Svensk författningssamling

Cybersäkerhetslag

SFS 2025:1506
Publicerad
den 17 december 2025

Utfärdad den 11 december 2025

Enligt riksdagens beslut[1] föreskrivs[2] följande.

1 kap. Inledande bestämmelser

Syftet med lagen och lagens innehåll

1 § Syftet med denna lag är att uppnå en hög nivå av cybersäkerhet i samhället.

Bestämmelserna i lagen genomför delvis 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).

Uttryck i lagen

2 § I denna lag betyder

1. *allmänt elektroniskt kommunikationsnät*: detsamma som i 1 kap. 7 § lagen (2022:482) om elektronisk kommunikation,
2. *anknutet företag*: detsamma som i artikel 3 i bilagan till kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag,
3. *betrodd tjänst*: detsamma som i artikel 3.16 i Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EU:s förordning om elektronisk identifiering),
4. *cyberhot*: en potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverks- och informationssystem, användare av dessa system och andra personer,
5. *cybersäkerhet*: all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot,
6. *datacentraltjänst*: en tjänst som omfattar strukturer, eller grupper av strukturer, avsedda för centraliserad inkvartering, sammankoppling och drift av sådan it- och nätutrustning som tillhandahåller datalagrings-, databehandlings-

[1] Prop. 2025/26:28, bet. 2025/26:FöU2, rskr. 2025/26:113.
[2] 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.

och dataöverföringstjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll,

7. *domännamnssystemtjänst (DNS-tjänst)*: en allmän rekursiv tjänst för att lösa domännamnsfrågor till internetslutanvändare, eller en auktoritativ tjänst för att lösa domännamnsfrågor för användning av tredje part, med undantag för rotnamnsservrar,

8. *elektronisk kommunikationstjänst*: detsamma som i 1 kap. 7 § lagen om elektronisk kommunikation,

9. *enskild verksamhetsutövare*: den som uppfyller kraven i någon av 4–7 §§ och som inte är en offentlig verksamhetsutövare,

10. *incident*: en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem,

11. *kvalificerad tillhandahållare av betrodda tjänster*: detsamma som i artikel 3.20 i EU:s förordning om elektronisk identifiering,

12. *marknadsplats online*: en tjänst som

a) använder programvara, inbegripet en webbplats, en del av en webbplats eller en applikation,

b) administreras av en näringsidkare eller för dennas räkning, och

c) ger konsumenterna möjlighet att ingå distansavtal med andra näringsidkare eller konsumenter,

13. *medelstort företag*: ett företag som räknas som ett medelstort företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag, utan beaktande av artikel 3.4 enligt samma bilaga,

14. *molntjänst*: en digital tjänst som möjliggör administration på begäran och bred fjärråtkomst till en skalbar och elastisk pool av gemensamma dataresurser, inbegripet då sådana resurser är distribuerade på flera platser,

15. *nätverk för leverans av innehåll*: ett nätverk av geografiskt spridda servrar vars syfte är att säkerställa hög tillgänglighet för, tillgång till eller snabb leverans av digitalt innehåll och digitala tjänster till internetanvändare för innehålls- och tjänsteleverantörers räkning,

16. *nätverks- och informationssystem*:

a) ett elektroniskt kommunikationsnät enligt 1 kap. 7 § lagen om elektronisk kommunikation,

b) en enhet eller en grupp enheter som är sammankopplade eller hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av digitala uppgifter, eller

c) digitala uppgifter som lagras, behandlas, hämtas eller överförs med sådana hjälpmedel som omfattas av a och b för att de ska kunna användas, skyddas och underhållas,

17. *offentlig verksamhetsutövare*:

a) en statlig myndighet som omfattas av lagen enligt 3 eller 8 § eller uppfyller något av kraven i 4–7 §§, eller

b) en region, en kommun eller ett kommunalförbund,

18. *partnerföretag*: detsamma som i artikel 3 i bilagan till kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag,

19. *plattform för sociala nätverkstjänster*: en plattform som gör det möjligt för slutanvändare att interagera, dela och upptäcka innehåll, finna andra användare och kommunicera med andra via flera enheter, exempelvis genom chattar, inlägg, videor och rekommendationer,

