SVERIGES RIKSDAG

Försvarsutskottets betänkande 2025/26:FöU2

Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag

Sammanfattning

Utskottet ställer sig bakom regeringens förslag till cybersäkerhetslag som syftar till att genomföra det s.k. NIS 2-direktivet. Den nya lagen innebär att såväl offentliga som enskilda verksamhetsutövare inom vissa utpekade sektorer bl.a. ska vidta åtgärder för att skydda sina nätverks- och informationssystem samt rapportera betydande incidenter. I lagen finns också regler om tillsyn och ingripandemöjligheter vid överträdelser av lagens bestämmelser. Lagens syfte är att uppnå en hög nivå av cybersäkerhet i samhället. Utskottet tillstyrker även regeringens förslag till ändring i andra lagar som rör elektronisk kommunikation, toppdomäner och sekretess. De nya reglerna föreslås träda i kraft den 15 januari 2026. Utskottet anser att riksdagen bör avslå samtliga motionsyrkanden.

I betänkandet finns fem reservationer (S, V, C, MP).

Behandlade förslag

Proposition 2025/26:28 Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag.
Åtta yrkanden i följdmotioner.
Fyra yrkanden i motioner från allmänna motionstiden 2025/26.

Innehållsförteckning

Utskottets förslag till riksdagsbeslut 3
Redogörelse för ärendet 5
Ärendet och dess beredning 5
Propositionens huvudsakliga innehåll 6
Utskottets överväganden 7
Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag 7
Reservationer 30
1. Finansieringen av den nya lagen, punkt 2 (V, MP) 30
2. Ledningens ansvar, punkt 3 (C) 31
3. Påverkan på mindre företag och organisationer, punkt 4 (V, C, MP) 31
4. Övriga frågor om lagstiftningens framtida utformning, punkt 5 (V, C) 32
5. Cyberpolitikens utveckling, punkt 6 (S) 33
Bilaga 1
Förteckning över behandlade förslag 35
Propositionen 35
Följdmotionerna 35
Motioner från allmänna motionstiden 2025/26 36
Bilaga 2
Regeringens lagförslag 37

Utskottets förslag till riksdagsbeslut

1. Regeringens lagförslag

Riksdagen antar regeringens förslag till

1. cybersäkerhetslag,

2. lag om ändring i lagen (2006:24) om nationella toppdomäner för Sverige på internet,

3. lag om ändring i offentlighets- och sekretesslagen (2009:400),

4. lag om ändring i lagen (2022:482) om elektronisk kommunikation.

Därmed bifaller riksdagen proposition 2025/26:28 punkterna 1–4 och avslår motionerna

2025/26:3405 av Emma Berginger m.fl. (MP) yrkandena 10 och 68 samt 2025/26:3652 av Aylin Nouri m.fl. (S) yrkande 18.

2. Finansieringen av den nya lagen

Riksdagen avslår motion

2025/26:3834 av Ulf Holm m.fl. (MP).

Reservation 1 (V, MP)

3. Ledningens ansvar

Riksdagen avslår motion

2025/26:3838 av Mikael Larsson och Niels Paarup-Petersen (båda C) yrkande 1.

Reservation 2 (C)

4. Påverkan på mindre företag och organisationer

Riksdagen avslår motion

2025/26:3838 av Mikael Larsson och Niels Paarup-Petersen (båda C) yrkande 5.

Reservation 3 (V, C, MP)

5. Övriga frågor om lagstiftningens framtida utformning

Riksdagen avslår motion

2025/26:3838 av Mikael Larsson och Niels Paarup-Petersen (båda C) yrkandena 2–4, 6 och 7.

Reservation 4 (V, C)

6. Cyberpolitikens utveckling

Riksdagen avslår motion

2025/26:3556 av Peter Hultqvist m.fl. (S) yrkande 97.

Reservation 5 (S)

Stockholm den 2 december 2025

På försvarsutskottets vägnar

Peter Hultqvist

Följande ledamöter har deltagit i beslutet: Peter Hultqvist (S), Matheus Enholm (SD), Jörgen Berglund (M), Helén Pettersson (S), Helena Bouveng (M), Hanna Westerén (S), Gulan Avci (L), Erik Ezelius (S), Hanna Gunnarsson (V), Mikael Oscarsson (KD), Lars Püss (M), Per Söderlund (SD), Markus Selin (S), Camilla Brunsberg (M), Ann-Sofie Alm (M), Kerstin Lundgren (C) och Ulf Holm (MP).

Redogörelse för ärendet

Ärendet och dess beredning

I betänkandet behandlar utskottet proposition 2025/26:28 Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag. I propositionen finns en redogörelse för ärendets beredning fram till regeringens beslut om propositionen.

Regeringens förslag till riksdagsbeslut finns i bilaga 1. Regeringens lagförslag finns i bilaga 2. Två motioner med sammanlagt åtta yrkanden har väckts med anledning av propositionen. I betänkandet behandlas även fyra yrkanden i motioner från allmänna motionstiden 2025/26. Förslagen i motionerna finns i bilaga 1.

Bakgrund

I juli 2016 antog Europaparlamentet och rådet direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen, det s.k. NIS-direktivet. Syftet med direktivet var att förbättra den inre marknadens funktion genom att bl.a. fastställa åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverks- och informationssystem inom unionen. Direktivet gällde för leverantörer av samhällsviktiga tjänster inom sju särskilt utpekade sektorer.

NIS-direktivet genomfördes i svensk rätt genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster och den tillhörande förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Den 14 december 2022 antog Europaparlamentet och rådet direktiv (EU) 2022/2555 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 (det s.k. NIS 2-direktivet).

Genom NIS 2-direktivet upphävdes alltså NIS-direktivet. Medlemsstaterna skulle senast den 17 oktober 2024 ha antagit de nationella bestämmelser som krävs för att genomföra det nya direktivet.

Propositionens huvudsakliga innehåll

EU antog 2022 ett direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå inom EU, det s.k. NIS 2-direktivet. I syfte att genomföra direktivet i svensk rätt föreslår regeringen att det ska införas en ny cybersäkerhetslag.

Den nya lagen innebär att offentliga och enskilda verksamhetsutövare inom vissa utpekade sektorer bl.a. ska vidta åtgärder för att skydda sina nätverks- och informationssystem samt rapportera betydande incidenter. Den nya lagen innehåller också regler om tillsyn och ingripandemöjligheter för verksamhetsutövare som inte följer lagens bestämmelser. Därutöver föreslås ändringar i andra lagar som rör elektronisk kommunikation, toppdomäner och sekretess.

Den nya lagen och övriga lagändringar föreslås träda i kraft den 15 januari 2026.

Utskottets överväganden

Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag

Utskottets förslag i korthet

Riksdagen antar regeringens förslag till cybersäkerhetslag samt förslag till ändring i lagen om nationella toppdomäner för Sverige på internet, offentlighets- och sekretesslagen och lagen om elektronisk kommunikation. Riksdagen avslår motionsyrkanden som får anses tillgodosedda genom lagförslagen.

Riksdagen avslår även övriga motionsyrkanden som rör bl.a. olika aspekter av lagstiftningens framtida utformning.

Jämför reservation 1 (V, MP), 2 (C), 3 (V, C, MP), 4 (V, C) och 5 (S).

Propositionen

Regeringen redovisar i propositionen i huvudsak följande förslag och bedömningar.

NIS 2-direktivet

En översyn av NIS-direktivet har visat brister som hindrat direktivet från att effektivt hantera utmaningar på cybersäkerhetsområdet. Översynen har också visat på stora skillnader i genomförandet, vilket har medfört en fragmentering av den inre marknaden. NIS 2-direktivets mål är att undanröja skillnaderna mellan medlemsstaterna. Mot den bakgrunden upphävdes NIS-direktivet och ersattes av NIS 2-direktivet.

Syftet med NIS 2-direktivet är att förbättra den inre marknadens funktion genom att fastställa åtgärder för att uppnå en hög gemensam cybersäkerhetsnivå inom unionen. NIS 2-direktivet innebär skärpta krav på berörda aktörer jämfört med NIS-direktivet och omfattar betydligt fler aktörer.

Direktivet är tillämpligt på offentliga eller privata entiteter av den typ som avses i direktivets bilaga 1 eller 2, som uppfyller ett visst storlekskrav och som tillhandahåller sina tjänster eller bedriver sin verksamhet i unionen. Direktivet är även tillämpligt på vissa entiteter oavsett storlek. I bilagorna till direktivet anges de 18 sektorer, uppdelade i högkritiska och andra kritiska sektorer, som omfattas av direktivet:

- energi
- transporter
- bankverksamhet

- finansmarknadsinfrastruktur
- hälso- och sjukvårdssektorn
- dricksvatten
- avloppsvatten
- digital infrastruktur
- förvaltning av tjänster inom informations- och kommunikationsteknik (IKT), mellan företag
- offentlig förvaltning
- rymden
- post- och budtjänster
- avfallshantering
- tillverkning, produktion och distribution av kemikalier
- produktion, bearbetning och distribution av livsmedel
- tillverkning
- digitala leverantörer
- forskning.

Jämfört med det förra direktivet (som gällde sju utpekade sektorer) omfattas alltså många fler sektorer. Kraven har även skärpts på vilka åtgärder berörda aktörer ska vidta för att bl.a. hantera risker och förhindra incidenter kopplade till de nätverks- och informationssystem som de använder. Dessutom har mer precisa rapporteringsskyldigheter införts, bl.a. när det gäller skyldigheten att rapportera betydande incidenter till en utpekad myndighet. Det finns också bestämmelser om tillsyns- och efterlevnadskontrollåtgärder samt sanktioner.

I likhet med vad som gällde enligt NIS-direktivet ska medlemsstaterna enligt NIS 2-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 ha en sambandsfunktion som säkerställer gränsöverskridande samarbete mellan olika medlemsstaters myndigheter och ett sektorsövergripande samarbete mellan de nationella behöriga myndigheterna i varje medlemsstat. NIS 2-direktivet föreskriver, i likhet med vad som gällde tidigare, att det ska finnas en eller flera enheter för hantering av it-säkerhetsincidenter, s.k. CSIRT-enheter (Computer Security Incident Response Team). Vidare ska medlemsstaterna utse en eller flera behöriga myndigheter, s.k. cyberkrishanteringsmyndigheter, som ska ansvara för hanteringen av storskaliga cybersäkerhetsincidenter och cyberkriser.

Genom NIS-direktivet inrättades bl.a. en samarbetsgrupp för att stödja och underlätta strategiskt samarbete och utbyte av information mellan medlemsstaterna samt ett nätverk för nationella CSIRT-enheter. I NIS 2-direktivet stärks det befintliga samarbetet samt inrättas nya forum för samarbete mellan medlemsstaterna. Ett av dessa är det europeiska kontaktnätverket för cyberkriser, EU-CyCLONe, som ska verka stödjande vid samordning och hantering av storskaliga incidenter och cyberkriser. I likhet med NIS-direktivet

föreskriver NIS 2-direktivet också en skyldighet för medlemsstaterna att anta en nationell strategi för cybersäkerhet.

NIS 2-direktivet är ett s.k. minimidirektiv, vilket innebär att medlemsstaterna får anta eller behålla bestämmelser som säkerställer en högre cybersäkerhetsnivå, förutsatt att sådana bestämmelser står i överensstämmelse med medlemsstaternas förpliktelser enligt unionsrätten.

En ny cybersäkerhetslag ska införas

Regeringen föreslår att NIS 2-direktivet i huvudsak ska genomföras genom en ny cybersäkerhetslag. Syftet med den nya lagen ska vara att uppnå en hög nivå av cybersäkerhet i samhället.

Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster ska samtidigt upphävas.

Vilka ska omfattas av lagen?

I propositionen föreslår regeringen att såväl offentliga som enskilda verksamhetsutövare ska omfattas av den nya lagen enligt följande.

Lagen ska gälla för en verksamhetsutövare som i Sverige tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster.

Lagen ska även gälla för en verksamhetsutövare som har huvudsakligt etableringsställe i Sverige, eller en företrädare som är etablerad i Sverige, och som är en registreringsenhet för toppdomäner eller erbjuder domännamnssystemtjänster (DNS-tjänster) eller domännamnsregistreringstjänster.

Lagen ska vidare gälla för en verksamhetsutövare som har huvudsakligt etableringsställe i Sverige, eller en företrädare som är etablerad i Sverige, och som storleksmässigt motsvarar eller är större än ett medelstort företag, och erbjuder molntjänster, datacentraltjänster, nätverk för leverans av innehåll, utlokaliserade driftstjänster, utlokaliserade säkerhetstjänster, marknadsplatser online, sökmotorer eller plattformar för sociala nätverkstjänster.

Lagen ska även gälla för en verksamhetsutövare som är etablerad i Sverige och tillhandahåller betrodda tjänster.

