Sammanfattning

Direktivet

Europaparlamentet och rådet antog den 14 december 2022 två nya EU-direktiv, NIS2-direktivet, se bilaga 3 och CER-direktivet. Utredningen redovisar i detta delbetänkande förslag om införlivning av NIS2-direktivet och kommer att i sitt slutbetänkande i september 2024 att lämna förslag om införlivning av CER-direktivet.

NIS2-direktivet ställer krav på säkerhet i nätverks- och informationssystem. Det ersätter det tidigare NIS-direktivet från 2016, som genomfördes i svensk rätt genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Utredningen föreslår att NIS2-direktivet i huvudsak införlivas genom en ny lag, cybersäkerhetslagen och att den tidigare lagen upphävs.

NIS2-direktivet skärper kraven jämfört med det tidigare direktivet för verksamhetsutövare och innehåller bestämmelser om ett mer långtgående samarbete inom unionen. Syftet är att uppnå en högre cybersäkerhet. Det är ett minimidirektiv med innebörd att den svenska lagstiftningen skulle kunna innehålla längre gående skyldigheter. Utredningen föreslår med något undantag inte några skyldigheter utöver vad som följer av direktivet.

Vem omfattas av cybersäkerhetsregleringen?

Det finns två viktiga skillnader mellan gällande lagstiftning och förslaget till cybersäkerhetsreglering. Den första är att cybersäkerhetslagen föreslås omfatta betydligt fler aktörer, eftersom antalet sektorer utökas från sju till 18. Den andra viktiga skillnaden är att kraven kommer att gälla för hela verksamheten inte bara för samhällsviktiga och digitala tjänster.

De sektorer som kommer att omfattas är:

- Energi
- Transporter
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Hälso- och sjukvårdssektorn
- Dricksvatten
- Avloppsvatten
- Digital infrastruktur
- Förvaltning av IKT-tjänster (mellan företag)
- Offentlig förvaltning
- Rymden
- Post- och budtjänster
- Avfallshantering
- Tillverkning, produktion och distribution av kemikalier
- Produktion, bearbetning och distribution av livsmedel
- Tillverkning
- Digitala leverantörer
- Forskning

Innebörden är att den som bedriver verksamhet inom någon av sektorerna som utgångspunkt omfattas av kraven i cybersäkerhetsregleringen. Det gäller för såväl offentliga som enskilda verksamhetsutövare.

Som framgår av uppräkningen av sektorer är offentlig förvaltning en egen sektor. Det får till följd att nästan hela den offentliga sektorn omfattas av lagens krav. Utredningen föreslår att cybersäkerhetslagen ska gälla för de flesta statliga myndigheter i Sverige. De som är undantagna är regeringen, Regeringskansliet, myndigheter som lyder under Riksdagen, och domstolar. Detsamma gäller för sammanlagt

16 myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpning.

Vidare omfattas samtliga regioner och kommuner av lagens krav. Undantag gäller enbart för region- eller kommunfullmäktige. Utredningen föreslår också att lärosäten med examenstillstånd ska omfattas av regleringen.

För enskilda verksamhetsutövare gäller som huvudregel ett storlekskrav med innebörd att verksamheten måste sysselsätta minst 50 personer eller ha en årsomsättning som överstiger 10 miljoner euro för att omfattas av lagen. Det betyder att små företag som utgångspunkt inte kommer att beröras. Vissa särskilt utpekade enskilda verksamhetsutövare omfattas dock oavsett storlek. Myndigheten för samhällsskydd och beredskap (MSB) kommer också att ha möjlighet att peka ut vissa särskilt kritiska mindre verksamheter. Enskilda verksamhetsutövare som enbart bedriver säkerhetskänslig verksamhet, brottsbekämpning eller erbjuder tjänster till myndigheter som gör det, är undantagna.

Därutöver kommer lagen att gälla i begränsad utsträckning för offentliga verksamhetsutövare som bedriver säkerhetskänslig verksamhet eller brottsbekämpning, men där den delen inte utgör en väsentlig andel. Motsvarande kommer att gälla för enskilda verksamhetsutövare som bedriver annan verksamhet tillsammans med säkerhetskänslig verksamhet eller brottsbekämpning. För den säkerhetskänsliga delen av verksamheten eller den delen av verksamheten som avser brottsbekämpning kommer det endast att gälla en anmälnings- och uppgiftsskyldighet. Detsamma gäller för verksamheter som redan omfattas av skyldigheter med motsvarande verkan som kraven i cybersäkerhetslagen. Så kommer vara fallet för exempelvis finansiella verksamhetsutövare som omfattas av Dora-förordningen.

Kraven i direktivet

Den nya regleringen ställer krav på verksamhetsutövarna. En verksamhetsutövare som omfattas av lagen ska anmäla sig till sin tillsynsmyndighet och lämna uppgifter om bland annat identitet, kontaktuppgift och verksamhet.

Därutöver ska verksamhetsutövare vidta riskhanteringsåtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. Åtgärderna ska utgå från en riskanalys, vara proportionella i förhållande till risken och de ska utvärderas. Det ställs också krav på att verksamhetsutövaren ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete samt krav på att verksamhetens ledning ska genomgå utbildning och att anställda ska erbjudas utbildning.

Slutligen gäller en skyldighet för verksamhetsutövare att rapportera betydande incidenter till MSB i egenskap av CSIRT-enhet (se nedan) inom bestämda tidsgränser. Det betyder att en varning ska lämnas inom 24 timmar efter det att verksamhetsutövaren fått kännedom om den betydande incidenten. Vidare ska en incidentanmälan göras inom 72 timmar och en slutrapport inom en månad.

De uppgifter verksamhetsutövarna lämnar till sin tillsynsmyndighet ovan ska myndigheten använda för att klassificera verksamhetsutövarna som väsentliga eller viktiga och registrera dem.

Det ska också finnas ett särskilt register för gränsöverskridande verksamhetsutövare. Registret ska sedan vidarebefordras till MSB i egenskap av gemensam kontaktpunkt (se nedan) som i sin tur ska informera kommissionen.

Tillsyn

I kommittédirektivet anges att systemet för tillsyn bör utgå från den struktur som finns enligt dagens regelverk. Enligt den nu gällande NIS-lagen finns det för varje sektor och för de digitala tjänster som omfattas av lagen en utpekad tillsynsmyndighet som utövar tillsyn över att regelverket följs. Utredningen föreslår att det även fortsatt ska finnas en tillsynsmyndighet för varje sektor. I de sektorer som är oförändrade i förhållande till det första NIS-direktivet är utredningens förslag att befintliga tillsynsmyndigheter fortsätter att ansvara för dessa. Den kompetens som finns hos befintliga tillsynsmyndigheter bör så långt möjligt även nyttjas för de nya sektorer som omfattas av reglering. Flera tillsynsmyndigheter föreslås därför få utökade ansvarsområden. Utredningen föreslår också fem nya tillsynsmyndigheter. Dessa är länsstyrelserna i Stockholms, Skåne, Västra Götalands och Norrbottens län samt Läkemedelsverket.

Tillsynsmyndigheten ska utöva tillsyn över att cybersäkerhetslagen och föreskrifter som meddelats i anslutning till lagen följs. Tillsynsåtgärder för viktiga verksamhetsutövare får vidtas endast när tillsynsmyndigheten har befogad anledning att anta att regleringen inte följs.

Verksamhetsutövarna ska tillhandahålla tillsynsmyndigheten den information som behövs för tillsynen. Tillsynsmyndigheten får om det finns särskilda skäl ålägga en verksamhetsutövare att på egen bekostnad låta ett oberoende organ utföra en riktad säkerhetsrevision och att redovisa resultatet för tillsynsmyndigheten. Tillsynsmyndigheten får också låta genomföra säkerhetsskanningar hos verksamhetsutövare som omfattas av cybersäkerhetslagen.