20. *registreringsenhet för toppdomäner*: en verksamhetsutövare som har delegerats en specifik toppdomän och som ansvarar för administrationen av den, dock inte om toppdomänen används endast för registreringsenhetens eget bruk,

21. *sökmotor*: detsamma som i artikel 2.5 i Europaparlamentets och rådets förordning (EU) 2019/1150 av den 20 juni 2019 om främjande av rättvisa villkor och transparens för företagsanvändare av onlinebaserade förmedlingstjänster,

22. *utlokaliserad driftstjänst*: en tjänst som avser installation, förvaltning, drift eller underhåll av IKT-produkter, IKT-nät, IKT-infrastruktur, IKT-tillämpningar eller andra nätverks- och informationssystem, genom bistånd eller aktiv administration i kundernas lokaler eller på distans,

23. *utlokaliserad säkerhetstjänst*: en tjänst som tillhandahålls av en leverantör av utlokaliserade driftstjänster och som innebär hantering av eller utgör stöd för hantering av cybersäkerhetsrisker.

Lagens tillämpningsområde

3 § Lagen gäller för en verksamhetsutövare som är

1. en statlig myndighet med befogenhet att fatta beslut som påverkar fysiska eller juridiska personers rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital, eller
2. en region, en kommun eller ett kommunalförbund.

4 § Lagen gäller också för en verksamhetsutövare som

1. omfattas av bilaga 1 eller 2 till NIS 2-direktivet i den ursprungliga lydelsen, men inte av 5 § 4, 6 § eller 7 § 1–3, eller är en enskild utbildningsanordnare med tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina,
2. är etablerad i Sverige, och
3. storleksmässigt motsvarar eller är större än ett medelstort företag.

5 § Lagen gäller också för en verksamhetsutövare som uppfyller kraven i 4 § 1 och 2, om

1. verksamhetsutövaren är den enda leverantören av en tjänst i Sverige som är väsentlig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet,
2. en störning av den tjänst som verksamhetsutövaren tillhandahåller kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet eller folkhälsa eller kan medföra betydande systemrisker,
3. verksamhetsutövaren har särskild betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst eller för andra sektorer som är beroende av verksamhetsutövaren, eller
4. verksamhetsutövaren tillhandahåller betrodda tjänster.

6 § Lagen gäller också för en verksamhetsutövare som i Sverige tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster.

7 § Lagen gäller också för en verksamhetsutövare som har huvudsakligt etableringsställe i Sverige eller en företrädare som är etablerad här, om verksamhetsutövaren

1. uppfyller kravet i 4 § 3 eller något av kraven i 5 § 1–3 och erbjuder molntjänster, datacentraltjänster, nätverk för leverans av innehåll, utlokaliserade

driftstjänster, utlokaliserade säkerhetstjänster, marknadsplatser online, sökmotorer eller plattformar för sociala nätverkstjänster,

2. är en registreringsenhet för toppdomäner,
3. erbjuder DNS-tjänster, eller
4. erbjuder domännamnsregistreringstjänster.

8 § Lagen gäller också för de statliga myndigheter som regeringen bestämmer även om inte kraven i 3–7 §§ är uppfyllda.

Väsentliga och viktiga verksamhetsutövare

9 § Som väsentlig verksamhetsutövare räknas

1. en verksamhetsutövare som är en statlig myndighet,
2. en verksamhetsutövare som är större än ett medelstort företag och som
   a) är en kommun eller en region,
   b) i övrigt omfattas av bilaga 1 till NIS 2-direktivet i den ursprungliga lydelsen men inte av 7 § 2 eller 3, eller
   c) är en enskild utbildningsanordnare med tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina,
3. en verksamhetsutövare som avses i 6 § och som storleksmässigt motsvarar eller är större än ett medelstort företag,
4. en verksamhetsutövare som avses i 7 § 2 eller 3,
5. en verksamhetsutövare som är en kvalificerad tillhandahållare av betrodda tjänster, och
6. en verksamhetsutövare som räknas som väsentlig enligt föreskrifter som har meddelats med stöd av 15 § andra stycket.