Lagen ska också gälla för en verksamhetsutövare som omfattas av bilaga 1 eller 2 till NIS 2-direktivet i övrigt och är etablerad i Sverige samt en verksamhetsutövare som erbjuder molntjänster, datacentraltjänster, nätverk för leverans av innehåll, utlokaliserade driftstjänster, utlokaliserade säkerhetstjänster, marknadsplatser online, sökmotorer eller plattformar för sociala nätverkstjänster, om

- verksamhetsutövaren är den enda leverantören av en tjänst i Sverige som är väsentlig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet

- 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 eller
- 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.

Lagen ska därutöver gälla för en annan verksamhetsutövare som omfattas av bilaga 1 eller 2 till NIS 2-direktivet i övrigt, om verksamhetsutövaren är etablerad i Sverige och storleksmässigt motsvarar eller är större än ett medelstort företag.

Ett medelstort företag ska i lagen definieras som 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.

I propositionen redogör regeringen för att ett medelstort företag enligt definitionen innebär att en verksamhetsutövare som har minst 50 anställda eller en balansomslutning och årsomsättning som överstiger 10 000 000 euro per år omfattas av lagen.

Regeringen eller den myndighet som regeringen bestämmer ska enligt förslaget i propositionen få meddela ytterligare föreskrifter om kriterier för när verksamhetsutövare ska omfattas av lagen med hänvisning till deras särskilda betydelse.

Regeringen eller den myndighet som regeringen bestämmer ska också få meddela föreskrifter om vad som utgör huvudsakligt etableringsställe och om undantag från skyldigheterna enligt lagen för vissa partnerföretag och anknutna företag.

Regeringen eller den myndighet som regeringen bestämmer ska, i enskilda fall, om det finns särskilda skäl, få besluta om undantag från skyldigheterna enligt lagen för vissa partnerföretag och anknutna företag.

I regeringens förslag finns också regler om vilka lärosäten som omfattas av lagen.

Vidare föreslår regeringen att de verksamhetsutövare som uppfyller kriterierna för att omfattas av lagen ska som utgångspunkt omfattas av regelverket i sin helhet, dvs. lagens krav ska gälla hela verksamheten hos den aktuella utövaren och inte endast den del som faller inom någon av de utpekade sektorerna. Undantag finns dock för sådan verksamhet som bedriver säkerhetskänslig verksamhet till någon del (se nedan).

Andra offentliga verksamhetsutövare som ska omfattas av lagen

Offentliga verksamhetsutövare ska omfattas av lagen om de uppfyller något av kraven som beskrivits ovan. Därutöver föreslår regeringen att offentlig verksamhet ska omfattas av lagen enligt följande.

Statliga myndigheter som har befogenhet att fatta beslut som påverkar fysiska eller juridiska personers rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital ska omfattas av lagen.

Därutöver ska de statliga myndigheter som regeringen bestämmer omfattas av lagen. Regeringen, Regeringskansliet, utlandsmyndigheter, kommittéväsendet, myndigheter under riksdagen, domstolar och nämnder som utövar rättskipning ska däremot inte omfattas av lagen.

Även regioner, kommuner och kommunalförbund, med undantag för fullmäktige och förbundsdirektion, ska omfattas av lagen.

Väsentliga och viktiga verksamhetsutövare

Regeringen föreslår att verksamhetsutövarna ska delas in i väsentliga och viktiga sådana. Kategoriseringen får betydelse för bl.a. vilka tillsynsåtgärder som kan vidtas.

Enligt förslaget ska följande verksamhetsutövare betecknas som väsentliga:

- en verksamhetsutövare som är en statlig myndighet
- en verksamhetsutövare som är en kommun eller en region och som är större än ett medelstort företag
- en verksamhetsutövare som tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster och som storleksmässigt motsvarar eller är större än ett medelstort företag
- en verksamhetsutövare som är en kvalificerad tillhandahållare av betrodda tjänster
- en verksamhetsutövare som är en registreringsenhet för toppdomäner eller erbjuder DNS-tjänster eller
- en verksamhetsutövare som är större än ett medelstort företag och som i övrigt omfattas av bilaga 1 till NIS 2-direktivet eller som är en enskild utbildningsanordnare med tillstånd att utfärda examina enligt lagen (1993:792) om tillstånd att utfärda vissa examina.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela ytterligare föreskrifter om när verksamhetsutövare som omfattas av lagen med hänvisning till deras särskilda betydelse i samhället ska räknas som väsentliga.

Verksamhetsutövare som inte är väsentliga ska räknas som viktiga verksamhetsutövare.

Undantag från lagens tillämpningsområde

Undantag på grund av krav i andra författningar

Regeringen föreslår att 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 den nya lagen, med beaktande av bestämmelsernas

omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till kraven i bestämmelserna.

Regeringen anför att det kan finnas sådana bestämmelser inom t.ex. sjöfartssektorn, banksektorn och sektorn för finansmarknadsinfrastruktur.

Regeringen föreslår också vissa undantag från lagen med hänvisning till bestämmelser i den s.k. DORA-förordningen som gäller digital operativ motståndskraft i den finansiella sektorn.

Undantag för säkerhetskänslig verksamhet och brottsbekämpande verksamhet

Regeringen föreslår att lagen inte ska gälla för en enskild verksamhetsutövare som enbart bedriver säkerhetskänslig verksamhet.

Lagen ska enligt förslaget inte heller gälla för en statlig myndighet som till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpande verksamhet. Lagen ska inte gälla för en enskild verksamhetsutövare som enbart erbjuder tjänster till en sådan statlig myndighet.

För andra verksamhetsutövare som till någon del bedriver säkerhetskänslig verksamhet eller brottsbekämpande verksamhet eller till någon del erbjuder tjänster till en sådan statlig myndighet som anges ovan ska skyldigheterna enligt lagen, frånsett skyldigheten att utse företrädare och anmälningsskyldigheten, inte gälla i förhållande till den säkerhetskänsliga verksamheten eller brottsbekämpande verksamheten eller den verksamhet som erbjuder tjänsterna.

Undantagen ska inte gälla för en verksamhetsutövare som tillhandahåller betrodda tjänster.

I propositionen anför regeringen att säkerhetskänslig verksamhet som ska undantas från lagens tillämpningsområde är sådan verksamhet som omfattas av säkerhetsskyddslagen (2018:585). Med brottsbekämpande verksamhet avses sådan verksamhet som en brottsbekämpande myndighet bedriver för att förebygga, förhindra eller upptäcka brottslig verksamhet eller för att utreda eller lagföra brott.

Med anledning av remissynpunkter på gränsdragningsproblem framhåller regeringen att med uttrycket *övervägande del* i aktuell bestämmelse avses att myndighetens huvudsakliga verksamhet rör säkerhetskänslig verksamhet eller utgör brottsbekämpning. I de fallen undantas myndigheten i helhet från lagens tillämpningsområde. Vilka myndigheter som bedriver säkerhetskänslig verksamhet till övervägande del får enligt regeringen bedömas i varje enskilt fall. När det gäller verksamhetsutövare som till någon (men inte övervägande) del bedriver säkerhetskänslig eller brottsbekämpande verksamhet kommer den delen av verksamheten att omfattas endast av lagens krav på anmälan och, i förekommande fall, av kravet på att utse företrädare samt tillsyn och ingripanden kopplat till dessa. För den övriga delen gäller lagen i sin helhet. Även om det kan vara svårt att särskilja vilken del av verksamheten som är undantagen från den övriga anser regeringen att det utifrån direktivets formulering saknas utrymme för någon annan lösning.

Regeringen anför vidare att säkerhetsskyddsregleringen och den nya cybersäkerhetslagen kommer att gälla parallellt. Regeringen konstaterar också att de två regelverken har olika tillämpningsområden och syften. Införandet av den nya lagen innebär inte några förändrade krav enligt säkerhetsskyddslagen. De verksamhetsutövare som omfattas av den regleringen ska alltjämt göra noggranna säkerhetsskyddsanalyser och vidta de säkerhetsskyddsåtgärder som bedöms nödvändiga utifrån den analysen.

Undantag för säkerhetskyddsklassificerade uppgifter

Regeringen föreslår att skyldigheterna att lämna uppgifter enligt lagen inte ska gälla säkerhetsskyddsklassificerade uppgifter.

Verksamhetsutövares skyldigheter

Vissa enskilda verksamhetsutövare ska utse en företrädare

Regeringen föreslår att verksamhetsutövare som erbjuder vissa tjänster i Sverige, men saknar etablering inom EES, ska utse en företrädare med etablering i Sverige eller i något annat land inom EES där tjänsterna erbjuds. Skyldigheten ska gälla bl.a. om verksamhetsutövaren är en registreringsenhet för toppdomäner eller erbjuder DNS-tjänster eller domännamnsregistreringstjänster.

Samtliga verksamhetsutövare ska göra en anmälan

Regeringen föreslår en skyldighet för samtliga verksamhetsutövare att 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.

Skyldighet att vidta säkerhetsåtgärder

Regeringen föreslår en skyldighet för verksamhetsutövare att 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
10. vid behov användning av lösningar för autentisering, säkrade kommunikationer och säkrade nödkommunikationssystem.

Regeringen eller den myndighet som regeringen bestämmer ska få meddela ytterligare föreskrifter om säkerhetsåtgärder.

Ledningen ska genomgå utbildning om säkerhetsåtgärder

Regeringen föreslår att de personer som ingår i ledningen för en verksamhetsutövare ska genomgå utbildning om säkerhetsåtgärder. Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om utbildningen.

Regeringen bedömer däremot att det inte behöver införas någon särskild reglering om att ledningen ska godkänna säkerhetsåtgärder och övervaka genomförandet av dem.

Som skäl för regeringens bedömning i denna del anför regeringen att artikel 20 i direktivet ställer krav på att verksamhetsutövarens ledningsorgan ska godkänna och övervaka genomförandet av säkerhetsåtgärder samt genomgå utbildning med anledning av detta. Syftet är att ledningsorganen kan ställas till svars för överträdelser. Enligt regeringen omfattas ledningsorgan i både offentliga och privata entiteter av skyldigheterna, även om nationell rätt om bl.a. ansvarsregler som är tillämpliga på offentliga institutioner och ansvaret för statligt anställda inte ska påverkas enligt direktivet. Regeringen anser att uttrycket ledningsorgan som används, men inte definieras, i ett svenskt sammanhang motsvaras av uttrycket ledning. Detta uttryck har ingen vedertagen entydig innebörd och eftersom den nya lagen kommer att omfatta många olika typer av verksamhetsutövare måste en bedömning av vem som anses ingå i ledningen göras från fall till fall.

För ett aktiebolag får ledningen enligt regeringen primärt avse styrelsen. Av 8 kap. 4 § aktiebolagslagen (2005:551) framgår att styrelsen svarar för ett aktiebolags organisation och förvaltningen av bolagets angelägenheter. Enligt 8 kap. 27 och 29 §§ aktiebolagslagen ska den verkställande direktören utses av styrelsen och sköta den löpande förvaltningen enligt styrelsens riktlinjer och anvisningar. Den verkställande direktören är med andra ord underställd styrelsen. Med hänsyn till utformningen och innebörden av aktuell artikel i direktivet anser regeringen att ledningen i det här sammanhanget bör omfatta styrelsen, den verkställande direktören och ersättare för dessa. Motsvarande ordning gäller för ekonomiska föreningar enligt 7 kap. 4 och 29 §§ lagen (2018:672) om ekonomiska föreningar. För handelsbolag gäller enligt lagen (1980:1102) om handelsbolag och enkla bolag att bolagsmännen ansvarar för förvaltningen.

När det gäller offentliga verksamhetsutövare hänvisar regeringen till 2 § myndighetsförordningens definition av ledning. I den paragrafen framgår att huvudregeln är att en myndighet under regeringen leds av en myndighetschef om det är en enrådighetsmyndighet, en styrelse om det är en styrelsemyndighet och en nämnd om det är en nämndmyndighet. Av samma paragraf framgår att myndighetens ledningsform anges i myndighetens instruktion eller i någon annan författning. Regeringen anser inte att uttrycket bör ges någon annan betydelse i den nya lagen. För kommuner och regioner anser regeringen att ledningen utgörs av kommun- respektive regionstyrelsen i enlighet med 6 kap. 1 § kommunallagen (2017:725). Av paragrafen framgår att styrelsen ska leda och samordna förvaltningen av kommunens eller regionens angelägenheter och ha uppsikt över bl.a. övriga nämnders verksamhet.

Mot denna bakgrund anser regeringen att ledningen i enskilda och offentliga verksamhetsutövare ansvarar för att godkänna säkerhetsåtgärder och övervaka genomförandet av dem på det sätt som framgår av direktivet utan särskild reglering. Regeringen bedömer därmed att direktivets krav i denna del inte behöver regleras i lagen.

Incidentrapportering och informationsskyldighet

Regeringen föreslår en skyldighet för verksamhetsutövare att rapportera betydande incidenter enligt följande.

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 den betydande incidenten. Verksamhetsutövare ska till samma myndighet göra en incidentanmälan om den betydande incidenten så snart det kan ske, dock senast 72 timmar efter det att verksamhetsutövaren har fått kännedom om den betydande incidenten. För verksamhetsutövare som tillhandahåller betrodda tjänster ska anmälan i stället göras senast 24 timmar efter sådan kännedom. På begäran av myndigheten ska verksamhetsutövare lämna en delrapport med relevanta statusuppdateringar för den betydande incidenten. Senast en månad efter incidentanmälan ska verksamhetsutövare lämna en slutrapport till myndigheten. 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 den betydande incidenten har hanterats. Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om incidentrapporteringen.