MSB ska även fortsättningsvis leda ett samarbetsforum där tillsynsmyndigheterna ingår. Syftet med forumet ska vara att underlätta samordning och åstadkomma en effektiv och likvärdig tillsyn.

Gemensam kontaktpunkt, CSIRT-enhet och cyberkrishanteringsmyndighet

För att säkerställa gränsöverskridande samarbete ska varje medlemsstat utse en gemensam kontaktpunkt. Den gemensamma kontaktpunkten ska utöva en sambandsfunktion och bland annat lämna sammanfattande rapporter om betydande incidenter, cyberhot och tillbud till Enisa samt underrätta kommissionen och samarbetsgruppen om antalet verksamhetsutövare i Sverige.

Mot bakgrund av att MSB i dag fullgör de uppgifter som följer av att vara gemensam kontaktpunkt samt myndighetens uppgift att stödja och samordna arbetet med samhällets informationssäkerhet anser utredningen att MSB även fortsatt ska vara gemensam kontaktpunkt i Sverige.

Varje medlemsstat ska också utse eller inrätta en eller flera CSIRT-enheter (Computer Security Incident Response Team). CSIRT-enheten ska bland annat övervaka och analysera cyberhot, sårbarheter och incidenter på nationell nivå och tillhandahålla varningar och information. Vidare ska varje medlemsstat utse eller inrätta en eller flera myndigheter med ansvar för hanteringen av storskaliga cybersäkerhetsincidenter och kriser (cyberkrishanteringsmyndigheter).

Mot bakgrund av de uppdrag MSB har i dag och den kompetens som finns inom myndigheten bedömer utredningen att MSB även fortsatt ska vara CSIRT-enhet samt vara cyberkrishanteringsmyndighet i Sverige.

Varje medlemsstat ska anta en nationell plan för hanteringen av storskaliga cybersäkerhetsincidenter och kriser. Planen ska bland annat innehålla cyberkrishanteringsmyndighetens uppgifter och ansvarsområden. Utformningen av den nationella planen ingår inte i utredningens uppdrag.

Ingripanden och sanktioner

Nuvarande ingripanden och sanktioner

Enligt NIS-lagen får en tillsynsmyndighet ingripa mot överträdelser av vissa skyldigheter i lagen. Tillsynsmyndighetens möjligheter att ingripa beror på vilken skyldighet som har överträtts, men består av förelägganden som kan förenas med vite, eller sanktionsavgifter. Sanktionsavgifterna ska bestämmas till lägst 5 000 kronor och högst 10 000 000 kronor. Tillsynsmyndigheten ska ta särskild hänsyn till vissa omständigheter vid bestämmandet av sanktionsavgiftens storlek.

De nuvarande ingripandena och sanktionerna behålls och kompletteras

Tillsynsmyndighetens möjligheter att besluta om förelägganden (vid vite) och sanktionsavgifter behålls. Tillsynsmyndigheten ska även kunna förelägga en verksamhetsutövare att (1) offentliggöra information om överträdelser av lagens bestämmelser, och att (2) informera användare som kan påverkas av ett betydande cyberhot.

Vidare föreslås tillsynsmyndigheten få ansöka hos allmän förvaltningsdomstol om att en person med ledningsansvar hos en väsentlig verksamhetsutövare ska förbjudas att utöva ledningsfunktioner där. Det krävs särskilda omständigheter för att sådant förbud ska kunna meddelas.

Anmärkning införs som sanktion och ska alltid beslutas vid överträdelser om ingen annan sanktion har använts av tillsynsmyndigheten.

Sanktionsavgifternas maximinivå ska höjas

Lägstanivåerna för sanktionsavgifter behålls på 5 000 kronor. Högstanivåerna höjs väsentligt i jämförelse med gällande nivåer och uppgår:

För väsentliga verksamhetsutövare till det högsta av:

1. Två procent av den väsentliga verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. 10 000 000 euro.

För viktiga verksamhetsutövare till det högsta av:

1. 1,4 procent av verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. 7 000 000 euro.

För offentliga verksamhetsutövare till 10 000 000 kronor.

Tillsynsmyndigheten ska ingripa mot alla överträdelser och beakta fler omständigheter vid val och utformning av sanktioner

Utredningen föreslår att tillsynsmyndigheten ska ingripa mot alla överträdelser av lagen. Den ska i vissa särskilda fall ha möjlighet att avstå från att ingripa, till exempel för att inte bryta mot det s.k. dubbelprövningsförbudet.

Om tillsynsmyndigheten inte avstår från att ingripa ska den åtminstone meddela en anmärkning. Om den ingriper med någon annan sanktion behöver den inte meddela anmärkning.

När tillsynsmyndigheten ingriper ska den alltid beakta alla relevanta omständigheter, men fler omständigheter görs obligatoriska att beakta än vad som tidigare gällt.

Ekonomiska konsekvenser

Utredningens förslag medför ekonomiska konsekvenser för tillsynsmyndigheterna, MSB och verksamhetsutövarna. För tillsynsmyndigheterna handlar det om att betydligt fler verksamhetsutövare kommer att omfattas av lagen. Tillsynsmyndigheterna är enligt utredningens

förslag elva. Sex av dem bedriver redan tillsyn enligt gällande lagstiftning, men fem myndigheter är som framgår ovan nya. Utredningen har som underlag för konsekvensanalysen inhämtat en rapport från Sweco Aktiebolag, som intervjuat de föreslagna tillsynsmyndigheterna och MSB. Av rapporten följer att det varit förenat med svårigheter för myndigheterna att uppskatta de framtida kostnaderna.

Utredningen föreslår att de tillsynsmyndigheter som redan bedriver tillsyn med undantag av Finansinspektionen får ett förstärkt anslag med två miljoner kronor vardera för 2025 avseende löpande kostnader. Skälet är att tillsynsmyndigheterna bör ha utökade resurser för att kunna identifiera vilka verksamhetsutövare som omfattas av den nya lagen, utfärda nya föreskrifter och nya vägledningar utan att samtidigt behöva minska ambitionen med tillsyn. Även MSB bör tillföras motsvarande belopp. De myndigheter som inte redan har tillsynsuppdrag bör få ett förstärkt anslag med fem miljoner kronor vardera för 2025 för att bygga upp tillsynsverksamheten.

Samtidigt föreslår utredningen att regeringen ger Statskontoret i uppdrag att vidare utreda de ekonomiska konsekvenserna för tillsynsmyndigheterna och MSB samt att det för de första åren införs ett återrapporteringskrav för myndigheterna.

För de offentliga verksamhetsutövarna föreslår utredningen att kostnaderna ska finansieras inom befintlig ram. Skälen är att det är rimligt att offentliga verksamhetsutövare vidtar grundläggande säkerhetsåtgärder. Genom förslagen erhåller verksamhetsutövarna också stöd. Vidare kan åtgärder för att förebygga incidenter medföra besparingar.

Förslagen medför även kostnader för enskilda verksamhetsutövare, men även dessa får stöd genom förslagen och det förebyggande arbetet kan medföra besparingar. Som framgått omfattas som huvudregel inte små företag. Kraven kommer att gälla inom hela unionen. Utredningen bedömer därför att regleringen inte får effekter av betydelse för företags arbetsförutsättningar, konkurrensförmåga eller villkor i övrigt.

Ikraftträdande

Utredningen föreslår att förslagen ska träda i kraft den 1 januari 2025.