Verksamhetsutövare som inte är väsentliga är viktiga verksamhetsutövare.

Undantag från lagens tillämpningsområde

Krav i andra författningar

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

11 § Denna lag gäller inte för verksamhetsutövare som har undantagits enligt artikel 2.4 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 (DORA-förordningen).

För en verksamhetsutövare som omfattas av DORA-förordningen gäller inte skyldigheterna enligt 2 kap. 3–10 §§.

Säkerhetskänslig verksamhet och brottsbekämpande verksamhet

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

Lagen gäller inte heller för en enskild verksamhetsutövare som enbart bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen eller som enbart erbjuder tjänster till sådana statliga myndigheter som avses i första stycket.

För andra verksamhetsutövare som till någon del bedriver sådan verksamhet eller erbjuder sådana tjänster som avses i första eller andra stycket gäller inte skyldigheterna enligt 2 kap. 3–10 §§ för den delen av verksamheten.

Undantagen i första–tredje styckena gäller inte för en verksamhetsutövare som tillhandahåller betrodda tjänster.

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

Undantag för viss annan offentlig verksamhet

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

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

Bemyndigande och beslut om undantag

15 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om

1. undantag från skyldigheterna enligt denna lag för partnerföretag och anknutna företag som omfattas av lagen med stöd av 4 §, och
2. vad som utgör huvudsakligt etableringsställe enligt 7 §.

Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om kriterier för när verksamhetsutövare ska omfattas av lagen enligt 5 § 1–3 och för när sådana verksamhetsutövare ska räknas som väsentliga enligt 9 § första stycket 6.

16 § Regeringen eller den myndighet som regeringen bestämmer får, om det finns särskilda skäl, i enskilda fall besluta om undantag från skyldigheterna enligt denna lag för

1. enskilda utbildningsanordnare som avses i 4 § 1, och
2. partnerföretag och anknutna företag som omfattas av lagen med stöd av 4 §.

Uppdrag enligt NIS 2-direktivet

17 § Den myndighet som regeringen bestämmer ska vara gemensam kontaktpunkt, cyberkrishanteringsmyndighet och enhet för hantering av it-säkerhetsincidenter enligt artiklarna 8–10 i NIS 2-direktivet, i den ursprungliga lydelsen.

2 kap. Verksamhetsutövares skyldigheter

Skyldighet att utse företrädare

1 § Sådana verksamhetsutövare som saknar etablering inom Europeiska ekonomiska samarbetsområdet (EES), men som i övrigt uppfyller kraven i 1 kap. 7 § och erbjuder tjänster i Sverige, ska utse en företrädare med etablering i Sverige eller i något annat land inom EES där tjänsterna erbjuds.

Anmälningsskyldighet

2 § Verksamhetsutövare ska så snart det kan ske anmäla sig till den myndighet som regeringen bestämmer.

Om de förhållanden som har redovisats i en anmälan har ändrats ska verksamhetsutövare anmäla förändringen så snart det kan ske, dock senast 14 dagar efter det att förändringen ägde rum.

3 § Verksamhetsutövare ska vidta lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att skydda nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och systemens fysiska miljö mot incidenter (säkerhetsåtgärder).

Säkerhetsåtgärderna ska utgå från ett allriskperspektiv och säkerställa en nivå på säkerheten i nätverks- och informationssystemen som är lämplig i förhållande till risken. Säkerhetsåtgärderna ska åtminstone avse

1. strategier för riskanalys och för nätverks- och informationssystemens säkerhet,
2. incidenthantering,
3. kontinuitetshantering och krishantering,
4. säkerhet i leveranskedjan,
5. säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem,
6. strategier och förfaranden för att bedöma effektiviteten i säkerhetsåtgärderna,
7. grundläggande praxis för cyberhygien och utbildning i cybersäkerhet,
8. strategier och förfaranden för användning av kryptografi samt, vid behov, kryptering,
9. personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning, och
10. vid behov användning av lösningar för autentisering, säkrade kommunikationer och säkrade nödkommunikationssystem.

Utbildning

4 § De personer som ingår i ledningen för en verksamhetsutövare ska genomgå utbildning om säkerhetsåtgärder.