Regeringen föreslår vidare en informationsskyldighet för verksamhetsutövare vid betydande incidenter och betydande cyberhot enligt följande.

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. 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. Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om informationsskyldigheten.

Förhållandet till säkerhetsskyddslagen i fråga om incidentrapportering

Regeringen uppger att ett flertal remissinstanser har resonerat om hur förslaget om incidentrapportering förhåller sig till säkerhetsskyddsregleringen. En del har begärt ett förtydligande i fråga om att berörda aktörer inte ska behöva rapportera incidenter enligt såväl den nya lagen som säkerhetsskyddsregleringen. Med anledning av detta redogör regeringen för bl.a. följande regler ur det regelverket. Enligt 2 kap. 1 § säkerhetsskyddslagen ska en verksamhetsutövare anmäla och rapportera sådant som är av vikt för säkerhetsskyddet. Enligt 2 kap. 4 § säkerhetsskyddsförordningen (2021:955) ska en verksamhetsutövare skyndsamt göra en anmälan till Säkerhetspolisen vid säkerhetshotande händelser eller verksamhet. Detta gäller bl.a. om det inträffat en it-incident i ett informationssystem som verksamhetsutövaren är ansvarig för och som har betydelse för säkerhetskänslig verksamhet och där incidenten allvarligt kan påverka säkerheten i systemet. Om verksamhetsutövaren tillhör Försvarsmaktens tillsynsområde ska anmälan göras också till Försvarsmakten.

Regeringen påminner om att den nya lagen inte ska gälla för bl.a. statliga myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet och inte heller för enskilda verksamhetsutövare som enbart bedriver sådan verksamhet eller enbart erbjuder tjänster till en statlig myndighet som till övervägande del bedriver säkerhetskänslig verksamhet. För andra utövare som till någon del bedriver säkerhetskänslig verksamhet eller till någon del erbjuder tjänster till en statlig myndighet som i sin tur till övervägande del bedriver säkerhetskänslig verksamhet gäller inte vissa krav, t.ex. rapporteringsskyldigheten, för den del av verksamheten som är säkerhetskänslig eller tillhandahåller tjänsterna. För övriga delar föreslås lagen gälla i dess helhet. Regeringen anför att förslaget om rapportering enligt den nya lagen i allt väsentligt följer NIS 2-direktivets krav och därmed är nödvändigt för att genomföra direktivet i nationell rätt. Om en annan författning innehåller bestämmelser om krav på säkerhetsåtgärder eller incidentrapportering med motsvarande verkan gäller enligt regeringens förslag inte kraven i den nya lagen för verksamhetsutövaren (se ovan om undantag på grund av krav i andra författningar).

Regeringen konstaterar att det visserligen skulle kunna uppstå en situation då samma incident både påverkar den säkerhetskänsliga verksamhet som verksamhetsutövaren bedriver och övrig verksamhet. För verksamhetsutövare som endast undantas från rapporteringsskyldigheten i vissa delar kan det då bli fråga om att rapportera incidenten enligt båda regelverken. Regeringen uppger att den tar frågan om vilka negativa konsekvenser som parallella regelverk kan föra med sig på allvar. Regeringen bedömer dock att det inte finns något utrymme, med tanke på direktivets innehåll och regelverkens olika syften och tillämpningsområden, att t.ex. låta ett av regelverken vara subsidiärt

i förhållande till det andra. Mot bakgrund av att anmälningarna enligt den nya lagen och säkerhetsskyddslagen hanteras av olika myndigheter, utifrån olika befogenheter och ur olika perspektiv, bedömer regeringen att det inte finns risk för att verksamhetsutövare ska uppleva otydlighet i fråga om vad skyldigheterna innebär. Regeringen kan därför inte se att incidentrapporteringen enligt den nya lagen kan komma i konflikt med säkerhetsskyddsregleringen. Den administrativa börda som dubbla anmälningar kan innebära anses vidare vara godtagbar.

Tillsyn

Regeringen föreslår att det i lagen införs följande bestämmelser om tillsyn.

Den eller de myndigheter som regeringen bestämmer ska vara tillsynsmyndighet. Regeringen avser att peka ut dessa i förordningen till lagen.

En tillsynsmyndighet ska utöva tillsyn över att lagen och föreskrifter som har meddelats i anslutning till lagen följs. Tillsynsmyndigheten ska också utöva tillsyn över att sådana rättsakter följs som har antagits med stöd av NIS 2-direktivet.

I fråga om tillsynsmyndigheternas befogenheter föreslår regeringen att den som står under tillsyn ska vara skyldig att på begäran tillhandahålla en tillsynsmyndighet de uppgifter eller handlingar som myndigheten behöver för sin tillsyn. En tillsynsmyndighet ska ha rätt att i den omfattning som det behövs för tillsynen få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamheten. En tillsynsmyndighet ska också få begära handräckning av Kronofogdemyndigheten för att genomföra tillsynsåtgärderna. Vid handräckning ska bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande gälla. En tillsynsmyndighet ska få besluta att förelägga verksamhetsutövaren att tillhandahålla uppgifterna eller handlingarna och att ge tillträde. Ett föreläggande ska få förenas med vite. Ett vitesföreläggande ska även få riktas mot staten.

Regeringen föreslår vidare att en tillsynsmyndighet ska, om det finns särskilda skäl, få utföra riktade säkerhetsrevisioner av den som står under tillsyn eller låta ett oberoende organ utföra sådana säkerhetsrevisioner. En tillsynsmyndighet ska även få utföra regelbundna säkerhetsrevisioner av väsentliga verksamhetsutövare eller låta ett oberoende organ utföra sådana säkerhetsrevisioner. En tillsynsmyndighet ska också få genomföra säkerhetsskanningar hos den som står under tillsyn. En säkerhetsskanning ska ske i samarbete med verksamhetsutövaren. Tillsynsmyndigheten ska få förelägga verksamhetsutövare att medverka till säkerhetsrevisioner och till säkerhetsskanning. Ett sådant föreläggande ska få förenas med vite. Ett vitesföreläggande ska även få riktas mot staten. Regeringen eller den myndighet som regeringen bestämmer ska få meddela föreskrifter om säkerhetsrevisioner och om säkerhetsskanningar.

När det gäller viktiga verksamhetsutövare föreslår regeringen att tillsynsåtgärder endast ska få vidtas när tillsynsmyndigheten har anledning att anta att lagen, de föreskrifter som har meddelats i anslutning till lagen eller sådana rättsakter som har antagits med stöd av NIS 2-direktivet inte följs.

Med anledning av remissynpunkter på vikten av samordning mellan de tilltänkta tillsynsmyndigheterna konstaterar regeringen att det av 6 § myndighetsförordningen (2007:515) framgår att en myndighet ska verka för att genom samarbete med bl.a. andra myndigheter ta till vara de fördelar som kan vinnas för enskilda och för staten som helhet. Vidare följer av 8 § förvaltningslagen (2017:900) att en myndighet inom sitt verksamhetsområde ska samverka med andra myndigheter och i rimlig utsträckning hjälpa den enskilde genom att själv inhämta upplysningar eller yttranden från andra myndigheter. Regeringen utgår från att samverkan mellan tillsynsmyndigheterna kommer att fungera väl när det gäller bl.a. sådana frågor som behöver hanteras gemensamt.

Avgift vid tillsyn med koppling till viss digital infrastruktur

Regeringen föreslår att en tillsynsmyndighet ska få ta ut en handläggningsavgift och en årlig avgift av en verksamhetsutövare som tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster i Sverige och som har anmält sin verksamhet enligt lagen.

Handläggningsavgiften ska motsvara myndighetens kostnader för handläggningen av anmälningsärendet. De årliga avgifterna ska sammantagna motsvara de kostnader som myndigheten, utöver kostnaderna för handläggning av ärendet, har för sin verksamhet enligt lagen när det gäller nämnda slags verksamhetsutövare. Avgifterna ska fördelas med skälig andel på var och en av verksamhetsutövarna.

Ingripanden

Regeringen föreslår i propositionen i huvudsak följande bestämmelser om ingripanden vid överträdelser av lagen.

Vilka överträdelser ska kunna leda till ingripanden?

Enligt regeringens förslag ska en tillsynsmyndighet ingripa om en verksamhetsutövare har åsidosatt sina skyldigheter att utse företrädare, göra en anmälan, vidta säkerhetsåtgärder, låta de personer som ingår i ledningen genomgå utbildning, rapportera betydande incidenter eller informera vid betydande incidenter och betydande cyberhot enligt lagen eller enligt föreskrifter som har meddelats i anslutning till lagen. Tillsynsmyndigheten ska också ingripa om verksamhetsutövaren har åsidosatt sina skyldigheter enligt sådana rättsakter som har antagits med stöd av NIS 2-direktivet.

Vilka möjligheter till ingripande ska finnas?

Regeringen föreslår att ingripande ska ske genom ett beslut om föreläggande, en ansökan om förbud att inneha ledningsfunktion, ett beslut om sanktionsavgift eller genom en anmärkning. Tillsynsmyndigheten ska få avstå från ingripande om någon annan tillsynsmyndighet har vidtagit åtgärder mot verksamhetsutövaren med anledning av överträdelsen och dessa åtgärder bedöms tillräckliga.

Val av ingripande

Vid valet av ingripande ska enligt regeringens förslag 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 om verksamhetsutövaren tidigare har gjort sig skyldig till en överträdelse, vad verksamhetsutövaren har gjort för att förhindra eller minska skadan, om överträdelsen har varit uppsåtlig eller berott på oaktsamhet och den ekonomiska fördel som överträdelsen har inneburit för verksamhetsutövaren.

Regeringen föreslår att en överträdelse ska betraktas som allvarlig om verksamhetsutövaren

1. har begått upprepade överträdelser
2. inte har fullgjort sin skyldighet att rapportera eller informera om betydande incidenter
3. inte har avhjälpt en betydande incident
4. inte har följt ett föreläggande om att fullgöra vissa skyldigheter enligt lagen
5. har hindrat en tillsynsåtgärd eller
6. har lämnat falska eller andra grovt oriktiga uppgifter i fråga om säkerhetsåtgärder eller i samband med incidentrapportering eller fullgörande av informationsskyldighet.

Förelägganden

En tillsynsmyndighet ska få besluta om de förelägganden som behövs för att en verksamhetsutövare ska fullgöra sina skyldigheter att utse företrädare, göra en anmälan, vidta säkerhetsåtgärder, låta de personer som ingår i ledningen genomgå utbildning, rapportera betydande incidenter eller informera vid betydande incidenter och betydande cyberhot.

Tillsynsmyndigheten ska också få förelägga en verksamhetsutövare att offentliggöra information om överträdelser av dessa skyldigheter. Ett föreläggande ska få förenas med vite. Ett vitesföreläggande ska även få riktas mot staten.

Förbud att inneha ledningsfunktion

Regeringen föreslår att den som är befattningshavare hos en enskild verksamhetsutövare ska få förbjudas att inneha en ledningsfunktion hos verksamhetsutövaren, om

1. verksamhetsutövaren är väsentlig
2. det tidigare har riktats ett föreläggande mot verksamhetsutövaren om att fullgöra skyldigheterna att utse företrädare, göra en anmälan, vidta säkerhetsåtgärder, låta de personer som ingår i ledningen genomgå utbildning, rapportera betydande incidenter eller informera vid betydande incidenter och betydande cyberhot och föreläggandet inte har följts
3. den överträdelse som har legat till grund för föreläggandet har varit allvarlig
4. befattningshavaren har orsakat överträdelsen uppsåtligen eller av grov oaktsamhet.

Med anledning av remissynpunkter som gäller vilken krets av personer hos en enskild verksamhetsutövare som kan träffas av förbudet framhåller regeringen att enligt artikel 32.5 b i direktivet ska förbudet kunna träffa varje fysisk person som på nivån för verkställande direktör eller juridiskt ombud har ledningsansvar i den väsentliga entiteten. I artikel 20 anges att viktiga och väsentliga entiteters ledningsorgan har ett ansvar för att godkänna och övervaka genomförandet av säkerhetsåtgärder och att de ska kunna ställas till svars för entiteternas överträdelse av artikel 21 som rör sådana åtgärder. Personkretsen i artiklarna 20 och 32.5 b är alltså definierad på olika sätt och den senare skulle kunna uppfattas som snävare än den som omfattas av artikel 20. Regeringen anser dock att förbudet bör kunna träffa den bredare krets som avses i artikel 20. Inte minst för att upprätthålla systematiken och för att denna krets ska kunna bli föremål för ingripanden på det sätt som artikel 20 i direktivet förutsätter. Regeringen föreslår således att ett förbud ska kunna meddelas mot befattningshavare enligt 3 § andra stycket lagen om näringsförbud. Det kan därmed röra sig om t.ex. en styrelseledamot, en verkställande direktör samt ersättare för dessa i ett aktiebolag. Förbudet förutsätter dock att personen med ledningsansvar ska ha orsakat den allvarliga överträdelsen uppsåtligen eller av grov oaktsamhet.