Summary

Terms of reference

On 14 December 2022, the European Parliament and the Council adopted two new EU Directives: the Directive on measures for a high common level of cybersecurity across the Union (NIS 2) – see Annex 3 – and the Critical Entities Resilience Directive (CER). The Inquiry has outlined the proposals on incorporating the NIS 2 Directive in this interim report and will present proposals on incorporating the CER Directive in its final report in September 2024.

The NIS 2 Directive sets out requirements on network and information systems (NIS) security. It replaces the previous NIS Directive of 2016, which was implemented in Swedish law through the Act on information security for essential and digital services (2018:1174) (NIS Act). The Inquiry proposes implementing the NIS 2 Directive primarily through a new cyber security act that would replace the existing Act.

The NIS 2 Directive sets out stricter requirements on operators than those in the previous directive, and contains provisions on farther-reaching cooperation within the Union. The aim is to achieve a higher level of cybersecurity. This is a minimum directive, which means that Swedish legislation could contain more extensive obligations. With a few exceptions, the Inquiry does not propose any obligations beyond those set out in the Directive.

Who would be covered by the proposed regulation of cybersecurity?

There are two important differences between the current legislation and the proposed regulation of cybersecurity. Firstly, it is proposed that the cybersecurity act cover significantly more actors, as the number of sectors would be expanded from 7 to 18. Secondly, the requirements would apply to their entire operations rather than only essential and digital services.

The following sectors should be covered:

- energy
- transport
- banking
- financial market infrastructures
- health
- drinking water
- wastewater
- digital infrastructure
- Information and communication technology (ICT) service management (business to business)
- public administration
- space
- postal and courier services
- waste management
- chemicals
- food
- manufacturing
- digital services
- research

Under the proposed regulation of cybersecurity, operators carrying out activities in any of these sectors would be subject to the new requirements. This applies to both public and private operators.

As indicated by the list above, public administration would be considered its own sector. Consequently, almost the entire public sector would be subject to the act's requirements. The Inquiry proposes that the cybersecurity act apply to most central government agencies in Sweden. The Government, the Government Offices, government agencies under the Riksdag and the courts would be exempted. The same would apply for the 16 government agencies that primarily carry out security-sensitive activities or law enforcement.

All regions and municipalities would also be subject to the act's requirements. The only exceptions would be regional or municipal councils. The Inquiry further proposes that regulation of cybersecurity cover higher education institutions authorised to award degrees.

As regards private operators, the act's requirements would, as a general rule, apply only to operations that employ at least 50 people or have a minimum annual turnover of EUR 10 million. This means that most small enterprises would not be affected. However, certain specifically identified individual operators would be covered by the act regardless of size. In addition, the Swedish Civil Contingencies Agency would be empowered to identify certain especially critical smaller activities. Individual operators that strictly carry out security-sensitive activities or law enforcement, or offer services to government agencies that do so, would be exempted.

The act would also apply to a limited extent to public sector operators that carry out security-sensitive activities or law enforcement, but only if that part of their activities is not a substantial share of their overall operations. The same would apply to individual operators that carry out other activities together with security-sensitive activities or law enforcement. For the security-sensitive part of the activities or the part concerning law enforcement, only an incident reporting and notification obligation would apply. The same would apply to activities already subject to obligations that have an effect equivalent to that of the requirements of the cybersecurity act. For example, this would be the case for financial operators covered by the Regulation on digital operational resilience for the financial sector.

Requirements in the Directive

The proposed regulation of cybersecurity would set out requirements on operators. An operator covered by the act would have to register with their supervisory authority and provide information including their identity, contact details and activities.

The operator would also have to take risk management measures to protect network and information systems and their physical environments against incidents. These measures would be based on a risk analysis, be proportional to the risk and be subject to evaluation. The operator would also be required to carry out systematic, risk-based information security work, require its management to undergo training and offer training to employees.

Finally, operators would be obliged to report significant incidents to the Swedish Civil Contingencies Agency in its capacity as Computer Security Incident Response Team (CSIRT) (see below) within a specified timeframe. This means that an operator would have to report a warning to the CSIRT within 24 hours of having become aware of a significant incident. Moreover, an incident report would have to be submitted within 72 hours, and a final report within one month.

The information that the operators would be required to submit to their supervisory authority as specified above would be used by the authority to classify the operators as essential or important, and register them. There would also be a separate register for cross-border operators. This register would then be forwarded to the Swedish Civil Contingencies Agency in its capacity as the single point of contact (see below), which would in turn notify the European Commission.

Supervision

The committee terms of reference stipulate that the system for supervision should be based on the existing structure under the current regulatory framework. Under the currently applicable NIS Act, a specific supervisory authority responsible for each sector and for the digital services covered by the Act carries out supervision to ensure compliance with the regulatory framework. The Inquiry proposes that a supervisory authority continue to have responsibility for each

sector. In those sectors where the requirements would remain unchanged in relation to the first NIS Directive, the Inquiry proposes that the currently responsible supervisory authorities continue to have responsibility. The expertise in the current supervisory authorities should be utilised as far as possible for supervision of the additional sectors that would be covered by the proposed regulation. It is therefore proposed that several supervisory authorities gain expanded areas of responsibility. The Inquiry further proposes establishing five new supervisory authorities: the county administrative boards of Stockholm, Skåne, Västra Götaland and Norrbotten, and the Medical Products Agency.

Supervisory authorities should be tasked with carrying out supervision to ensure compliance with the cybersecurity act and regulations announced in connection with it. Supervisory measures against important operators would only be taken if a supervisory authority had reason to believe that the regulation was being not followed.

The operators would have to provide supervisory authorities with the information needed for supervision. If there are special grounds for doing so, a supervisory authority would be empowered to require an operator to arrange and pay for an independent body to conduct a targeted security audit and present the results to the supervisory authority. The supervisory authority would also be empowered to carry out security scans on the premises of operators covered by the cybersecurity act.

The Swedish Civil Contingencies Agency would continue to lead a cooperation forum of supervisory authorities. The purpose of the forum is to facilitate coordination and achieve effective and equivalent supervision.

Single point of contact, CSIRT and cyber crisis management authority

To ensure cross-border cooperation, each Member State must appoint a single point of contact. It is the task of the single point of contact to exercise a liaison function and submit summary reports on significant incidents, cyber threats and near misses to the European Network and Information Security Agency, and notify the Commis-

sion and the Cooperation Group of the number of operators in Sweden.

As it is currently the Swedish Civil Contingencies Agency's mandate to carry out the tasks associated with serving as a single point of contact and to support and coordinate work on society's information security, the Inquiry proposes that the Agency continue to serve as the single point of contact in Sweden.

Each Member State must also designate or establish one or multiple CSIRTs. A CSIRT's mandate includes monitoring and analysing cyber threats, vulnerabilities and incidents at national level, issuing warnings and providing information. Each Member State must also designate or establish one or more authorities with responsibility for the management of large-scale cybersecurity incidents and crises (cyber crisis management authorities).

In consideration of the Swedish Civil Contingencies Agency's current mandate and expertise, the Inquiry proposes that the Agency remain the CSIRT and serve as the cyber crisis management authority in Sweden.

Each Member State must adopt a large-scale national cybersecurity incident and crisis response plan. The plan must outline the tasks and responsibilities of the cyber crisis management authority. The formulation of this national plan is not part of the Inquiry's remit.

Enforcement measures and penalties

Current enforcement measures and penalties

According to the NIS Act, a supervisory authority may intervene against infringements of certain obligations under the Act. Depending on which obligation has been violated, a supervisory authority's enforcement measures consist of issuing orders – possibly in combination with a financial penalty – or administrative fines. The administrative fines should be set at no less than SEK 5 000 and no more than SEK 10 000 000. A supervisory authority should give special consideration to certain circumstances when determining the amount of the administrative fine.