Incidentrapportering och informationsskyldighet

Rapportering av betydande incidenter

5 § Verksamhetsutövare ska upplysa den myndighet som regeringen bestämmer om en betydande incident så snart det kan ske, dock senast 24 timmar efter det att verksamhetsutövaren har fått kännedom om incidenten.

En incident ska anses vara betydande om den har orsakat eller kan orsaka allvarlig driftsstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamhetsutövaren, eller om den har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande skada.

6 § Verksamhetsutövare ska till samma myndighet som avses i 5 § göra en incidentanmälan om den betydande incidenten så snart det kan ske. Verksamhetsutövare som tillhandahåller betrodda tjänster ska göra anmälan senast 24 timmar efter det att verksamhetsutövaren har fått kännedom om incidenten och övriga verksamhetsutövare senast 72 timmar efter sådan kännedom.

7 § På begäran av samma myndighet som avses i 5 § ska verksamhetsutövare lämna en delrapport med relevanta statusuppdateringar för den betydande incidenten.

8 § Senast en månad efter incidentanmälan enligt 6 § ska verksamhetsutövare lämna en slutrapport till samma myndighet. Om den betydande incidenten fortfarande är pågående ska i stället en lägesrapport lämnas vid denna tidpunkt och därefter en slutrapport inom en månad efter det att incidenten har hanterats.

Information vid betydande incidenter och betydande cyberhot

9 § Om det är lämpligt ska verksamhetsutövare så snart det kan ske informera mottagarna av deras tjänster om en betydande incident som sannolikt inverkar negativt på tillhandahållandet av tjänsterna.

10 § Vid ett betydande cyberhot ska verksamhetsutövare så snart det kan ske informera mottagarna av deras tjänster som kan påverkas av hotet om skydds- och motåtgärder som mottagarna kan vidta. Om det är lämpligt ska verksamhetsutövare även informera om själva hotet.

Ett cyberhot ska anses vara betydande om det, på grund av dess tekniska egenskaper, kan antas ha potential att ha en allvarlig påverkan på en verksamhetsutövares nätverks- och informationssystem eller användarna av verksamhetsutövarens tjänster genom att vålla betydande skada.

Skyldighet att föra register över domännamn

11 § En verksamhetsutövare som är en registreringsenhet för toppdomäner eller som erbjuder domännamnsregistreringstjänster ska föra ett register över tilldelade domännamn under toppdomänen och löpande upprätta säkerhetskopior av registeruppgifterna.

Registret ska innehålla

1. domännamnet,
2. namnet på domännamnsinnehavaren och dennes telefonnummer och e-postadress,
3. namnet på den som tekniskt administrerar domännamnet och dennes telefonnummer och e-postadress, och
4. registreringsdatum.

12 § Uppgifterna i det register som avses i 11 § ska kunna hämtas utan avgift via internet. Personuppgifter får dock göras tillgängliga på internet endast om den registrerade har samtyckt till det.

Därutöver ska uppgifter lämnas ut till den som gör en lagligen grundad och motiverad begäran. Uppgifterna ska då lämnas ut skyndsamt och senast 72 timmar från mottagandet av begäran.

En sådan verksamhetsutövare som avses i 11 § är personuppgiftsansvarig för behandling av personuppgifter i registret.

13 § De skyldigheter som följer av 11 och 12 §§ gäller inte för den som är domänadministratör enligt lagen (2006:24) om nationella toppdomäner för Sverige på internet. För en sådan domänadministratör gäller skyldighet att föra register enligt 6 § den lagen.

Bemyndigande

14 § Regeringen eller den myndighet som regeringen bestämmer får meddela ytterligare föreskrifter om säkerhetsåtgärder enligt 3 § och om vad som utgör en betydande incident enligt 5 § andra stycket.

Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om utbildning, incidentrapportering, informationsskyldighet och register enligt 4–12 §§.

3 kap. Tillsyn

Tillsynsmyndigheten och tillsynsmyndighetens uppdrag

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

En tillsynsmyndighet ska utöva tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs. Den ska också utöva tillsyn över att sådana rättsakter följs som har antagits med stöd av artiklarna 21.5 och 23.11 i NIS 2-direktivet, i den ursprungliga lydelsen.