Regeringen föreslår att ett förbud ska meddelas av allmän förvaltningsdomstol på ansökan av en tillsynsmyndighet. Ett förbud ska vara tidsbegränsat och gälla lägst ett och högst tre år. I propositionen lämnar regeringen också förslag på andra regler om förfarandet vid en ansökan om förbud.

Sanktionsavgifter

Regeringen föreslår att tillsynsmyndigheten ska få besluta att ta ut en sanktionsavgift av en verksamhetsutövare om verksamhetsutövaren åsidosatt sina skyldigheter att utse företrädare, göra en anmälan, vidta säkerhetsåtgärder, låta de personer som ingår i ledningen genomgå utbildning, rapportera betydande incidenter eller informera vid betydande incidenter och betydande cyberhot.

I fråga om sanktionsavgifternas storlek föreslår regeringen att för enskilda verksamhetsutövare som är väsentliga ska avgiften bestämmas till lägst 5 000 kronor och högst till det högsta av 2 procent av verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår eller ett belopp i

kronor motsvarande 10 000 000 euro. För enskilda verksamhetsutövare som är viktiga ska avgiften bestämmas till lägst 5 000 kronor och högst till det högsta av 1,4 procent av verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår eller ett belopp i kronor motsvarande 7 000 000 euro. För offentliga verksamhetsutövare ska avgiften bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor.

När det gäller förfarandet föreslår regeringen bl.a. att en sanktionsavgift inte ska få beslutas om överträdelsen omfattas av ett föreläggande om vite och överträdelsen ligger till grund för en ansökan om utdömande av vitet.

I propositionen framhåller regeringen att det inte finns utrymme att fastställa lägre maximibelopp för enskilda verksamhetsutövare än de föreslagna eftersom de följer av direktivet (artikel 34). Direktivet saknar däremot regler om miniminivåer. Av NIS-direktivet följde inte några beloppsgränser, men enligt 30 § NIS-lagen ska en sanktionsavgift bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor. Regeringen anser att det inte finns skäl att nu förändra miniminivån och den bör därför även fortsättningsvis vara 5 000 kronor för både offentliga och enskilda verksamhetsutövare.

Med anledning av remissynpunkter på diskrepansen mellan offentliga och enskilda verksamhetsutövare i fråga om sanktionsavgiftens maximibelopp konstaterar regeringen att det inom ramen för ett antal regleringar görs sådan skillnad (t.ex. i 7 kap. 4 § säkerhetsskyddslagen). Regeringen anför att inom den privata sektorn kan en överträdelse av regleringen medföra otillbörliga konkurrensfördelar som snedvrider marknaden. Någon sådan ekonomisk vinning, på bekostnad av andra aktörer på marknaden, kan offentliga verksamhetsutövare inte dra. Regeringen bedömer, i likhet med vad som gäller på andra områden och mot denna bakgrund, att det finns skäl att göra skillnad på offentliga och enskilda verksamhetsutövare i aktuellt avseende.

Med anledning av remissynpunkter på att sanktionsavgifternas storlek enligt den nya lagen och enligt säkerhetsskyddslagen bör harmonieras anför regeringen att utredningen i sitt slutbetänkande föreslog att maximibeloppet enligt säkerhetsskyddslagen, för andra än statliga myndigheter, kommuner och regioner, ska bestämmas till högst till det högsta av 120 000 000 kronor eller 2 procent av verksamhetsutövarens totala globala årsomsättning under föregående räkenskapsår. Förslaget bereds inom Regeringskansliet.

När sanktionsavgiftens storlek bestäms bör, enligt regeringens mening, tillsynsmyndigheten särskilt beakta de omständigheter som ska beaktas vid valet av ingripande. Vilken storlek på sanktionsavgiften som en överträdelse motiverar i det enskilda fallet kommer att avgöras av tillsynsmyndigheten eller, efter överklagande, av en domstol. Belopp i den övre delen av de föreslagna beloppsintervallen bör komma i fråga endast för mycket allvarliga överträdelser. Sanktionsavgiften ska i varje enskilt fall vara effektiv, proportionell och avskräckande i enlighet med direktivet.

Överklagande

Tillsynsmyndighetens beslut enligt lagen ska få överklagas till allmän förvaltningsdomstol. Tillsynsmyndigheten ska vid ett överklagande vara motpart i domstolen. Det ska krävas prövningstillstånd vid överklagande till kammarrätten.

Register för uppgifter om domännamnsregistrering

Regeringen föreslår att det i den nya cybersäkerhetslagen ska införas en skyldighet att föra register över tilldelade domännamn. Skyldigheten gäller dock inte för en domänadministratör som omfattas av lagen (2006:224) om nationella toppdomäner för Sverige på internet (toppdomänlagen). I propositionen lämnas även förslag på bl.a. innehållet i registret. Vidare förslås ändringar i toppdomänlagen med anledning av direktivet.

Ändringar i lagen om elektronisk kommunikation

Regeringen föreslår att vissa bestämmelser i lagen (2022:482) om elektronisk kommunikation ska upphöra att gälla eftersom den nya cybersäkerhetslagen kommer att innehålla motsvarande bestämmelser som kommer att träffa även den i förstnämnda lagen aktuella kretsen. I stället föreslås det införas en hänvisning till den nya cybersäkerhetslagen med upplysning om att det där finns krav som anknyter till lagen. Vidare föreslås vissa följdändringar.

Sekretess

Regeringen föreslår att det ska införas en ny bestämmelse i offentlighets- och sekretesslagen (2009:400) om att sekretess ska gälla för uppgift i en incidentrapport som lämnas enligt den nya lagen och för uppgift om vilka åtgärder som en verksamhetsutövare har vidtagit till följd av incidenten, om det inte står klart att uppgiften kan röjas utan att den rapporterande verksamhetsutövarens framtida verksamhet skadas eller syftet med vidtagen åtgärd motverkas. Sekretessen ska gälla i högst fyrtio år. Rätten att meddela och offentliggöra uppgifter ska inte ha företräde framför den tystnadsplikt som följer av sekretessen.

Regeringen föreslår vidare att det i samma lag ska införas en ny sekretessbrytande bestämmelse som gör det möjligt för Myndigheten för civilt försvar att lämna vidare en uppgift som omfattas av sekretess i det internationella samarbetet och som myndigheten har fått i egenskap av gemensam kontaktpunkt, cyberkrishanteringsmyndighet eller enhet för hantering av it-säkerhetsincidenter enligt den nya lagen, om uppgiften behövs för att den mottagande tillsynsmyndigheten ska kunna fullgöra sitt uppdrag enligt den nya lagen. Det ska också vara möjligt för en tillsynsmyndighet att vidarebefordra en uppgift som omfattas av sekretess i det internationella samarbetet till Myndigheten för civilt försvar, om uppgiften behövs för att den myndigheten ska kunna fullgöra sitt uppdrag enligt den nya lagen.

I den nya lagen föreslås det införas en bestämmelse som upplyser om att den myndighet som regeringen bestämmer ska vara gemensam kontaktpunkt, cyberkrishanteringsmyndighet och enhet för hantering av it-säkerhetsincidenter enligt NIS 2-direktivet.

Ikraftträdande- och övergångsbestämmelser

Regeringen föreslår att den nya lagen och övriga lagändringar ska träda i kraft den 15 januari 2026. Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster ska då upphöra att gälla. För överträdelser som regleras i den nya lagen, men som har skett före ikraftträdandet av den lagen, ska NIS-lagen respektive lagen om elektronisk kommunikation fortfarande gälla.

Konsekvenser

Konsekvenser för cybersäkerheten och samhällsekonomin

Regeringen bedömer att förslagen innebär att cybersäkerheten i samhället stärks och att de samhällsekonomiska effekterna av förslagen är godtagbara.

Ekonomiska konsekvenser för den offentliga sektorn

Regeringen redovisar att ett stort antal remissinstanser anser att det behövs kompletterande analyser av de ekonomiska konsekvenserna av förslagen för den offentliga sektorn och att tillräckliga resurser för genomförandet behöver säkerställas.

Regeringen bedömer att förslagen i propositionen innebär ökade kostnader för tillsynsmyndigheterna. De ökade kostnaderna för dessa myndigheter finansieras genom medel som tillfördes i budgetpropositionen för 2025. Samtliga myndigheter som föreslås ska pekas ut som tillsynsmyndigheter, förutom Finansinspektionen, fick nämligen ökade anslag med sammanlagt 28 000 000 kronor för detta ändamål. I den nya lagen föreslås vidare att det ska införas en bestämmelse som ger tillsynsmyndigheten för en viss del av sektorn digital infrastruktur rätt att ta ut avgifter för sin tillsyn.

Regeringen anför att förslagen även innebär skyldigheter och nya uppgifter för vissa andra statliga myndigheter än tillsynsmyndigheterna. Förslagen innebär förvisso att de statliga myndigheter som omfattas av lagen behöver vidta vissa åtgärder med koppling till deras cybersäkerhet som kan vara kostnadsdrivande. Samtidigt är åtgärderna i stor utsträckning förenliga med relevanta europeiska och internationella standarder på området. Många aktörer arbetar redan aktivt utifrån dessa åtgärder för att förhindra cybersäkerhetsincidenter, medan andra behöver genomföra vissa förändringar för att nå upp till de krav som föreslås gälla. Åtgärderna kan förväntas leda till högre motståndskraft mot cybersäkerhetsincidenter och därmed färre incidenter och i förlängningen mindre kostnader. Effekterna kommer enligt regeringens bedömning sannolikt att uppväga eventuella kostnader. Regeringen konstaterar att förslagen leder till ökade kostnader för lärosäten. Det finansieras genom förslag i budgetpropositionen för 2026 på att berörda

lärosäten tillförs medel för att vidta åtgärder som behövs för att uppfylla kraven. Regeringen bedömer att kostnaderna för övriga berörda myndigheter bör kunna hanteras inom befintliga budgetramar.

Regeringen anför att den kommunala finansieringsprincipen innebär att kommuner och regioner ska kompenseras för statligt beslutade åtgärder som direkt tar sikte på den kommunala verksamheten. Regeringen konstaterar att förslagen i propositionen innebär att kommuner och regioner, liksom andra verksamhetsutövare, bl.a. ska vidta säkerhetsåtgärder och i vissa fall rapportera incidenter. Även om effekten av kraven i den nya lagen i förlängningen kan innebära kostnadsbesparingar för verksamhetsutövarna konstaterar regeringen att förslagen leder till ökade kostnader för kommuner och regioner som kräver finansiering enligt den kommunala finansieringsprincipen. Regeringen föreslår därför i budgetpropositionen för 2026 finansieringen av dessa kostnader.

Regeringen bedömer att förslagen innebär ökade kostnader även för allmänna förvaltningsdomstolar. Kostnaderna bedöms dock rymmas inom domstolarnas befintliga anslagsramar.

Konsekvenser för enskilda

Regeringen redovisar att flera remissinstanser efterfrågar bl.a. en mer gedigen konsekvensanalys vad gäller företagens merkostnader. En annan synpunkt är att konsekvensutredningen inte uppfyller erforderliga krav eftersom det saknas information om vilka företag som berörs och hur de påverkas av regleringen.

Regeringen konstaterar att den föreslagna regleringen kommer att innehålla bestämmelser som innebär att enskilda aktörer behöver uppfylla vissa krav. Regeringen uppskattar, med stöd av beräkningar som har gjorts inom Regeringskansliet, att drygt 1 500 företag i Sverige med sammanlagt runt 500 000 sysselsatta skulle kunna beröras av den nya lagen och tillhörande föreskrifter. I beräkningen ingår företag som har minst 50 personer anställda. Lagen kommer dock i vissa fall att gälla även för verksamhetsutövare som inte behöver uppfylla ett storlekskrav. Vilka företag som träffas av den nya lagen och vilka åtgärder som de ska vidta är i allt väsentligt en följd av direktivets utformning.

Regeringen bedömer att förslagen kan innebära ökade kostnader och administrativa bördor för de företag som kommer att räknas som enskilda verksamhetsutövare. Detta gäller även med beaktande av den omständigheten att förslagen också, som EU-kommissionen bedömer, kan innebära minskade kostnader för hanteringen av cybersäkerhetsincidenter.