Current enforcement measures and penalties should be retained and supplemented

Supervisory authorities should retain the power to issue orders (as regards financial penalties) and administrative fines. They should also be able to order an operator to (1) announce information about infringements of the act's provisions and (2) inform individuals who are potentially affected by a significant cyber threat.

The Inquiry also proposes empowering supervisory authorities to apply to a general administrative court to prohibit an individual at chief executive officer or legal representative level from exercising managerial functions at an essential operator. Special circumstances would be required to issue such a prohibition.

A reprimand should be introduced as a penalty and always be issued in connection with infringements unless another penalty has been issued by the supervisory authority.

The maximum amount of an administrative fine should be increased

The minimum level of administrative fines should remain at SEK 5 000. The maximum level should be increased substantially in comparison with current levels as follows:
for essential operators, a maximum of

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

for important operators, a maximum of:

1. 1.4 per cent of the operator's entire global turnover of the preceding fiscal year, or
2. EUR 7 000 000; and

for public sector operators, SEK 10 000 000.

A supervisory authority should intervene against all infringements and take account of additional circumstances when determining penalties

The Inquiry proposes that supervisory authorities intervene against all infringements of the act. In certain cases, they should have the option to refrain from intervening, e.g. to avoid double jeopardy situations.

If a supervisory authority does not refrain from intervening, it should, at a minimum, issue a reprimand. If it issues some other penalty, it need not issue a reprimand.

When a supervisory authority intervenes, it should always consider all relevant circumstances. However, it should be obliged to consider more circumstances than is currently the case.

Financial impact

If adopted, the Inquiry's proposals would have a financial impact on the supervisory authorities, the Swedish Civil Contingencies Agency and the operators. This would be due to the new act covering significantly more operators. The Inquiry proposes designating 11 supervisory authorities. Six of these already carry out supervision under currently applicable legislation. The other five authorities mentioned above would be newly empowered. As a basis for its consequence analysis, the Inquiry has examined a report from Sweco Aktiebolag, which interviewed the proposed supervisory authorities and the Swedish Civil Contingencies Agency. The report indicates that it is difficult for those authorities to estimate the future costs.

The Inquiry proposes that the supervisory authorities that already carry out supervision, with the exception of the Swedish Financial Supervisory Authority, each receive an additional SEK 2 million in funding for 2025 to cover running costs. This would provide the supervisory authorities with additional resources, thus enabling them to identify which operators are covered by the new act and issue new regulations and new guidelines without simultaneously diminishing the efficacy of the supervision. The Swedish Civil Contingencies Agency should also be allocated an equivalent amount. The supervisory authorities that do not currently have a supervisory mandate

should each receive an additional SEK 5 million for 2025 to build their supervisory organisation.

At the same time, the Inquiry proposes that the Government instruct the Swedish Agency for Public Management to investigate the financial impact on the supervisory authorities and the Swedish Civil Contingencies Agency, and that the authorities be required to report the financial impact for the first few years.

For public sector operators, the Inquiry proposes financing the costs within existing frameworks. This is because it is reasonable to require public sector operators to take basic security measures. Through these proposals, the operators also receive support. Measures to prevent incidents also result in savings.

The proposals would also entail additional costs for individual operators, but they would also receive support through the proposals, and the preventive work could result in savings. As stated earlier, the act would not cover small enterprises in general. The new requirements will apply throughout the Union. The Inquiry has therefore concluded that the proposed regulation would not have a significant impact on businesses' working conditions, competitiveness or other conditions.

Entry into force

The Inquiry proposes that the proposals enter into force on 1 January 2025.

1 Författningsförslag

1.1 Förslag till lag om cybersäkerhet

Härigenom föreskrivs följande.

1 kap. Inledande bestämmelser

Lagens syfte

1 § Syftet med denna lag är att uppnå en hög cybersäkerhetsnivå.

Uttryck i lagen

2 § I lagen avses med

1. allmän dataskyddsförordning: Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG,

2. allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster: begreppen har samma innebörd som i lagen (2022:482) om elektronisk kommunikation,

3. betrodda tjänster: begreppet har samma innebörd som 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,

4. betydande cyberhot: ett cyberhot som, 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 materiell eller immateriell skada,

5. cyberhot: ett cyberhot enligt definitionen i artikel 2.8 i Cybersäkerhetsakten,

6. cybersäkerhet: cybersäkerhet enligt definitionen i artikel 2.1 i Cybersäkerhetsakten,

7. Cybersäkerhetsakten: Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013,

8. datacentraltjänst: en tjänst som omfattar strukturer, eller grupper av strukturer, avsedda för centraliserad inkvartering, sammankoppling och drift av it- och nätutrustning som tillhandahåller datalagrings-, databehandlings- och dataöverföringstjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll,

9. domännamnsregistreringstjänster: registrar eller en annan verksamhetsutövare som verkar som ombud eller återförsäljare av domännamn,

10. domännamnssystem (DNS): ett hierarkiskt distribuerat namnsystem som möjliggör identifieringen av tjänster och resurser på internet,

11. domännamnssystemtjänster (DNS-tjänster): allmänna rekursiva tjänster för att lösa domännamnsfrågor till internetslutanvändare, eller auktoritativa tjänster för att lösa domännamnsfrågor för användning av tredje part, med undantag för rotnamnsservrar,

12. Dora-förordning: 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,

13. EES: Europeiska ekonomiska samarbetsområdet,

14. enskilda verksamhetsutövare: fysiska och juridiska personer som inte är en myndighet, region eller en kommun och som bedriver verksamhet,

15. forskningsorganisation: en verksamhetsutövare vars främsta mål är att bedriva tillämpad forskning i kommersiellt syfte, men som inte inbegriper utbildningsinstitutioner,

16. hanterade säkerhetstjänster: en verksamhet som utför eller tillhandahåller stöd för annan verksamhet gällande hantering av tjänster som hanterar cybersäkerhetsrisker,

17. hanterade tjänster: en verksamhet som erbjuder tjänster som rör installation, förvaltning, drift eller underhåll av IKT-produkter, IKT-nät, IKT-infrastruktur, IKT-tillämpningar eller andra nätverks- och informationssystem, via bistånd eller aktiv administration antingen i kundernas lokaler eller på distans,

18. IKT-produkt, IKT-tjänst och IKT-process: enligt begreppens definitioner i artiklarna 2.12, 2.13 och 2.14 i Cybersäkerhetsakten,

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

20. kommissionens rekommendation 2003/361/EG: bilagan till kommissionens rekommendation av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag,

21. kvalificerade tillhandahållare av betrodda tjänster: begreppet har samma innebörd som 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,

22. marknadsplatser online: en marknadsplats online enligt definitionen i artikel 2 n i Europaparlamentets och rådets direktiv 2005/29/EG av den 11 maj 2005 om otillbörliga affärsmetoder som tillämpas av näringsidkare gentemot konsumenter på den inre marknaden och om ändring av rådets direktiv 84/450/EEG och Europaparlamentets och rådets direktiv 97/7/EG, 98/27/EG och 2002/65/EG samt Europaparlamentets och rådets förordning (EG) nr 2006/2004 (direktiv om otillbörliga affärsmetoder),

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

24. NIS2-direktivet: Europaparlamentets och rådets direktiv 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,

25. 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.

26. nätverks- och informationssystem:

1. ett elektroniskt kommunikationsnät enligt 1 kap. 7 § lagen (2022:482) om elektronisk kommunikation,

2. 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

3. digitala uppgifter som lagras, behandlas, hämtas eller överförs med sådana hjälpmedel som omfattas av 1 och 2 för att de ska kunna driftas, användas, skyddas och underhållas,

27. partnerföretag och anknutna företag: begreppen har samma innebörd som i artikel 3 i rekommendation 2003/361/EG,

28. plattformar 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, särskilt genom chattar, inlägg, videor och rekommendationer.