2 § Tillsynsåtgärder enligt 3, 4, 6 och 7 §§ får när det gäller viktiga verksamhetsutövare vidtas endast när tillsynsmyndigheten har anledning att anta att verksamhetsutövarna inte följer

1. denna lag eller föreskrifter som har meddelats i anslutning till lagen, eller
2. sådana rättsakter som har antagits med stöd av artiklarna 21.5 och 23.11 i NIS 2-direktivet, i den ursprungliga lydelsen.

Tillsynsmyndighetens befogenheter

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

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

5 § En tillsynsmyndighet får utföra regelbundna säkerhetsrevisioner av väsentliga verksamhetsutövare eller låta ett oberoende organ utföra sådana säkerhetsrevisioner.

6 § En tillsynsmyndighet får om det finns särskilda skäl utföra riktade säkerhetsrevisioner av den som står under tillsyn eller låta ett oberoende organ utföra sådana säkerhetsrevisioner.

7 § En tillsynsmyndighet får genomföra säkerhetsskanningar hos den som står under tillsyn.

En säkerhetsskanning ska ske i samarbete med verksamhetsutövaren.

8 § En tillsynsmyndighet får besluta att förelägga den som står under tillsyn att medverka till tillsynsåtgärder enligt 3–7 §§.

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

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

10 § Regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om säkerhetsrevisioner och säkerhetsskanningar enligt 5–7 §§.

Avgift

11 § En tillsynsmyndighet får av en sådan verksamhetsutövare som avses i 1 kap. 6 § och som anmäler verksamhet enligt 2 kap. 2 § ta ut en avgift för handläggningen av anmälningsärendet. Avgiften ska motsvara myndighetens kostnader för handläggningen av ärendet.

En tillsynsmyndighet ska ta ut en årlig avgift av en sådan verksamhetsutövare som avses i första stycket. De årliga avgifterna ska sammantagna motsvara de kostnader som myndigheten, utöver de kostnader som avses i första stycket, har för sin verksamhet enligt denna lag när det gäller dessa verksamhetsutövare. Avgifterna ska fördelas med skälig andel på var och en av verksamhetsutövarna.

4 kap. Ingripanden

När och hur tillsynsmyndigheten ska ingripa

1 § En tillsynsmyndighet ska ingripa om en verksamhetsutövare har åsidosatt sina skyldigheter enligt 2 kap. 1–10 §§ eller enligt föreskrifter som har meddelats i anslutning till de paragraferna eller enligt sådana rättsakter som har antagits med stöd av artiklarna 21.5 och 23.11 i NIS 2-direktivet, i den ursprungliga lydelsen.

Ett ingripande sker genom ett beslut om föreläggande enligt 4 §, en ansökan om förbud att inneha ledningsfunktion enligt 7 §, ett beslut om sanktionsavgift enligt 9 § eller, om det inte finns skäl att ingripa mot en överträdelse på något annat sätt, genom en anmärkning.

Tillsynsmyndigheten får avstå från ett ingripande om någon annan tillsynsmyndighet har vidtagit åtgärder mot verksamhetsutövaren med anledning av överträdelsen och dessa åtgärder bedöms tillräckliga.

Omständigheter som ska beaktas vid valet av ingripande

2 § Vid valet av ingripande ska hänsyn tas till hur allvarlig överträdelsen är, hur länge den har pågått och den skada eller risk för skada som uppstått till följd av överträdelsen. Vid bedömningen ska särskilt beaktas

1. om verksamhetsutövaren tidigare har gjort sig skyldig till en överträdelse,
2. vad verksamhetsutövaren har gjort för att förhindra eller minska skadan,
3. om överträdelsen har varit uppsåtlig eller berott på oaktsamhet, och
4. den ekonomiska fördel som överträdelsen har inneburit för verksamhetsutövaren.