I fråga om vilka ökade kostnader och administrativa bördor som regelverket kan innebära för enskilda verksamhetsutövare anför regeringen följande. Skyldigheten att göra en anmälan bör generellt sett ge upphov till mindre kostnader. Det analysarbete som krävs för att bedöma om aktören omfattas av lagen, och om en anmälan därmed ska göras, kommer att underlättas genom stöd och tydlig vägledning från berörda myndigheter. Regeringen bedömer att även kostnader som kan hänföras till skyldigheten att rapportera betydande

incidenter bör bli begränsade. Även om incidenter på cybersäkerhetsområdet är vanligt förekommande bör det generellt sett röra sig om ett begränsat antal fall som ett enskilt företag behöver rapportera, särskilt eftersom det gäller endast betydande incidenter. Inte heller informationsskyldigheten bör innebära någon större kostnad eftersom den gäller enbart vid betydande incidenter och betydande cyberhot. När det gäller kostnader kopplade till tillsynsåtgärder konstaterar regeringen att för viktiga verksamhetsutövare får sådana åtgärder vidtas endast när en tillsynsmyndighet har anledning att anta att regleringen inte följs. Skyldigheten att medverka till tillsynsåtgärder, när sådana väl vidtas, bör inte innebära någon större kostnad för den enskilda verksamhetsutövaren.

Regeringen bedömer att den största kostnaden för enskilda hänför sig till de säkerhetsåtgärder som ska vidtas enligt den nya lagen. Det är tillsynsmyndigheten, eller ytterst en domstol, som avgör vilka åtgärder som en enskild verksamhetsutövare är skyldig att vidta för att uppfylla kraven och det är inte möjligt att göra några uppskattningar som är relevanta för alla verksamhetsutövare. Säkerhetsåtgärderna som ska vidtas ska för varje verksamhetsutövare vara lämpliga och proportionerliga och ska säkerställa en nivå på säkerheten som är lämplig i förhållande till risken. De som föreslås räknas som enskilda verksamhetsutövare bedriver verksamhet inom vitt skilda sektorer och deras verksamheter kan se mycket olika ut. Vidare påverkar nivån av cybersäkerhet som verksamhetsutövaren i dagsläget når upp till behovet av ytterligare åtgärder. Det går enligt regeringen inte att presentera en mer exakt och för samtliga företag relevant uppskattning av kostnaderna kopplade till införandet av den nya lagen, men flera av förslagen bör inte heller innebära några beaktansvärda kostnader. Det kan konstateras att förslagen i allt väsentligt är nödvändiga för att genomföra NIS 2-direktivet i Sverige.

Regeringen bedömer att förslagen är förenliga med näringsfriheten och att förslaget om register för domännamnsregistreringsuppgifter innebär en godtagbar risk för ökat integritetsintrång.

Med anledning av svårigheterna att ge en exakt och för samtliga företag relevant uppskattning av kostnaderna kopplade till införandet av den nya lagen bedömer regeringen att konsekvenserna för företagen bör utvärderas. En sådan utvärdering bör göras tre år efter ikraftträdandet av den nya lagen. I samband med detta bör en översyn av författningarna kopplade till genomförandet av NIS 2-direktivet göras.

Motionerna

I kommittémotion 2025/26:3834 anser Ulf Holm m.fl. (MP) att regeringen bör återkomma med en fördjupad analys av lagens ekonomiska konsekvenser för den offentliga sektorn och säkerställa att det finns tillräcklig finansiering för kommuner och regioner.

I kommittémotion 2025/26:3838 föreslår Mikael Larsson och Niels Paarup-Petersen (båda C) flera tillkännagivanden till regeringen med anledning av regeringens lagförslag. Sålunda föreslås att regeringen bör återkomma med förslag som innebär att

- ledningens ansvar för att cybersäkerheten i en verksamhet lever upp till lagens krav tydliggörs (yrkande 1)
- utformningen av sanktionsavgifterna ses över för att säkerställa att de är rimliga, proportionerliga och förutsägbara (yrkande 2)
- sanktionsnivåerna och tillämpningen mellan cybersäkerhetslagen och säkerhetsskyddslagen harmoniseras (yrkande 3)
- det tydliggörs vilka myndigheter som ansvarar för tillsyn och tillämpning av cybersäkerhetslagen respektive säkerhetsskyddslagen samt att man säkerställer samordning för att undvika överlappande tillsyn (yrkande 4)
- det klargörs vilka företag och aktiviteter som omfattas av lagen för att undvika orimliga krav på mindre företag och organisationer (yrkande 5)
- det införs en nationell mekanism för tillsyn och kunskapsdelning (yrkande 6)
- lagen införs stegvis (yrkande 7).

I kommittémotion 2025/26:3405 av Emma Berginger m.fl. (MP) yrkande 10 begärs ett tillkännagivande om att regeringen ska stärka cybersäkerheten i både offentlig och privat sektor. I yrkande 68 begärs ett tillkännagivande om att Sverige ska verka för att cybersäkerhetssamarbetet på EU-nivå ska utvecklas.

Peter Hultqvist m.fl. (S) anför i kommittémotion 2025/26:3556 yrkande 97 att regeringen bör säkerställa utvecklingen för den svenska cyberpolitiken.

I kommittémotion 2025/26:3652 yrkande 18 begär Aylin Nouri m.fl. (S) ett tillkännagivande om en offensiv politik mot cyberattacker och dataintrång.

Utskottets ställningstagande

Ett starkt skydd för nätverks- och informationssystem som används i samhällsviktig verksamhet, i såväl offentlig som privat regi, är centralt för ett motståndskraftigt samhälle. Eftersom den snabba och omfattande digitala utvecklingen är gränsöverskridande är det nödvändigt med internationellt samarbete, inte minst inom EU, för att åstadkomma en hög nivå av cybersäkerhet. Mot den bakgrunden välkomnar utskottet regeringens höjda ambitionsnivå inom området genom förslaget på genomförande av NIS 2-direktivet.

Utskottet tillstyrker därmed regeringens förslag till cybersäkerhetslag och övriga lagförslag av de skäl som anförs i propositionen.

Vidare bedömer utskottet att motionerna 2025/26:3405 (MP) yrkandena 10 och 68, 2025/26:3556 (S) yrkande 97 och 2025/26:3652 (S) yrkande 18 får anses vara tillgodosedda genom regeringens lagförslag, varför de bör avslås.

Utskottet övergår nu till att behandla motionsyrkanden som innehåller förslag om tillkännagivanden till regeringen i olika frågor som ansluter till lagförslagen.

När det gäller motionsyrkandet om ledningens ansvar för cybersäkerheten i en verksamhet vill utskottet anföra följande. Av NIS 2-direktivets artikel 20 framgår bl.a. att medlemsstaterna ska säkerställa att verksamhetsutövarens ledning godkänner och övervakar genomförandet av de säkerhetsåtgärder som verksamhetsutövaren är skyldig att vidta för att skydda sina nätverks- och informationssystem enligt artikel 21. Syftet är att ledningen ska kunna ställas till svars för eventuella överträdelser. Utskottet har ingen annan uppfattning än regeringen om att det redan följer av annan författning att ledningen i såväl privata som offentliga verksamheter ansvarar för organisationen och förvaltningen av sina respektive verksamheters angelägenheter, inklusive på det sätt som följer av artikel 20. Utskottet instämmer således i regeringens bedömning att detta inte behöver regleras särskilt i cybersäkerhetslagen. Vidare konstaterar utskottet att det i den nya lagen införs möjlighet att vid vissa typer överträdelser av lagens bestämmelser meddela förbud för en befattningshavare att inneha ledningsfunktion. Utskottet avstyrker således motion 2025/26:3838 (C) yrkande 1.

I fråga om sanktionsavgifternas storlek konstaterar utskottet det inte finns utrymme att fastställa lägre maximibelopp för enskilda verksamhetsutövare än de som regeringen föreslår eftersom nivåerna följer av direktivet. Spannet mellan det lägsta möjliga beloppet och det högsta är mycket stort för dessa utövare. Som regeringen anför kommer dock sanktionsavgiften i varje enskilt fall att avgöras av en tillsynsmyndighet eller, efter överklagande, av en domstol som vid sin bedömning ska ta hänsyn till en rad omständigheter, t.ex. hur allvarlig överträdelsen varit. Utskottet menar att detta ger goda förutsättningar för att i varje enskilt fall kunna bestämma avgiften så att den är effektiv, proportionerlig och förebyggande i enlighet med direktivet. Vidare delar utskottet regeringens bedömning att det finns skäl att göra skillnad på maximibeloppet för en enskild verksamhetsutövare och en offentlig sådan, inte

minst då risken för en otillbörlig konkurrensfördel när en privat verksamhetsutövare begår överträdelser inte aktualiseras när överträdelser sker i offentlig verksamhet. När det gäller diskrepansen mellan cybersäkerhetslagens nivåer och de som gäller enligt säkerhetsskyddslagen konstaterar utskottet att det inom Regeringskansliet bereds ett förslag om höjning av maximibeloppet i den sistnämnda lagen. Utskottet ser sammanfattningsvis inte anledning att ta något initiativ i fråga om sanktionsavgifternas storlek och avstyrker således motion 2025/26:3838 (C) yrkandena 2 och 3.

När det gäller yrkande 4 i samma motion om förhållandet mellan cybersäkerhetslagen och säkerhetsskyddsregleringen vill utskottet anföra följande. För det första kan konstateras att cybersäkerhetslagen inte ska gälla för statliga myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen och inte heller för enskilda verksamhetsutövare som enbart bedriver sådan verksamhet eller enbart erbjuder tjänster till en sådan statlig myndighet. Dessa verksamhetsutövare är alltså helt undantagna från cybersäkerhetslagens tillämpningsområde. För andra utövare som till någon del bedriver säkerhetskänslig verksamhet eller erbjuder sådana tjänster kommer den delen av verksamheten att omfattas endast av vissa av kraven i cybersäkerhetslagen. För övriga delar kommer lagen att gälla i dess helhet. Som regeringen konstaterar kommer de två regelverken att gälla parallellt och det kan uppstå en situation då t.ex. en incident både påverkar den säkerhetskänsliga verksamheten och övrig verksamhet, vilket gör att incidenten kan behöva rapporteras enligt båda regelverken. Utskottet tar fasta på regeringens bedömning att det inte finns något utrymme, med tanke på direktivets innehåll och regelverkens olika syften och tillämpningsområden, att t.ex. låta ett av dem vara subsidiärt i förhållande till det andra. Utskottet konstaterar vidare att regeringen avser att i förordning peka ut relevanta myndigheter för cybersäkerhetslagens tillsyn och att motsvarande myndigheter för säkerhetsskyddsregelverket är utpekade sedan tidigare. I fråga om samordning konstaterar utskottet att myndigheter enligt författningar är skyldiga att samverka med varandra för att ta till vara de fördelar som kan vinnas för både enskilda och för staten som helhet. Utskottet ser sammanfattningsvis inget skäl att ta något initiativ med anledning av det aktuella motionsyrkandet, varför det avstyrks.

Med anledning av yrkande 5 i samma motion om klargörande av lagens tillämpningsområde utifrån mindre företags perspektiv konstaterar utskottet för det första att storlekskravet innebär att ett företag omfattas av lagen om det har minst 50 anställda eller en balansomslutning och årsomsättning som överstiger 10 000 000 euro per år. De flesta mindre företag kommer alltså inte att omfattas av lagens bestämmelser. Lagen kommer dock att gälla för vissa verksamhetsutövare även om de inte uppfyller storlekskravet, om de i stället uppfyller vissa andra i lagen definierade kriterier. Vilka de kvalificeringsgrunderna är framgår av lagen. Regeringen är i propositionen tydlig med att en verksamhetsutövare som uppfyller kriterierna för att omfattas av lagen ska omfattas av regelverket i sin helhet, dvs. lagen gäller hela verksamheten och

inte endast den del som faller inom en utpekad sektor. Undantag finns dock enligt ovan för sådan verksamhet som bedriver säkerhetskänslig verksamhet till någon del. Utskottet som därmed inte ser något behov för klargöranden i denna fråga avstyrker motionsyrkandet.

När det gäller yrkande 6 i samma motion om tillsyn och kunskapsdelning konstaterar utskottet att regeringen avser att i förordning peka ut relevanta tillsynsmyndigheter samt den myndighet som enligt NIS-direktivet ska vara gemensam kontaktpunkt, cyberkrishanteringsmyndighet och enhet för hantering av it-säkerhetsincidenter. Den gemensamma kontaktpunkten kommer bl.a. att ha en sambandsfunktion. Som utskottet konstaterat ovan är myndigheter enligt författningar skyldiga att samverka med varandra och utskottet, liksom regeringen, utgår från att samverkan mellan de berörda tillsynsmyndigheterna kommer att fungera väl. Utskottet avstyrker således det aktuella motionsyrkandet.

När det slutligen gäller frågan om konsekvenser av lagens införande vill utskottet först framhålla att medlemsstaterna enligt direktivet skulle ha antagit nationella bestämmelser för att genomföra direktivet senast den 17 oktober 2024. Det är således angeläget att cybersäkerhetslagen kommer på plats och att förslaget antas i sin helhet. Samtidigt konstaterar utskottet att det varit svårt att ange en exakt och för alla företag relevant uppskattning av kostnaderna för genomförandet av lagen. Utskottet välkomnar därför regeringens bedömning om att en utvärdering av konsekvenserna för enskilda företag bör göras tre år efter ikraftträdandet och i samband med det även en översyn av lagstiftningen. Utskottet avstyrker med anledning av detta motion 2025/26:3838 (C) yrkande 7. I fråga om de ekonomiska konsekvenserna för offentliga verksamhetsutövare konstaterar utskottet att regeringen har bedömt att lagförslagen kommer att innebära ökade kostnader för tillsynsmyndigheterna och att detta också har finansierats genom ökade anslag i förra årets budgetproposition. Regeringen har också konstaterat att förslaget innebär ökade kostnader för kommuner och regioner som kräver finansiering enligt den kommunala finansieringsprincipen. Regeringen har därför föreslagit finansiering av dessa kostnader i budgetpropositionen för 2026. Utskottet utgår från att regeringen följer upp att tillskottet är tillräckligt och avstyrker därmed även motion 2025/26:3834 (MP).