29. registreringsenhet för toppdomäner: en verksamhet som har delegerats en specifik toppdomän och som ansvarar för att administrera, förvalta, sköta teknisk drift samt registrering av domännamn under en specifik toppdomän, dock inte om toppdomänen endast avses för eget bruk,

30. risk: risk för förlust eller störning orsakad av en incident, som ska uttryckas som en kombination av omfattningen av förlusten eller störningen och sannolikheten för att en sådan incident inträffar,

31. sökmotor: en sökmotor enligt definitionen 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 online baserade förmedlingstjänster,

32. tillbud: en händelse som kunde ha undergrävt 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, men som framgångsrikt hindrades från att utvecklas eller som inte uppstod,

33. verksamhetsutövare: juridisk eller fysisk person som bedriver verksamhet. Samlingsterm i denna lag för bland annat leverantör, producent, vårdgivare, leverantör eller tillhandahållare.

Lagens tillämpningsområde

Offentliga verksamhetsutövare

3 § Denna lag gäller för

1. statliga myndigheter i Sverige med undantag för regeringen, Regeringskansliet, utlandsmyndigheter, kommittéväsendet, Riksrevisionen, Riksdagens ombudsmän, Sveriges Riksbank, Riksdagsförvaltningen och Sveriges domstolar,
2. regioner i Sverige med undantag för regionfullmäktige, och
3. kommuner i Sverige med undantag för kommunfullmäktige.

Enskilda verksamhetsutövare

4 § Denna lag gäller för enskilda verksamhetsutövare om

1. verksamheten omfattas av bilaga 1 eller 2 i NIS2-direktivet eller är ett lärosäte med examenstillstånd,
2. inte annat följer av 5 och 6 §§, verksamheten är etablerad i Sverige, och
3. inte annat följer av 7 och 8 §§, verksamheten uppfyller kraven för medelstort företag enligt artikel 2 och 3.1–3.3 i bilagan till kommissionens rekommendation 2003/361/EG.

Regeringen eller den myndighet regeringen bestämmer får i föreskrifter meddela undantag för 3 avseende partnerföretag eller anknutna företag som inte i sig uppfyller storlekskravet.

5 § Verksamhetsutövare som erbjuder allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster behöver inte vara etablerade i Sverige för att omfattas av lagen utan det är tillräckligt att verksamhetsutövaren erbjuder tjänster i Sverige.

6 § Gränsöverskridande verksamhetsutövare är verksamhetsutövare som erbjuder:

1. DNS-tjänster,
2. registreringsenheter för toppdomäner,
3. domännamnsregistrering,
4. molntjänster,
5. datacentraltjänster,
6. nätverk för leverans av innehåll,
7. hanterade tjänster,
8. hanterade säkerhetstjänster, eller
9. marknadsplatser online, sökmotorer eller plattformar för sociala nätverkstjänster.

Gränsöverskridande verksamhetsutövare som erbjuder tjänster inom EES, men saknar etablering där ska utse en företrädare med etablering i något av de länder där tjänster erbjuds.

För gränsöverskridande verksamhetsutövare krävs det i stället för etablering att Sverige är huvudsakligt etableringsställe eller att företrädaren är etablerad i Sverige för att verksamhetsutövaren ska omfattas av lagen.

För gränsöverskridande verksamhetsutövare som erbjuder tjänster i Sverige, men inte utser en företrädare gäller kap. 5.

Regeringen får meddela föreskrifter om vad som utgör huvudsakligt etableringsställe.

7 § Verksamhetsutövare som uppfyller kraven i 4 § med undantag för storlekskravet i 3 och som erbjuder allmänna elektroniska kommunikationsnät, allmänt tillgängliga elektroniska kommunikationstjänster, betrodda tjänster, registreringsenhet för toppdomäner, DNS-tjänster eller domännamnsregistrering omfattas av lagen.

8 § Verksamhetsutövare som uppfyller kraven i 4 § med undantag för storlekskravet i 3 omfattas också av lagen om,

1. verksamheten är väsentlig för att upprätthålla kritiska funktioner i samhället och ekonomiska funktioner,
2. en störning kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet, folkhälsa eller medföra betydande systemrisker särskilt om det får gränsöverskridande konsekvenser, eller

3. verksamheten är kritisk på grund av sin särskilda betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer som är beroende av denna verksamhet.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter.

Undantag från lagens tillämpningsområde

Krav i andra författningar

9 § Om annan författning innehåller bestämmelser om krav på riskhanteringsåtgärder eller incidentrapportering för en verksamhetsutövare med motsvarande verkan gäller inte kraven i 3 kap. för verksamhetsutövaren.

Vid jämförelsen av verkan mellan författningarna ska hänsyn tas till bestämmelsernas omfattning samt vilken tillsyn och vilka sanktioner som är kopplade till bestämmelserna.

Regeringen får i föreskrifter ange vilka andra bestämmelser om riskhanteringsåtgärder och incidentrapportering som har motsvarande verkan.

10 § Lagen ska inte tillämpas på verksamheter som undantagits enligt artikel 2.4 i Dora-förordningen.

Sveriges säkerhet eller brottsbekämpning

11 § Lagen gäller inte statliga myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen (2018:585) eller brottsbekämpning.

Regeringen får i föreskrifter ange vilka statliga myndigheter som till övervägande del bedriver säkerhetskänslig verksamhet eller brottsbekämpning.

12 § För andra statliga myndigheter som utövar säkerhetskänslig verksamhet eller brottsbekämpning än de som avses i 11 § gäller inte kraven i 6 § andra och fjärde stycket samt kap. 3 för den del av verksamheten som är säkerhetskänslig eller utgör brottsbekämpning. För den övriga delen av verksamheten gäller lagen i dess helhet.

Vad som anförs i första stycket gäller även regioner och kommuner.

13 § Lagen gäller inte för enskilda verksamhetsutövare som enbart bedriver säkerhetskänslig verksamhet, brottsbekämpning eller som enbart erbjuder tjänster till statliga myndigheter som avses i 11 §.

Om en enskild verksamhetsutövare bedriver även annan verksamhet gäller för den säkerhetskänsliga verksamheten, brottsbekämpningen och verksamheten som avser tjänster till statliga myndigheter enligt 11 § inte kraven i 6 § andra och fjärde stycket samt kap. 3. För den övriga delen av verksamheten gäller lagen i dess helhet.

Vad som anförs ovan i andra stycket gäller inte om verksamhetsutövaren är en tillhandahållare av betrodda tjänster. För dessa verksamhetsutövare gäller lagen i dess helhet.

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

2 kap. Klassificering och registrering

1 § Följande verksamhetsutövare är väsentliga:

1. Statliga myndigheter,

2. verksamhetsutövare som bedriver verksamhet enligt bilaga 1 till NIS2-direktivet, är en kommun eller ett lärosäte med examenstillstånd och vars verksamhet överstiger trösklarna för medelstora företag enligt artikel 2 och 3.1–3 i bilagan till kommissionens rekommendation 2003/361/EG,

3. verksamhetsutövare som erbjuder allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster och vars verksamhet är medelstora företag enligt artikel 2 och 3.1–3 i bilagan till kommissionens rekommendation 2003/361/EG,

4. kvalificerade tillhandahållare av betrodda tjänster,

5. registreringsenheter för toppdomäner,
6. verksamhetsutövare som erbjuder DNS-tjänster och
7. verksamhetsutövare som anges i 1 kap. 8 § och identifierats som väsentliga enligt 33 § förordning om cybersäkerhet.

Verksamhetsutövare som inte är väsentliga är viktiga verksamhetsutövare.

