebefordra information till Europeiska unionens cybersäkerhetsbyrå (Enisa) i enlighet med artikel 27.4 i NIS 2-direktivet, i den ursprungliga lydelsen, avseende verksamhetsutövare som omfattas av 1 kap. 7 § cybersäkerhetslagen (2025:1506).

CSIRT-enhet

31 § Myndigheten för civilt försvar ska vara enhet för hantering av it-säkerhetsincidenter (CSIRT-enhet) i enlighet med artikel 10 i NIS 2-direktivet, i den ursprungliga lydelsen.

32 § CSIRT-enheten ska

1. säkerställa en hög nivå av tillgänglighet för sina kommunikationskanaler och kunna kontaktas och kontakta andra när som helst och på flera olika sätt,
2. ha lokaler och informationssystem på säkra platser,
3. ha ett ändamålsenligt system för handläggning och dirigering av förfrågningar,
4. säkerställa verksamhetens konfidentialitet och trovärdighet,
5. ha tillräckligt med personal för att säkerställa att deras tjänster är ständigt tillgängliga och säkerställa att personalen har fått lämplig utbildning,
6. ha redundanta system och reservlokaler för att säkerställa kontinuiteten i tjänsterna, och
7. kunna delta i internationella samarbetsnätverk.

CSIRT-enheten ska ha tillgång till en lämplig, säker och motståndskraftig kommunikations- och informationsstruktur för utbyte av information med verksamhetsutövare och andra relevanta intressenter.

33 § CSIRT-enheten ska

1. övervaka och analysera cyberhot, sårbarheter och incidenter på nationell nivå och tillhandahålla varningar och information till verksamhetsutövare samt till tillsynsmyndigheter och andra relevanta intressenter,
2. på begäran tillhandahålla stöd till verksamhetsutövare avseende realtidsövervakning eller nära realtidsövervakning av deras nätverks- och informationssystem,
3. ta emot incidentrapporter, vidta åtgärder till följd av incidenter och erbjuda stöd till berörda verksamhetsutövare,
4. efter att ha mottagit en incidentanmälan skyndsamt uppmana verksamhetsutövaren att anmäla incidenten till Polismyndigheten om den kan antas ha sin grund i en brottslig gärning,
5. tillgängliggöra informationen i incidentrapporter så snart det kan ske för tillsynsmyndigheten,
6. samla in och analysera forensiska uppgifter,

7. tillhandahålla dynamiska risk- och incidentanalyser samt lägesuppfattning när det gäller cybersäkerhet,

8. på begäran av en verksamhetsutövare utföra en proaktiv skanning av den berörda verksamhetsutövarens nätverks- och informationssystem,

9. delta i det nätverk som inrättats enligt artikel 15 i NIS 2-direktivet, i den ursprungliga lydelsen (CSIRT-nätverket),

10. vara samordnare för samordnad delgivning av information om sårbarheter enligt artikel 12.1 i NIS 2-direktivet, i den ursprungliga lydelsen, och

11. upprätta samarbetsförbindelser med relevanta intressenter inom privat och offentlig sektor samt bidra till samverkan i frågor om cybersäkerhet.

34 § CSIRT-enheten får utföra proaktiva, icke-inkräktande skanningar av verksamhetsutövarnas allmänt tillgängliga nätverks- och informationssystem i syfte att upptäcka sårbara eller osäkert konfigurerade system.

Cyberkrishanteringsmyndighet

35 § Myndigheten för civilt försvar ska vara cyberkrishanteringsmyndighet i enlighet med artikel 9 i NIS 2-direktivet, i den ursprungliga lydelsen.

36 § Myndigheten för civilt försvar ska i enlighet med artikel 16.2 i NIS 2-direktivet, i den ursprungliga lydelsen, delta i det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe).

Rätt att meddela föreskrifter

37 § Post- och telestyrelsen får för sina tillsynsområden, med undantag för 8 § 1, meddela

1. ytterligare föreskrifter om säkerhetsåtgärder enligt 2 kap. 3 § cybersäkerhetslagen (2025:1506),

2. ytterligare föreskrifter om vad som utgör en betydande incident enligt 2 kap. 5 § samma lag,

3. föreskrifter om informationsskyldighet enligt 2 kap. 9 och 10 §§ samma lag, och

4. närmare föreskrifter om avgift enligt 3 kap. 11 § samma lag.

Post- och telestyrelsen får också meddela föreskrifter om register enligt 2 kap. 11 och 12 §§ cybersäkerhetslagen.

38 § Myndigheten för civilt försvar får meddela

1. föreskrifter om undantag från skyldigheterna enligt cybersäkerhetslagen (2025:1506) för partnerföretag och anknutna företag som omfattas av lagen med stöd av 1 kap. 4 § samma lag,

2. föreskrifter om vad som utgör huvudsakligt etableringsställe enligt 1 kap. 7 § samma lag,

3. ytterligare föreskrifter om kriterier för när verksamhetsutövare ska omfattas av 1 kap. 5 § 1–3 cybersäkerhetslagen och för när sådana verksamhetsutövare ska räknas som väsentliga enligt 1 kap. 9 § första stycket 6 samma lag,

4. närmare föreskrifter om anmälningsskyldigheten enligt 2 kap. 2 § samma lag,

5. föreskrifter om utbildning enligt 2 kap. 4 § samma lag,

6. föreskrifter om incidentrapportering enligt 2 kap. 5–8 §§ samma lag, och

7. föreskrifter om säkerhetsrevisioner och säkerhetsskanningar enligt 3 kap. 5–7 §§ samma lag.

39 § Myndigheten för civilt försvar får för andra tillsynsområden än dem som avses i 37 § meddela

1. ytterligare föreskrifter om säkerhetsåtgärder enligt 2 kap. 3 § cybersäkerhetslagen (2025:1506),
2. ytterligare föreskrifter om vad som utgör en betydande incident enligt 2 kap. 5 § samma lag, och
3. föreskrifter om informationsskyldighet enligt 2 kap. 9 och 10 §§ samma lag.

Samarbetsforum för effektiv och likvärdig tillsyn

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

Beslut om förbud

41 § När ett beslut om förbud enligt 4 kap. 6 § cybersäkerhetslagen (2025:1506) har fått laga kraft ska domstolen underrätta Bolagsverket och verksamhetsutövaren om beslutet och dess innehåll. Om verksamhetsutövaren är en stiftelse ska den länsstyrelse som är registreringsmyndighet för stiftelsen underrättas i stället för Bolagsverket.

Domstolen ska skicka motsvarande underrättelser, om ett sådant förbud upphävs enligt 4 kap. 8 § andra stycket cybersäkerhetslagen.

42 § Bolagsverket eller länsstyrelsen ska efter en underrättelse enligt 41 § avregistrera personen som befattningshavare hos verksamhetsutövaren i det aktuella registret.

Bolagsverket eller länsstyrelsen ska säkerställa att personen inte registreras på nytt som befattningshavare hos verksamhetsutövaren under förbudstiden.

---

1. Denna förordning träder i kraft den 15 januari 2026.
2. Genom förordningen upphävs förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.
3. Den upphävda förordningen gäller dock fortfarande för överträdelser som har skett före ikraftträdandet.

På regeringens vägnar

CARL-OSKAR BOHLIN

Samuel Rudvall
(Försvarsdepartementet)