Reservationer

1. Finansieringen av den nya lagen, punkt 2 (V, MP)

av Hanna Gunnarsson (V) och Ulf Holm (MP).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 2 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion 2025/26:3834 av Ulf Holm m.fl. (MP).

Ställningstagande

Vi välkomnar propositionen som ett steg för att stärka Sveriges motståndskraft mot cyberhot. I en tid av ökade säkerhetspolitiska spänningar, där hybridhot såsom cyberattacker, sabotage och påverkansoperationer är en del av vardagen, är ett starkt och systematiskt cybersäkerhetsarbete helt avgörande. Vi står därför bakom regeringens förslag till en ny cybersäkerhetslag med nya krav på verksamhetsutövare att vidta åtgärder för att säkra sina informationssystem och rapportera incidenter. Samtidigt vill vi understryka vår oro för finansieringen av den nya lagen. Ett stort antal remissinstanser har påtalat att lagens genomförande riskerar att bli mycket kostsam – särskilt för kommuner och regioner som redan i dag befinner sig i ett ekonomiskt kärvt läge. Även om regeringen aviserat ökade generella statsbidrag inför 2026 för att finansiera genomförandet av lagen, är det osäkert om dessa medel kommer att vara tillräckliga för kommuner och regioner, särskilt med tanke på de många andra krav som åläggs sektorn i totalförsvarsuppbyggnaden. Kommuner och regioner är centrala aktörer i det civila försvaret. Det är därför orimligt att staten inte samtidigt säkerställer att de har ekonomiska förutsättningar att säkra välfärden och fullfölja de uppgifter som följer med totalförsvarsutbyggnaden.

Vi anser att regeringen bör återkomma med en fördjupad analys av de ekonomiska konsekvenserna för den offentliga sektorn och säkerställa tillräcklig finansiering för kommuner och regioner.

2. Ledningens ansvar, punkt 3 (C)

av Kerstin Lundgren (C).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 3 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion 2025/26:3838 av Mikael Larsson och Niels Paarup-Petersen (båda C) yrkande 1.

Ställningstagande

Jag välkomnar att regeringen har lämnat förslag om en ny cybersäkerhetslag. Även om lagen är efterlängtad vill jag framföra ett antal synpunkter. Jag efterlyser mer tydlighet vad gäller ledningens ansvar för att cybersäkerheten i en verksamhet lever upp till lagens krav. Enligt NIS 2-direktivet, som är en av orsakerna till lagen, skulle ledningen inom enskilda verksamheter få ett personligt ansvar för överträdelser av kraven på säkerhetsåtgärder. Detta saknas i cybersäkerhetslagen och har i praktiken ersatts av ett krav på att ledningen ska utbildas. Denna förändring medför kraftigt minskade krav på ledningen i utpekade och för samhället kritiska organisationer.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage det för regeringen.

3. Påverkan på mindre företag och organisationer, punkt 4 (V, C, MP)

av Hanna Gunnarsson (V), Kerstin Lundgren (C) och Ulf Holm (MP).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 4 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion 2025/26:3838 av Mikael Larsson och Niels Paarup-Petersen (båda C) yrkande 5.

Ställningstagande

Flera remissinstanser har påpekat brister i den föreslagna lagen när det gäller vilka företag eller aktiviteter som verkligen kommer att påverkas. För många

aktörer kan den nya lagen tydligt omfatta en del av verksamheten, medan andra delar inte är relevanta. Det bör förtydligas hur lagen ska tolkas och om det endast är de delar av verksamheten som påverkar säkerheten i relevanta tjänster som ska omfattas. Dagens otydlighet kan skapa stora problem för mindre företag och t.ex. inom gröna näringar. Regeringens förändringar på cyberområdet skapar inte optimala förutsättningar för att stärka motståndskraften hos svenska företag och mindre organisationer.

Vi anser att regeringen bör återkomma med klargöranden i dessa frågor för att undvika orimliga krav på mindre företag och organisationer.

4. Övriga frågor om lagstiftningens framtida utformning, punkt 5 (V, C)

av Hanna Gunnarsson (V) och Kerstin Lundgren (C).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 5 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion 2025/26:3838 av Mikael Larsson och Niels Paarup-Petersen (båda C) yrkandena 2–4, 6 och 7.

Ställningstagande

I regeringens förslag till cybersäkerhetslag finns möjlighet att ta ut sanktionsavgifter vid överträdelser. Enligt förslaget kan sanktionsavgiften bestämmas till högst 10 miljoner euro för företag respektive 10 miljoner kronor för offentliga organisationer. Det är en kraftig differens i bötesbelopp som, tillsammans med otydligheten om när sanktioner kan bli aktuella, skapar risk för orimliga skillnader mellan olika organisationsformer. Vi anser att man bör se över sanktionsavgifternas utformning för att säkerställa att de är rimliga, proportionerliga och förutsägbara, särskilt för mindre verksamheter. Vi anser också att lagen missar att harmonisera sanktionsavgifternas storlek mellan cybersäkerhetslagen och säkerhetsskyddslagen, vilket kan skapa ojämlik behandling och osäkerhet. Regeringen bör återkomma till riksdagen med förslag i denna riktning.

Det bör vidare klargöras vilka myndigheter som ansvarar för tillsyn och tillämpning av cybersäkerhetslagen respektive säkerhetsskyddslagen. Vidare bör man säkerställa samordning mellan de båda regelverken för att undvika att flera myndigheter har överlappande tillsyn och att samma typ av överträdelse leder till olika sanktioner beroende på vilket regelverk den hanteras under. Regeringen måste också tydliggöra myndigheters ansvar genom kravställningar i regleringsbrev och instruktioner.

En majoritet av Sveriges företag påpekar att de behöver ökat stöd och information från myndigheter för att skapa den höga nivå av cybersäkerhet vi alla vill se. Denna lag är inget undantag och riskerar att bidra till ökad osäkerhet. Det behövs en nationellt samordnad tillsynsmodell där roller och ansvar förtydligas. Vi anser därför att en nationell koordineringsmekanism för tillsyn och kunskapsdelning bör införas, så att om en myndighet utövat tillsyn över en verksamhet kan andra tillsynsmyndigheter ta del av det.

Finansiering och stöd till mindre aktörer som inte tidigare omfattats av liknande lagstiftning behövs om det ska vara möjligt att leva upp till lagen i tid. Alternativt anser vi att det finns behov av ett stegvis införande av lagen så att mer tid ges till de organisationer som inte har så stora resurser och kompetens. Det är särskilt relevant för mindre företag och organisationer.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

5. Cyberpolitikens utveckling, punkt 6 (S)

av Peter Hultqvist (S), Helén Pettersson (S), Hanna Westerén (S), Erik Ezelius (S) och Markus Selin (S).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 6 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2025/26:3556 av Peter Hultqvist m.fl. (S) yrkande 97.

Ställningstagande

Det svenska cyberförsvaret och vår gemensamma beredskap mot cyberangrepp måste stärkas. I en tid när digitaliseringen genomsyrar hela samhället är det viktigare än någonsin att myndigheter, kommuner och företag bedriver ett systematiskt och ansvarsfullt informationssäkerhetsarbete. Det handlar om att skydda människor, välfärd och samhällsservice. Därför är det av särskild vikt att både it- och cybersäkerheten utvecklas, liksom samhällets förmåga att möta allt mer avancerade och asymmetriska cyberhot.

Vi ser hur cyberangreppen från kriminella aktörer blir fler, samtidigt som angreppen från främmande stater ökar i omfattning och komplexitet. Dessa aktörer har resurser att skada samhällsviktiga funktioner som livsmedelsförsörjning, betalningssystem, elförsörjning och sjukvård, vilket i förlängningen riskerar att slå hårt mot tryggheten i människors vardag. Effekterna av cyberattacker kan i värsta fall bli lika allvarliga som ett konventionellt väpnat angrepp. Därför måste statens ansvar och förmåga inom cybersäkerhet fortsätta att byggas ut och fördjupas.

Utvecklingen inom svensk cyberpolitik visar att viktiga steg redan har tagits. Under den S-ledda regeringen 2020 etablerades Nationellt cybersäkerhetscentrum, Centrum för cyberförsvar och informationssäkerhet vid KTH samt en spetsutbildning inom Försvarsmakten där den första kullen cybersoldater ryckte in. Det är exempel på satsningar som stärker både kompetens och kapacitet, och som måste fortsätta att utvecklas. Cyberangrepp behöver förebyggas, upptäckas och hanteras på ett samordnat och kraftfullt sätt. I dag är cyberförsvar en självklar och integrerad del av det militära försvaret och utgör en militärstrategisk resurs som kan genomföra både offensiva och defensiva operationer. Försvarsmakten har förmåga att upptäcka, identifiera och avvärja hot från de mest kvalificerade aktörerna.

En del av samhällets robusthet handlar också om något så grundläggande som våra betalnings- och kontanthanteringssystem. Här behöver Sverige fortsätta att stärka redundansen. Vi ligger långt fram internationellt när det gäller elektroniska betalningar, men vi har också betydligt färre kontanttransaktioner än många EU-länder. Medan kontanter fortfarande dominerar i flera andra länder blir de alltmer ovanliga här hemma. Det gör det än viktigare att våra betalningssystem är trygga, tillförlitliga och motståndskraftiga och det även i kris.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

BILAGA 1

Förteckning över behandlade förslag

Propositionen

Proposition 2025/26:28 Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag:

1. Riksdagen antar regeringens förslag till cybersäkerhetslag.
2. Riksdagen antar regeringens förslag till lag om ändring i lagen (2006:24) om nationella toppdomäner för Sverige på internet.
3. Riksdagen antar regeringens förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400).
4. Riksdagen antar regeringens förslag till lag om ändring i lagen (2022:482) om elektronisk kommunikation.

Följdmotionerna

2025/26:3834 av Ulf Holm m.fl. (MP):

Riksdagen ställer sig bakom det som anförs i motionen om att regeringen bör återkomma med en fördjupad analys av lagens ekonomiska konsekvenser för offentlig sektor och säkerställa tillräcklig finansiering för kommuner och regioner, och detta tillkännager riksdagen för regeringen.

2025/26:3838 av Mikael Larsson och Niels Paarup-Petersen (båda C):

1. Riksdagen ställer sig bakom det som anförs i motionen om att öka tydligheten i ledningens ansvar för att cybersäkerheten i en verksamhet lever upp till lagens krav och tillkännager detta för regeringen.
2. Riksdagen ställer sig bakom det som anförs i motionen om att se över utformningen av sanktionsavgifterna för att säkerställa att de är rimliga, proportionerliga och förutsägbara och tillkännager detta för regeringen.
3. Riksdagen ställer sig bakom det som anförs i motionen om att regeringen bör återkomma med förslag som harmoniserar sanktionsnivåerna och tillämpningen mellan cybersäkerhetslagen och säkerhetsskyddslagen och tillkännager detta för regeringen.
4. Riksdagen ställer sig bakom det som anförs i motionen om att tydliggöra vilka myndigheter som ansvarar för tillsyn och tillämpning av cybersäkerhetslagen respektive säkerhetsskyddslagen samt säkerställa samordning för att undvika överlappande tillsyn och tillkännager detta för regeringen.

5. Riksdagen ställer sig bakom det som anförs i motionen om klargöranden för att undvika orimliga krav på mindre företag och organisationer och tillkännager detta för regeringen.
6. Riksdagen ställer sig bakom det som anförs i motionen om en nationell mekanism för tillsyn och kunskapsdelning och tillkännager detta för regeringen.
7. Riksdagen ställer sig bakom det som anförs i motionen om behoven av ett stegvis införande av lagen och tillkännager detta för regeringen.

Motioner från allmänna motionstiden 2025/26

2025/26:3405 av Emma Berginger m.fl. (MP):

10. Riksdagen ställer sig bakom det som anförs i motionen om att stärka cybersäkerheten i både offentlig och privat sektor och tillkännager detta för regeringen.
68. Riksdagen ställer sig bakom det som anförs i motionen om att Sverige ska verka för att cybersäkerhetssamarbetet på EU-nivå utvecklas och tillkännager detta för regeringen.

2025/26:3556 av Peter Hultqvist m.fl. (S):

97. Riksdagen ställer sig bakom det som anförs i motionen om att säkerställa utvecklingen för den svenska cyberpolitiken och tillkännager detta för regeringen.

2025/26:3652 av Aylin Nouri m.fl. (S):

18. Riksdagen ställer sig bakom det som anförs i motionen om vikten av en offensiv politik mot cyberattacker och dataintrång och tillkännager detta för regeringen.