2 § Verksamhetsutövare ska i en anmälan till tillsynsmyndigheten lämna uppgift om identitet, kontaktuppgift, IP-adressintervall, verksamhet och uppgift om i vilka länder verksamheten bedrivs. Gränsöverskridande verksamhetsutövare ska även lämna uppgift om huvudsakligt etableringsställe och i förekommande fall kontaktuppgift till företrädaren.

Ändras uppgifterna ska verksamhetsutövaren anmäla förändringen inom 14 dagar.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om uppgifterna.

3 kap. Riskhanteringsåtgärder och incidentrapportering

1 § Verksamhetsutövaren ska vidta tekniska, driftsrelaterade och organisatoriska riskhanteringsåtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter. Åtgärderna ska utgå från ett allriskperspektiv och en riskanalys och vara proportionella i förhållande till risken. De ska utvärderas och särskilt innefatta följande:

1. Incidenthantering,
2. kontinuitetshantering,
3. säkerhet i leveranskedjan,
4. säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem inklusive hantering av sårbarheter och sårbarhetsinformation,
5. strategier och förfaranden för användning av kryptografi och kryptering,
6. personalsäkerhet,
7. strategier för åtkomstkontroll och tillgångsförvaltning,
8. säkrade lösningar för kommunikation, och
9. lösningar för autentisering.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om riskhanteringsåtgärder.

2 § Verksamhetsutövare ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om systematiskt och riskbaserat informationssäkerhetsarbete.

3 § Ledningen i enskilda och offentliga verksamheter ska genomgå utbildning om riskhanteringsåtgärder och anställda ska erbjudas sådan utbildning.

Regeringen eller den myndighet regeringen bestämmer får meddela föreskrifter om utbildning.

4 § Med betydande incident avses

1. En incident som orsakat eller kan orsaka allvarlig driftsstörning för den erbjudna tjänsten eller ekonomisk skada för den berörda verksamhetsutövaren, eller

2. en incident som har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada.

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

5 § Verksamhetsutövaren ska som en varning underrätta CSIRT-enheten om betydande incidenter inom 24 timmar efter det att verksamhetsutövaren fått kännedom om den. Det ska anges om att det finns misstanke om incidenten orsakats uppsåtligen och om incidenten kan ha gränsöverskridande effekter.

6 § Verksamhetsutövaren ska också inom 72 timmar från tidpunkten från kännedom göra en incidentanmälan till CSIRT-enheten om betydande incidenter. Den ska innehålla en inledande bedömning av hur allvarlig den betydande incidenten är, konsekvenserna av den och förekomsten av angreppsindikatorer. Vidare ska tidigare varning enligt 5 § uppdateras.

För verksamhetsutövare som erbjuder betrodda tjänster ska en incidentanmälan göras inom 24 timmar.

CSIRT-enheten får begära ytterligare information av verksamhetsutövaren.

Verksamhetsutövaren ska samtidigt även informera kunder som kan antas påverkas av den betydande incidenten. Kunderna ska vid behov informeras om avhjälpande åtgärder. Detsamma gäller betydande cyberhot.

7 § Verksamhetsutövaren ska inom en månad från incidentanmälan i 5 § lämna en slutrapport till CSIRT-enheten. Om incidenten fortfarande är pågående ska i stället en lägesrapport lämnas som ska kompletteras med en slutrapport en månad efter det att incidenten har hanterats. Slutrapporten eller lägesrapporten ska innehålla en beskrivning av

1. Incidenten och dess konsekvenser,
2. hur allvarlig incidenten bedöms vara,
3. vad som sannolikt utlöst incidenten,
4. åtgärderna för att begränsa incidenten, och
5. incidentens möjliga gränsöverskridande effekter.

8 § Regeringen eller den myndigheten regeringen bestämmer får meddela föreskrifter om incidentrapporteringen enligt 5–7 §§.

4 kap. Tillsyn

Tillsynsmyndighet

1 § Den myndighet som regeringen bestämmer ska vara tillsynsmyndighet.

Tillsynsmyndighetens uppdrag

2 § Tillsynsmyndigheten ska utöva tillsyn över att denna lag och föreskrifter som har meddelats i anslutning till lagen följs.

3 § Tillsynsåtgärder för viktiga verksamhetsutövare får vidtas endast när tillsynsmyndigheten har befogad anledning att anta att denna lag eller föreskrifter som meddelats i anslutning till lagen inte följs.

Tillsynsmyndighetens undersökningsbefogenheter

4 § Den som står under tillsyn ska på begäran tillhandahålla tillsynsmyndigheten den information som behövs för tillsyn.

5 § Tillsynsmyndigheten har i den omfattning det behövs för tillsynen rätt att få tillträde till områden, lokaler och andra utrymmen, dock inte bostäder, som används i verksamheten.

6 § Tillsynsmyndigheten får förelägga den som står under tillsyn att tillhandahålla information och ge tillträde enligt 4 och 5 §§.

Ett sådant föreläggande får förenas med vite.

7 § Tillsynsmyndigheten får begära handräckning av Kronofogdemyndigheten för att genomföra de åtgärder som avses i 4 och 5 §§. Vid handräckning gäller bestämmelserna i utsökningsbalken om verkställighet av förpliktelser som inte avser betalningsskyldighet, avhysning eller avlägsnande.

Säkerhetsrevision

8 § Tillsynsmyndigheten får om det finns särskilda skäl ålägga en verksamhetsutövare att på egen bekostnad låta ett oberoende organ utföra en riktad säkerhetsrevision och att redovisa resultatet för tillsynsmyndigheten.

Tillsynsmyndigheten får även anlita ett oberoende organ för att utföra regelbundna säkerhetsrevisioner av väsentliga verksamhetsutövare.

Regeringen får meddela föreskrifter om säkerhetsrevisioner.

Säkerhetsskanning

9 § Tillsynsmyndigheten får låta genomföra säkerhetsskanningar hos verksamhetsutövare som omfattas av denna lag.

En säkerhetsskanning ska ske i samarbete med verksamhetsutövaren.

5 kap. Ingripanden och sanktioner

Inledande bestämmelser

1 § Tillsynsmyndigheten ska ingripa om en verksamhetsutövare har åsidosatt sina skyldigheter enligt denna lag, eller föreskrifter som har meddelats med stöd av bestämmelserna om

1. skyldighet att utse företrädare enligt 1 kap. 6 §,
2. anmälningsskyldighet enligt 2 kap. 2 §,
3. riskhanteringsåtgärder enligt 3 kap. 1 §,
4. utbildning enligt 3 kap. 3 §, eller
5. incidentrapportering enligt 3 kap. 5–7 §§.

2 § Ingripanden sker genom att tillsynsmyndigheten

1. meddelar föreläggande enligt 6 §,
2. ansöker om förbud att utöva ledningsfunktion enligt 7 §, eller
3. meddelar sanktionsavgift enligt 11 §.

Om tillsynsmyndigheten inte finner skäl att ingripa enligt första stycket ska den i stället meddela verksamhetsutövaren en anmärkning.

Tillsynsmyndigheten får avstå från att ingripa enligt första och andra stycket om någon annan tillsynsmyndighet har vidtagit åtgärder mot verksamhetsutövaren eller den fysiska personen med anledning av överträdelsen, och tillsynsmyndigheten bedömer att dessa åtgärder är tillräckliga.

Omständigheter som ska beaktas vid ett ingripande

3 § Vid val och utformning av ingripandeåtgärder enligt 2 § ska hänsyn tas till hur allvarlig överträdelsen är, hur länge den har pågått, samt den skada eller risk för skada som uppstått till följd av överträdelsen.