3 § En överträdelse ska betraktas som allvarlig om verksamhetsutövaren

1. har begått upprepade överträdelser,
2. inte har fullgjort sin skyldighet att rapportera eller informera enligt 2 kap. 5–9 §§,
3. inte har avhjälpt en betydande incident,
4. inte har följt ett föreläggande enligt 4 § första stycket,
5. har hindrat en tillsynsåtgärd enligt 3 kap. 3–7 §§, eller
6. har lämnat falska eller andra grovt oriktiga uppgifter i fråga om säkerhetsåtgärder enligt 2 kap. 3 § eller i samband med incidentrapportering eller fullgörande av informationsskyldighet enligt 2 kap. 5–10 §§.

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

Tillsynsmyndigheten får också förelägga en verksamhetsutövare att offentliggöra information om överträdelser av sådana skyldigheter som avses i första stycket.

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

5 § En tillsynsmyndighet får besluta de förelägganden som behövs för att en verksamhetsutövare ska fullgöra skyldigheterna enligt 2 kap. 11 och 12 §§ eller enligt föreskrifter som har meddelats i anslutning till de paragraferna.

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

Förbud att inneha ledningsfunktion

6 § Den som är befattningshavare enligt 3 § andra stycket lagen (2014:836) om näringsförbud hos en enskild verksamhetsutövare får förbjudas att inneha en ledningsfunktion hos verksamhetsutövaren, om

1. verksamhetsutövaren är väsentlig,
2. det tidigare har riktats ett föreläggande mot verksamhetsutövaren enligt 4 § första stycket och föreläggandet inte har följts,
3. den överträdelse som har legat till grund för föreläggandet har varit allvarlig, och
4. befattningshavaren har orsakat överträdelsen uppsåtligen eller av grov oaktsamhet.

7 § Förbud enligt 6 § meddelas av allmän förvaltningsdomstol på ansökan av en tillsynsmyndighet.

Ansökan om förbud ska innehålla uppgifter om den person, befattning och verksamhetsutövare som ansökan avser. Den ska också innehålla uppgift om överträdelsen och de omständigheter som behövs för att kännetecknа den samt de bestämmelser som är tillämpliga på överträdelsen. Ansökan ska lämnas in till den förvaltningsrätt inom vars domkrets tillsynsmyndigheten är belägen.

Domstolen ska pröva målet skyndsamt.

8 § Ett förbud enligt 6 § ska meddelas för en viss tid, lägst ett och högst tre år, och gäller från det att beslutet om förbud får laga kraft.

På ansökan av tillsynsmyndigheten eller den enskilde ska den domstol som avses i 7 § upphäva förbudet, om det inte längre finns förutsättningar för det enligt 6 §. Ett beslut om upphävande gäller omedelbart.

Den enskilde ska vid ett beslut om förbud upplysas om sin rätt att ansöka om att förbudet upphävs enligt andra stycket.

Tillsynsmyndigheten ska så snart det kan ske ansöka om upphävande av förbudet, om den bedömer att det inte längre finns förutsättningar för förbudet.

Sanktionsavgift

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

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

1. det högsta av 2 procent av den totala globala årsomsättningen närmast föregående räkenskapsår eller ett belopp i kronor motsvarande 10 000 000 euro för en enskild verksamhetsutövare som är väsentlig,

2. det högsta av 1,4 procent av den totala globala årsomsättningen närmast föregående räkenskapsår eller ett belopp i kronor motsvarande 7 000 000 euro för en enskild verksamhetsutövare som är viktig, eller

3. 10 000 000 kronor för en offentlig verksamhetsutövare.

11 § 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.

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

Ett beslut om sanktionsavgift ska delges.

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

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

Sanktionsavgiften tillfaller staten.

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

5 kap. Överklagande

1 § Tillsynsmyndighetens beslut enligt denna lag får överklagas till allmän förvaltningsdomstol. När ett sådant beslut överklagas är tillsynsmyndigheten motpart i domstolen. Övriga beslut får inte överklagas.

Prövningstillstånd krävs vid överklagande till kammarrätten.

---

1. Denna lag träder i kraft den 15 januari 2026.

2. Genom lagen upphävs lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

3. Den upphävda lagen gäller dock fortfarande för överträdelser som har skett före ikraftträdandet.

På regeringens vägnar

ULF KRISTERSSON

CARL-OSKAR BOHLIN
(Försvarsdepartementet)