BILAGA 2

Regeringens lagförslag

1 Förslag till cybersäkerhetslag

Härigenom föreskrivs[1] 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- och dataöverföringstjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll,

[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. *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.

Säkerhetsåtgärder

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.

Bemyndigande

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 §§.

Förelägganden

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.

2 Förslag till lag om ändring i lagen (2006:24) om nationella toppdomäner för Sverige på internet

Härigenom föreskrivs[1] att 1, 2 och 4–11 §§ lagen (2006:24) om nationella toppdomäner för Sverige på internet[2] ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
1 §	
Denna lag gäller teknisk drift av nationella toppdomäner för Sverige på *Internet* samt tilldelning och registrering av domännamn under dessa toppdomäner.	Denna lag gäller teknisk drift av nationella toppdomäner för Sverige på *internet* samt tilldelning och registrering av domännamn under dessa toppdomäner.
2 §	
I denna lag avses med	
domännamnssystemet: det internationella hierarkiska system som för befordringsändamål på *Internet* används för att tilldela domännamn,	*domännamnssystemet*: det internationella hierarkiska system som för befordringsändamål på *internet* används för att tilldela domännamn,
domän: nivå i domännamnssystemet och del av domännamn,	
domännamn: unikt namn sammansatt av domäner, där en i domännamnssystemet lägre placerad domän står före en domän som är högre placerad i systemet,	
toppdomän: den domän som återfinns sist i ett domännamn,	
nationell toppdomän: toppdomän som betecknar en nation eller en region,	
administration: teknisk drift av en toppdomän samt tilldelning och registrering av domännamn under denna,	
domänadministratör: den som ansvarar för administration av en nationell toppdomän för Sverige,	
namnserver: dator i ett elektroniskt kommunikationsnät som programmerats så att den lagrar och distribuerar information om domännamn samt tar emot och svarar på frågor om domännamn.	
4 §	
En domänadministratör *skall* anmäla sin verksamhet till den myndighet som regeringen bestämmer (tillsynsmyndigheten). Domänadministratören *skall* också till till-	En domänadministratör *ska* anmäla sin verksamhet till den myndighet som regeringen bestämmer (tillsynsmyndigheten). Domänadministratören *ska* också till tillsyns-

[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.
[2] Senaste lydelse av lagens rubrik 2019:184.

synsmyndigheten anmäla om administrationen helt eller delvis uppdras åt annan.	myndigheten anmäla om administrationen helt eller delvis uppdras åt annan.
5 §	
En domänadministratör *skall* bedriva verksamheten på ett säkert och effektivt sätt i allmänhetens intresse. Domänadministratören *skall*	En domänadministratör *ska* bedriva verksamheten på ett säkert och effektivt sätt i allmänhetens intresse. Domänadministratören *ska*
1. lagra tilldelade domännamn och andra uppgifter som är nödvändiga för att stödja den del av domännamnssystemet som toppdomänen omfattar i en databas,	
2. distribuera uppgifterna till namnservrarna för toppdomänen och se till att informationen i dessa är korrekt och lätt tillgänglig,	
3. säkerställa en fungerande trafik mellan namnservrarna och *Internet*,	3. säkerställa en fungerande trafik mellan namnservrarna och *internet*,
4. upprätthålla ett effektivt skydd av uppgifterna i toppdomänen,	
5. ha personal med tillräcklig kompetens och erfarenhet för verksamheten, samt	
6. ha sådana rutiner för verksamheten som uppfyller erkända standarder.	
6 §	
En domänadministratör *skall* föra ett register över tilldelade domännamn under toppdomänen och löpande upprätta säkerhetskopior av registeruppgifterna.	En domänadministratör *ska* föra ett register över tilldelade domännamn under toppdomänen och löpande upprätta säkerhetskopior av registeruppgifterna.
Registret *skall* innehålla	Registret *ska* innehålla
1. domännamnet,	
2. namnet på domännamnsinnehavaren och dennes *postadress,* telefonnummer och *adress för elektronisk post*,	2. namnet på domännamnsinnehavaren och dennes telefonnummer och *e-postadress*,
3. namnet på den som tekniskt administrerar domännamnet och dennes *postadress,* telefonnummer och *adress för elektronisk post*,	3. namnet på den som tekniskt administrerar domännamnet och dennes telefonnummer och *e-postadress*,
4. uppgifter om de namnservrar som är knutna till domännamnet, *samt*	4. uppgifter om de namnservrar som är knutna till domännamnet,
5. övrig teknisk information som behövs för att administrera domännamnet.	5. övrig teknisk information som behövs för att administrera domännamnet*, och*
	6. registreringsdatum.
Uppgifterna i registret *skall* kunna hämtas utan avgift via *Internet*.	Uppgifterna i registret *ska* kunna hämtas utan avgift via *internet. Personuppgifter får dock göras tillgängliga på internet endast om den registrerade har samtyckt till det.*

Personuppgifter får dock göras tillgängliga på detta sätt 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.*

Domänadministratören är personuppgiftsansvarig för behandling av personuppgifter i registret.

7 §

En domänadministratör *skall* fastställa och ge offentlighet åt sina regler för tilldelning, registrering, avregistrering och överföring av domännamn under toppdomänen. Reglerna *skall* utformas så att förfarandet är öppet och icke-diskriminerande, med särskilt beaktande av	En domänadministratör *ska* fastställa och ge offentlighet åt sina regler för tilldelning, registrering, avregistrering och överföring av domännamn under toppdomänen. Reglerna *ska* utformas så att förfarandet är öppet och icke-diskriminerande, med särskilt beaktande av

1. skyddet för den personliga integriteten,
2. användarnas intressen och andra allmänna intressen, samt

3. utvecklingen inom *Internet-området*.	3. utvecklingen inom *internet-området*.
Domänadministratören *skall* tillhandahålla ett effektivt förfarande för lösning av tvister om tilldelning av domännamn.	Domänadministratören *ska* tillhandahålla ett effektivt förfarande för lösning av tvister om tilldelning av domännamn.

8 §

En domänadministratör *skall* se till att uppgifterna i den databas som anges i 5 § 1 och det register som anges i 6 § överförs till tillsynsmyndigheten.	En domänadministratör *ska* se till att uppgifterna i den databas som anges i 5 § 1 och det register som anges i 6 § överförs till tillsynsmyndigheten.

9 §

Regeringen eller, efter regeringens bemyndigande, tillsynsmyndigheten får meddela föreskrifter om

1. på vilket sätt skyldigheter enligt 5 § *skall* fullgöras,	1. på vilket sätt skyldigheter enligt 5 § *ska* fullgöras,

2. register och säkerhetskopior enligt 6 §, samt
3. överföring enligt 8 §.

10 §

Tillsynsmyndigheten *skall* ha tillsyn över efterlevnaden av lagen och av föreskrifter som har meddelats med stöd av lagen.	Tillsynsmyndigheten *ska* ha tillsyn över efterlevnaden av lagen och av föreskrifter som har meddelats med stöd av lagen.

11 §

En domänadministratör *skall* på tillsynsmyndighetens begäran lämna den information och bereda den tillgång till utrustning och annat som behövs för tillsynen.	En domänadministratör *ska* på tillsynsmyndighetens begäran lämna den information och bereda den tillgång till utrustning och annat som behövs för tillsynen.

Tillsynsmyndigheten har rätt att när det behövs för tillsynen få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, där verksamhet som omfattas av denna lag bedrivs.

Denna lag träder i kraft den 15 januari 2026.

3 Förslag till lag om ändring i offentlighets- och sekretesslagen (2009:400)

Härigenom föreskrivs[1] i fråga om offentlighets- och sekretesslagen (2009:400)[2]

dels att nuvarande 18 kap. 8 b och 8 c §§ ska betecknas 18 kap. 8 c och 8 d §§,

dels att 18 kap. 19 § ska ha följande lydelse,

dels att rubrikerna närmast före 18 kap. 8 b och 8 c §§ ska sättas närmast före 18 kap. 8 c respektive 8 d §§,

dels att det ska införas två nya paragrafer, 15 kap. 3 c § och 18 kap. 8 b §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	15 kap.
	3 c §
	Sekretessen enligt 1 a § hindrar inte att Myndigheten för civilt försvar i egenskap av en sådan gemensam kontaktpunkt, cyberkrishanteringsmyndighet eller enhet för hantering av it-säkerhetsincidenter som avses i 1 kap. 17 § cybersäkerhetslagen (2025:000) lämnar en uppgift till en tillsynsmyndighet enligt samma lag, om uppgiften behövs för att tillsynsmyndigheten ska kunna fullgöra sitt uppdrag.
	Sekretessen hindrar inte heller att en sådan tillsynsmyndighet som avses i första stycket lämnar en uppgift till Myndigheten för civilt försvar, om uppgiften behövs för att Myndigheten för civilt försvar ska kunna fullgöra sitt uppdrag som sådan gemensam kontaktpunkt, cyberkrishanteringsmyndighet eller enhet för hantering av it-säkerhetsincidenter som avses i första stycket.

[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.

[2] Senaste lydelse av
18 kap. 8 b § 2019:305
18 kap. 8 c § 2019:305.

En uppgift enligt första eller andra stycket får lämnas endast om intresset av att uppgiften lämnas har företräde framför det intresse som sekretessen ska skydda.

18 kap.

8 b §

Sekretess gäller för uppgift i en incidentrapport enligt cybersäkerhetslagen (2025:000) och för uppgift om vilka åtgärder som en verksamhetsutövare har vidtagit till följd av incidenten, om det inte står klart att uppgiften kan röjas utan att den rapporterande verksamhetsutövarens framtida verksamhet skadas eller syftet med vidtagen åtgärd motverkas.

För uppgift i en allmän handling gäller sekretessen i högst fyrtio år.

19 §[3]

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 b*, 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 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

[3] Senaste lydelse 2024:477.

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.

Denna lag träder i kraft den 15 januari 2026.

4 Förslag till lag om ändring i lagen (2022:482) om elektronisk kommunikation

Härigenom föreskrivs[1] i fråga om lagen (2022:482) om elektronisk kommunikation[2]

dels att 8 kap. 1–4 §§ ska upphöra att gälla,

dels att rubriken närmast före 8 kap. 1 § ska utgå,

dels att nuvarande 8 kap. 5–9 §§ ska betecknas 8 kap. 1–5 §§,

dels att 1 kap. 7 § och 12 kap. 1 § ska ha följande lydelse,

dels att rubrikerna närmast före 8 kap. 5 och 6 §§ ska sättas närmast före 8 kap. 1 respektive 2 §§,

dels att det ska införas en ny paragraf, 1 kap. 4 a §, av följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
	1 kap.
	4 a §
	I cybersäkerhetslagen (2025:000) finns det bestämmelser om säkerhetsåtgärder, säkerhetsrevision, incidentrapportering och informationsskyldighet.
	7 §
I lagen avses med	
abonnent: den som har ingått avtal med en tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster om tillhandahållande av sådana tjänster,	
allmänt elektroniskt kommunikationsnät: ett elektroniskt kommunikationsnät som helt eller huvudsakligen används för att tillhandahålla allmänt tillgängliga elektroniska kommunikationstjänster och som stöder informationsöverföring mellan nätanslutningspunkter,	
användare: den som använder eller efterfrågar en allmänt tillgänglig elektronisk kommunikationstjänst,	
Berec: Organet för europeiska regleringsmyndigheter för elektronisk kommunikation,	
elektronisk kommunikationstjänst: en tjänst som vanligen tillhandahålls mot ersättning via elektroniska kommunikationsnät och som – med undantag för dels tjänster i form av tillhandahållande av innehåll som överförs med hjälp av elektroniska kommunikationsnät och elektroniska kommunikationstjänster, dels tjänster som innebär utövande av redaktionellt ansvar över sådant innehåll – är en	
1. internetanslutningstjänst enligt artikel 2.2 i Europaparlamentets och rådets förordning (EU) 2015/2120 av den 25 november 2015 om åtgärder rörande en öppen internetanslutning och slutkundsavgifter för reglerad	

[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.