Vid bedömningen ska särskilt beaktas

1. de åtgärder verksamhetsutövaren vidtagit för att förhindra eller minska skadan,
2. verksamhetsutövarens samarbete med tillsynsmyndigheten,
3. om överträdelsen begåtts med uppsåt eller oaktsamhet, och
4. den ekonomiska fördel som verksamhetsutövaren fått till följd av överträdelsen.

4 § Utöver vad som anges i 3 § ska det beaktas som försvårande om verksamhetsutövaren tidigare har begått en överträdelse.

I förmildrande riktning ska beaktas om verksamhetsutövaren har följt godkända uppförandekoder eller godkända certifieringsmekanismer.

5 § En överträdelse ska betraktas som allvarlig om verksamhetsutövaren

1. har begått upprepade överträdelser,
2. inte har rapporterat eller avhjälpt en betydande incident,
3. inte har följt ett tidigare föreläggande från en tillsynsmyndighet,
4. har hindrat säkerhetsrevisioner eller tillsynsåtgärder som tillsynsmyndigheten beslutat om, eller
5. har lämnat oriktiga uppgifter avseende riskhanteringsåtgärder eller rapporteringsskyldigheter enligt 3 kap. 1 eller 5–7 §§.

Förelägganden

6 § Tillsynsmyndigheten får meddela de förelägganden som behövs för att verksamhetsutövare ska uppfylla skyldigheterna som följer av 1 §.

Förelägganden enligt denna paragraf får förenas med vite.

7 § Tillsynsmyndigheten får förelägga en verksamhetsutövare att offentliggöra information på det sätt som tillsynsmyndigheten beslutar rörande överträdelser av denna lag och föreskrifter som har meddelats med stöd av lagen.

Tillsynsmyndigheten får förelägga en verksamhetsutövare att informera de användare som kan påverkas av ett betydande cyberhot om hotet och vilka skydds- eller motåtgärder de kan vidta.

Förelägganden enligt denna paragraf får förenas med vite.

Förbud att utöva ledningsfunktion

8 § Om ett föreläggande enligt 6 § inte följts får tillsynsmyndigheten ingripa mot en person som ingår i verksamhetsutövarens ledning. Ingripande sker genom att tillsynsmyndigheten ansöker hos

allmän förvaltningsdomstol om att en person inte ska få vara befattningshavare hos en viss verksamhetsutövare (förbud).

Ett sådant ingripande får riktas mot den som är befattningshavare enligt 3 § andra stycket lagen (2014:836) om näringsförbud.

Ett ingripande får endast göras om överträdelsen som ligger till grund för föreläggandet är allvarlig och om personen i fråga uppsåtligen eller av grov oaktsamhet orsakat överträdelsen.

9 § Ett beslut om förbud enligt 8 § fattas av förvaltningsrätten på ansökan från tillsynsmyndigheten. En ansökan ska innehålla uppgifter om

1. den person som ansökan avser,
2. verksamhetsutövaren,
3. överträdelsen och de omständigheter som behövs för att kännetecknа den, och
4. de bestämmelser som är tillämpliga på överträdelsen.

Ett förbud ska tidsbegränsas till lägst ett år och högst tre år och ska upphävas omedelbart när föreläggandet har följts.

Förbud får inte riktas mot offentliga verksamhetsutövare.

Ansökan ska prövas skyndsamt av domstolen.

10 § Ett beslut om förbud ska upphävas om det inte längre finns förutsättningar för förbudet.

11 § Förvaltningsrätten ska pröva om ett beslutat förbud ska upphävas om tillsynsmyndigheten eller den enskilde begär det, eller om det annars finns skäl för det. Den enskilde ska upplysas om sin rätt att begära att ett förbud ska upphävas.

Om tillsynsmyndigheten bedömer att det inte längre finns förutsättningar för förbudet ska den omedelbart begära att förvaltningsrätten ska upphäva förbudet.

Sanktionsavgift

12 § Tillsynsmyndigheten får besluta att en verksamhetsutövare ska betala en sanktionsavgift till följd av en överträdelse enligt 1 §.

Sanktionsavgiftens storlek

13 § Sanktionsavgiften ska för väsentliga verksamhetsutövare bestämmas till lägst 5 000 kr och högst till det högsta av:

1. Två procent av den väsentliga verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. 10 000 000 euro.

14 § Sanktionsavgiften ska för viktiga verksamhetsutövare bestämmas till lägst 5 000 kr och högst till det högsta av:

1. 1,4 procent av verksamhetsutövarens totala globala årsomsättning närmast föregående räkenskapsår, eller
2. 7 000 000 euro.

15 § Sanktionsavgiften ska för offentliga verksamhetsutövare bestämmas till lägst 5 000 kr och högst 10 000 000 kr.

Hur sanktionsavgiften ska bestämmas

16 § När sanktionsavgiftens storlek bestäms ska tillsynsmyndigheten särskilt beakta de omständigheter som följer av 3–5 §§.

Hinder mot att ta ut sanktionsavgift

17 § 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.

En sanktionsavgift får inte heller beslutas för samma överträdelse som lett till att verksamhetsutövaren har påförts en sanktionsavgift enligt Allmänna dataskyddsförordningen.

Betalning, verkställighet och preskription

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

Beslut om sanktionsavgift ska delges.

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

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

Sanktionsavgift tillfaller staten.

20 § En beslutad sanktionsavgift ska falla bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

Förordnande om att beslut ska gälla omedelbart

21 § Tillsynsmyndigheten får bestämma att ett beslut om föreläggande enligt denna lag ska gälla omedelbart.

6 kap. Överklagande

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

Prövningstillstånd krävs vid överklagande till kammarrätten.

---

1. Denna lag träder i kraft den 1 januari 2025.

2. Genom lagen upphävs lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Lagen ska dock fortfarande gälla för överträdelser som har skett före ikraftträdandet.

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

Härigenom föreskrivs att rubriken till lag (2006:24) om nationella toppdomäner för Sverige på internet samt 1, 2 och 6 §§ ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*
Lag om *nationella* toppdomäner *för Sverige* på internet	**Lag om toppdomäner på internet**
1 §	
Denna lag gäller teknisk drift av *nationella* toppdomäner *för* Sverige på *I*nternet *samt* tilldelning och registrering av domännamn under dessa toppdomäner.	Denna lag gäller teknisk drift av toppdomäner *med huvudsakligt etableringsställe i* Sverige på *i*nternet. *Vidare omfattar lagen* 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,	
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*,	domänadministratör: den som ansvarar för administration av en toppdomän,

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.

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,	
3. namnet på den som tekniskt administrerar domännamnet och dennes postadress, telefonnummer och adress för elektronisk post,	
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 *I*nternet.	Uppgifterna i registret *ska* kunna hämtas utan avgift via *i*nternet. *Därutöver ska uppgifter även på begäran lämnas ut skyndsamt till myndigheter och andra med offentligrättsliga uppgifter inom EES.*
Personuppgifter får *dock* göras tillgängliga på *detta sätt endast* om den registrerade har samtyckt till det.	Personuppgifter får *endast* göras tillgängliga på *internet* om den registrerade har samtyckt till det.

Domänadministratören är personuppgiftsansvarig för behandling av personuppgifter i registret.

Denna lag träder i kraft den 1 januari 2025.

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

Härigenom föreskrivs i fråga om lagen (2022:482) om elektronisk kommunikation

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

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

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

Nuvarande lydelse	*Föreslagen lydelse*
	12 kap.
	1 §[1]
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	

[1] Senaste lydelse 2023:411.