[2] Senaste lydelse av 8 kap. 5 § 2022:1086.

kommunikation inom EU och om ändring av direktiv 2002/22/EG och förordning (EU) nr 531/2012,

2. interpersonell kommunikationstjänst, eller

3. tjänst som utgörs helt eller huvudsakligen av överföring av signaler, såsom överföringstjänster som används för tillhandahållande av maskin-till-maskin-tjänster eller för rundradio,

elektroniskt kommunikationsnät: ett system för överföring och i tillämpliga fall utrustning för koppling eller dirigering samt passiva nätdelar och andra resurser som medger överföring av signaler, via tråd eller radiovågor, på optisk väg eller via andra elektromagnetiska överföringsmedier, oberoende av vilken typ av information som överförs,

elektroniskt meddelande: all information som utbyts eller överförs mellan ett begränsat antal parter genom en allmänt tillgänglig elektronisk kommunikationstjänst, utom information som överförs som del av sändningar av ljudradio- och tv-program som är riktade till allmänheten via ett elektroniskt kommunikationsnät om inte denna information kan sättas i samband med den enskilda abonnenten eller användaren av informationen,

harmoniserat frekvensutrymme: ett frekvensutrymme för vilket harmoniserade villkor för användning har fastställts i en teknisk genomförandeåtgärd i enlighet med artikel 4 i Europaparlamentets och rådets beslut nr 676/ 2002/EG av den 7 mars 2002 om ett regelverk för radiospektrumpolitiken i Europeiska gemenskapen (radiospektrumbeslut),

integritetsincident: en händelse som leder till oavsiktlig eller otillåten utplåning, förlust eller ändring eller otillåtet avslöjande av eller otillåten åtkomst till uppgifter som behandlas i samband med tillhandahållandet av allmänt tillgängliga elektroniska kommunikationstjänster,

internetåtkomst: möjlighet till överföring av ip-paket som ger användaren tillgång till internet,

interpersonell kommunikationstjänst: en tjänst som vanligen tillhandahålls mot ersättning och som möjliggör ett direkt interpersonellt och interaktivt informationsutbyte via elektroniska kommunikationsnät mellan ett begränsat antal personer, varigenom de personer som inleder eller deltar i kommunikationen bestämmer vem eller vilka som ska vara mottagare av denna, dock inte en tjänst som möjliggör interpersonell och interaktiv kommunikation enbart som en extrafunktion av mindre betydelse som är direkt kopplad till en annan tjänst,

lokaliseringsuppgift:

1. en uppgift som behandlas i ett allmänt mobilt elektroniskt kommunikationsnät och som anger den geografiska positionen för en slutanvändares terminalutrustning, eller

2. en uppgift i ett allmänt fast elektroniskt kommunikationsnät om nätanslutningspunktens fysiska adress,

meddelandehantering: utbyte eller överföring av ett elektroniskt meddelande som inte är ett samtal och inte heller är information som överförs som en del av sändningar av ljudradio- eller tv-program,

mikroföretag: ett företag som, i enlighet med avdelning I i bilagan till kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag, sysselsätter färre än 10 personer och vars omsättning eller balansomslutning inte överstiger 2 miljoner euro per år,

misslyckad uppringning: en uppringning som kopplas fram utan att nå en mottagare,

nummerbaserad interpersonell kommunikationstjänst: en interpersonell kommunikationstjänst som etablerar en förbindelse till nummer i nationella eller internationella nummerplaner eller som möjliggör kommunikation med sådana nummer,

nummeroberoende interpersonell kommunikationstjänst: en interpersonell kommunikationstjänst som varken etablerar en förbindelse till nummer i nationella eller internationella nummerplaner eller möjliggör kommunikation med sådana nummer,

nätanslutningspunkt: en fysisk punkt vid vilken en slutanvändare ansluts till ett allmänt elektroniskt kommunikationsnät,

nät med mycket hög kapacitet: ett elektroniskt kommunikationsnät som helt består av fiberoptik åtminstone fram till slutanvändarnas lokaler eller en basstation eller ett elektroniskt kommunikationsnät som kan erbjuda liknande nätprestanda under normala högtrafikförhållanden,

nödkommunikation: kommunikation med samhällets alarmeringstjänst genom en interpersonell kommunikationstjänst,

operatör: den som tillhandahåller eller avser att tillhandahålla ett allmänt elektroniskt kommunikationsnät eller en tillhörande facilitet,

operatörslås: sådana begränsningar när det gäller användningen av terminalutrustning som en tillhandahållare har infört eller låtit införa för att hindra att utrustningen används för nyttjande av andra tillhandahållares elektroniska kommunikationstjänster,

radioanläggning: en anordning som möjliggör radiokommunikation eller bestämning av position, hastighet eller andra kännetecken hos ett föremål genom sändning av radiovågor (radiosändare) eller mottagning av radiovågor (radiomottagare),

radiokommunikation: överföring, utsändning eller mottagning av tecken, signaler, skrift, bilder, ljud eller meddelanden av varje slag med hjälp av radiovågor,

radiovågor: elektromagnetiska vågor med frekvenser från 9 kilohertz till 3 000 gigahertz som breder ut sig utan särskilt anordnad ledare,

rent grossistföretag: ett företag som inte bedriver verksamhet på någon slutkundsmarknad, inte är närstående till eller genom ägarintressen kontrollerar ett företag som bedriver verksamhet på någon slutkundsmarknad och inte genom avtal är bundet att exklusivt handla med ett enskilt företag som verkar på någon slutkundsmarknad,

samtal: en förbindelse genom en allmänt tillgänglig interpersonell kommunikationstjänst som möjliggör talkommunikation i båda riktningarna,

samtrafik: fysisk och logisk sammankoppling av allmänna elektroniska kommunikationsnät för att göra det möjligt för användare att kommunicera med varandra eller få tillgång till tjänster som tillhandahålls i näten,

skadlig störning: en störning som äventyrar funktionen hos en radionavigationstjänst eller någon annan säkerhetstjänst eller som på något annat sätt allvarligt försämrar, hindrar eller upprepat avbryter en radiokommunikationstjänst som fungerar i enlighet med gällande bestämmelser, inbegripet störning av befintliga eller planerade tjänster på nationellt tilldelade frekvenser,

slutanvändare: en användare som inte tillhandahåller ett allmänt elektroniskt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst,

små företag: företag som, i enlighet med avdelning I i bilagan till kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag, sysselsätter färre än 50 personer och vars omsättning eller balansomslutning inte överstiger 10 miljoner euro per år,

säkerhet i nät och tjänster: elektroniska kommunikationsnäts och elektroniska kommunikationstjänsters förmåga att vid en viss tillförlitlighetsnivå motstå händelser som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos näten eller tjänsterna, hos lagrade, överförda eller behandlade uppgifter eller hos de närliggande tjänster som erbjuds genom eller är tillgängliga via dessa elektroniska kommunikationsnät eller elektroniska kommunikationstjänster,

säkerhetsincident: en händelse med en faktisk negativ inverkan på tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst, hos lagrade, överförda eller behandlade uppgifter eller hos de närliggande tjänster som erbjuds genom eller är tillgängliga via dessa elektroniska kommunikationsnät eller elektroniska kommunikationstjänster, eller på förmågan att motstå sådana händelser,

talkommunikationstjänst: en allmänt tillgänglig elektronisk kommunikationstjänst som gör det möjligt att ringa och ta emot samtal via ett eller flera nummer inom en nationell eller internationell nummerplan,

telefonitjänst: en elektronisk kommunikationstjänst som innebär en möjlighet att ringa eller ta emot samtal via ett eller flera nummer inom en nationell eller internationell nummerplan,

tillhörande facilitet: en anordning, funktion eller något annat som har samband med ett elektroniskt kommunikationsnät eller en elektronisk kommunikationstjänst och som möjliggör, stöder eller kan stödja tillhandahållande av tjänster via det nätet eller den tjänsten,

trafikuppgift: en uppgift som behandlas i syfte att befordra ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller för att fakturera detta meddelande,

trådlösa accesspunkter med kort räckvidd: små trådlösa nätanslutningsutrustningar med låg effekt och kort räckvidd som kan vara utrustade med en eller flera antenner med låg visuell inverkan och som gör det möjligt för användare att få trådlös tillgång till elektroniska kommunikationsnät oberoende av om den underliggande nättopologin är mobil eller fast,

trådlösa lokala nät: trådlösa kommunikationssystem med låg effekt och kort räckvidd som på icke-exklusiv grund använder ett harmoniserat frekvensutrymme och som har låg risk för störningar på andra sådana system som utnyttjas av andra användare i omedelbar närhet av systemet,

vertikalt integrerad operatör: en operatör som tillhandahåller tjänster till företag som den konkurrerar med på marknader i efterföljande handelsled.

12 kap.

1 §[3]

Tillsynsmyndigheten ska besluta att ta ut en sanktionsavgift av den som

1. inte tillhandahåller en sammanfattning av avtalet i enlighet med 7 kap. 1 §, föreskrifter som har meddelats med stöd av den paragrafen eller genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 102.3 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,

2. inte tillämpar villkor om bindningstid eller uppsägningstid i enlighet med 7 kap. 8, 13 eller 14 §,

3. inte uppfyller kraven på nummerportabilitet i enlighet med 7 kap. 19 och 20 §§ eller föreskrifter om nummerportabilitet som har meddelats med stöd av 7 kap. 21 § första stycket,

4. inte vidtar åtgärder för att hantera risker som hotar säkerheten i nät och tjänster i enlighet med 8 kap. 1 §, föreskrifter som har meddelats med stöd av den paragrafen eller genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,

5. inte rapporterar om säkerhetsincidenter i enlighet med 8 kap. 3 §, föreskrifter som har meddelats med stöd av den paragrafen eller genomförandeakter som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,

6. inte informerar om hot om säkerhetsincidenter i enlighet med 8 kap. 4 §, föreskrifter som har meddelats med stöd av den paragrafen eller genomförandeakter

[3] Senaste lydelse 2022:1086.

som Europeiska kommissionen har meddelat med stöd av artikel 40.5 i direktiv (EU) 2018/1972, i den ursprungliga lydelsen,	
7. inte vidtar skyddsåtgärder i enlighet med 8 kap. 5 § eller föreskrifter som har meddelats med stöd av den paragrafen,	*4.* inte vidtar skyddsåtgärder i enlighet med 8 kap. *1 §* eller föreskrifter som har meddelats med stöd av den paragrafen,
8. inte vidtar åtgärder för att säkerställa skydd av uppgifter som behandlas i samband med tillhandahållandet av en tjänst i enlighet med 8 kap. 6 § eller föreskrifter som har meddelats med stöd av den paragrafen,	*5.* inte vidtar åtgärder för att säkerställa skydd av uppgifter som behandlas i samband med tillhandahållandet av en tjänst i enlighet med 8 kap. *2 §* eller föreskrifter som har meddelats med stöd av den paragrafen,
9. inte informerar abonnenten om särskilda risker för bristande skydd av behandlade uppgifter i enlighet med 8 kap. 7 §,	*6.* inte informerar abonnenten om särskilda risker för bristande skydd av behandlade uppgifter i enlighet med 8 kap. *3 §*,
10. inte underrättar om integritetsincidenter i enlighet med 8 kap. 8 § eller kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott enligt Europaparlamentets och rådets direktiv 2002/58/EG vad gäller personlig integritet och elektronisk kommunikation,	*7.* inte underrättar om integritetsincidenter i enlighet med 8 kap. *4 §* eller kommissionens förordning (EU) nr 611/2013 av den 24 juni 2013 om åtgärder tillämpliga på anmälan av personuppgiftsbrott enligt Europaparlamentets och rådets direktiv 2002/58/EG vad gäller personlig integritet och elektronisk kommunikation,
11. inte behandlar uppgifter i ett elektroniskt meddelande eller trafikuppgifter som hör till detta meddelande i enlighet med 9 kap. 27 §,	*8.* inte behandlar uppgifter i ett elektroniskt meddelande eller trafikuppgifter som hör till detta meddelande i enlighet med 9 kap. 27 §,
12. inte bedriver sin verksamhet så att beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs i enlighet med 9 kap. 29 § första stycket eller föreskrifter som har meddelats i anslutning till det stycket,	*9.* inte bedriver sin verksamhet så att beslut om hemlig avlyssning av elektronisk kommunikation och hemlig övervakning av elektronisk kommunikation kan verkställas och så att verkställandet inte röjs i enlighet med 9 kap. 29 § första stycket eller föreskrifter som har meddelats i anslutning till det stycket,
13. inte ordnar uppgifter och gör dem tillgängliga i ett format som gör att de enkelt kan tas om hand i enlighet med 9 kap. 29 b § andra stycket eller föreskrifter som har meddelats i anslutning till det stycket,	*10.* inte ordnar uppgifter och gör dem tillgängliga i ett format som gör att de enkelt kan tas om hand i enlighet med 9 kap. 29 b § andra stycket eller föreskrifter som har meddelats i anslutning till det stycket,

14. inte överför signaler till samverkanspunkter i enlighet med 9 kap. 30 § eller föreskrifter som har meddelats med stöd av den paragrafen, eller

15. inte lämnar ut en uppgift i enlighet med 9 kap. 33 §.

11. inte överför signaler till samverkanspunkter i enlighet med 9 kap. 30 § eller föreskrifter som har meddelats med stöd av den paragrafen, eller

12. inte lämnar ut en uppgift i enlighet med 9 kap. 33 §.

En sanktionsavgift enligt första stycket 2 ska, när det är fråga om ett paket enligt 7 kap. 26 §, tas ut endast om överträdelsen avser en allmänt tillgänglig elektronisk kommunikationstjänst som inte är en nummeroberoende interpersonell kommunikationstjänst eller en överföringstjänst som används för tillhandahållande av maskin-till-maskintjänster.

---

1. Denna lag träder i kraft den 15 januari 2026.
2. Äldre bestämmelser gäller fortfarande för överträdelser som skett före ikraftträdandet.

Tryck: Elanders Sverige AB, Vällingby 2025