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 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,

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,

9. inte informerar abonnenten om särskilda risker för bristande skydd av behandlade uppgifter i enlighet med 8 kap. 7 §,

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

4. inte vidtar skyddsåtgärder i enlighet med 8 kap. 5 § 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. 6 § eller föreskrifter som har meddelats med stöd av den paragrafen,

6. inte informerar abonnenten om särskilda risker för bristande skydd av behandlade uppgifter i enlighet med 8 kap. 7 §,

7. 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,

11. 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,

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,

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 §.

integritet och elektronisk kommunikation,

8. inte behandlar uppgifter i ett elektroniskt meddelande eller trafikuppgifter som hör till detta meddelande i enlighet med 9 kap. 27 §,

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,

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,

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-maskin-tjänster.

1. Denna lag träder i kraft den 1 januari 2025.
2. Äldre bestämmelser gäller fortfarande för överträdelser som skett före ikraftträdandet.

1.4 Förslag till förordning om cybersäkerhet

Härigenom föreskrivs följande.

Inledande bestämmelser

1 § Denna förordning kompletterar lagen om cybersäkerhet.

Uttryck i förordningen

2 § Uttryck som används i förordningen har samma innebörd som i lagen om cybersäkerhet.

Huvudsakligt etableringsställe

3 § Vid bedömningen av vad som utgör huvudsakligt etableringsställe enligt 1 kap. 6 § tredje stycket lagen om cybersäkerhet ska följande omständigheter beaktas i angiven rangordning:

1. Plats för beslut om riskhanteringsåtgärder för cybersäkerhet,
2. plats för cybersäkerhetsverksamhet, eller
3. plats där verksamhetsutövaren har flest anställda.

Enskilda verksamhetsutövare

4 § Enskilda verksamhetsutövare får ansöka hos tillsynsmyndighet om att undantas från 1 kap. 4 § första stycket 3 lagen om cybersäkerhet. Myndigheten får meddela ett sådant undantag om verksamheten inte i sig uppfyller storlekskravet i paragrafen, men gör det som partnerföretag eller anknutet företag om ett undantag är skäligt med hänsyn till den lagens syfte.

Verksamhetsutövare som omfattas av krav om cybersäkerhet i andra författningar

5 § I bilaga till denna förordning anges de lagar och andra författningar som innehåller krav på riskhanteringsåtgärder och incidentrapportering med verkan som sammantaget motsvarar skyldigheterna enligt lagen om cybersäkerhet.

Verksamhetsutövare som bedriver säkerhetskänslig verksamhet eller brottsbekämpning till övervägande del

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

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

Tillsynsmyndighet

8 § Följande myndigheter ska vara tillsynsmyndighet enligt lagen om cybersäkerhet och denna förordning för angivna tillsynsområden.

Tillsynsmyndighet	**Sektor**
Statens energimyndighet	Energi
Transportstyrelsen	Transporter
	Tillverkning av motorfordon, släpfordon, påhängsvagnar och andra transportmedel
Finansinspektionen	Bankverksamhet
	Finansmarknadsinfrastruktur

Inspektionen för vård och omsorg	Vårdgivare[1] i Hälso- och sjukvårdssektorn
Läkemedelsverket	Hälso- och sjukvårdssektorn, med undantag för vårdgivare Tillverkning av medicintekniska produkter och medicintekniska produkter för in vitro-diagnostik
Livsmedelsverket	Avloppsvatten Dricksvatten Produktion, bearbetning och distribution av livsmedel
Post- och telestyrelsen	Digital infrastruktur Digitala leverantörer Förvaltning av IKT-tjänster Post- och budtjänster Rymden
Länsstyrelserna i Norrbottens, Skåne, Stockholms och Västra Götalands län	Avfallshantering Forskning Lärosäten med examenstillstånd Offentlig förvaltning Tillverkning, produktion och distribution av kemikalier Tillverkning av datorer, elektronikvaror och optik Tillverkning av elapparatur Tillverkning av övriga maskiner

9 § Länsstyrelsen i Norrbottens län ska vara tillsynsmyndighet för kommuner och regioner som hör till Västernorrlands, Jämtlands, Västerbottens eller Norrbottens län och verksamhetsutövare som har sitt säte i något av dessa län samt Länsstyrelsen i Stockholms län.

10 § Länsstyrelsen i Skåne län ska vara tillsynsmyndighet för kommuner och regioner som hör till Kronobergs, Blekinge, Kalmar eller Skåne län och verksamhetsutövare som har sitt säte i något av dessa län samt Länsstyrelsen i Västra Götalands län.

[1] Vårdgivare enligt definitionen i artikel 3 g i Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård.

11 § Länsstyrelsen i Stockholms län ska vara tillsynsmyndighet för kommuner och regioner som hör till Stockholms, Uppsala, Södermanlands, Västmanlands, Värmlands, Gotlands, Örebro, Dalarnas eller Gävleborgs län och verksamhetsutövare som har sitt säte i något av dessa län samt Länsstyrelsen i Norrbottens län.

12 § Länsstyrelsen i Västra Götalands län ska vara tillsynsmyndighet för kommuner och regioner som hör till Hallands, Jönköpings, Västra Götalands eller Östergötlands län och verksamhetsutövare som har sitt säte i något av dessa län samt Länsstyrelsen i Skåne län.

13 § Om tillsyn över en verksamhetsutövare utövas av fler än en tillsynsmyndighet ska respektive tillsynsmyndighet inte utöva tillsyn gällande den del av verksamheten som anges som en annan tillsynsmyndighets tillsynsområde i 8 §.

Tillsynsmyndighetens uppgifter

14 § Tillsmyndigheten ska upprätta ett register över väsentliga och viktiga verksamhetsutövare. Registret ska ges in till den gemensamma kontaktpunkten senast den 1 mars 2025. Därefter ska det ske en uppdatering och ny rapportering i vart fall vartannat år.

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

Om tillsynsmyndigheten, när den bedriver tillsyn enligt lagen om cybersäkerhet, får kännedom om en omständighet som kan innebära en personuppgiftsincident som ska anmälas enligt den allmänna dataskyddsförordningen ska tillsynsmyndigheten utan onödigt dröjsmål informera Integritetsskyddsmyndigheten.

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

17 § Tillsynsmyndigheten ska samarbeta med och bistå tillsynsmyndigheter i andra medlemsstater inom EES avseende verksamhetsutövare som erbjuder tjänster i mer än en medlemsstat eller erbjuder tjänster i en eller flera medlemsstater och dess nätverks- och informationssystem finns i en eller flera medlemsstater.

18 § Tillsynsmyndigheten får avslå en begäran om bistånd enligt 17 § om myndigheten inte är behörig att tillhandahålla biståndet, om biståndet inte är proportionerligt i förhållande till tillsynsmyndighetens uppgifter eller om begäran avser information eller omfattar verksamhet som om den skulle lämnas ut eller utförs, skulle inverka skadligt på Sveriges säkerhetsintressen, allmänna säkerhet eller försvar.

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

19 § Tillsynsmyndigheten ska lämna stöd till Sveriges representant i den samarbetsgrupp som inrättats enligt artikel 14 i NIS2-direktivet.

Gemensam kontaktpunkt

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

Gemensamma kontaktpunktens uppgifter

21 § Den gemensamma kontaktpunkten ska utöva en sambandsfunktion som säkerställer ett gränsöverskridande samarbete med myndigheter i andra medlemsstater, kommissionen och Enisa samt ett sektorsövergripande samarbete med tillsynsmyndigheterna.

22 § Den gemensamma kontaktpunkten är Sveriges representant i den samarbetsgrupp som inrättats enligt artikel 14 i NIS2-direktivet.

23 § Den gemensamma kontaktpunkten ska på begäran av CSIRT-enheten vidarebefordra incidentrapporter till de gemensamma kontaktpunkterna i andra medlemsstater.

24 § Den gemensamma kontaktpunkten ska var tredje månad lämna in en sammanfattande rapport till Enisa med anonymiserade och aggregerade uppgifter om betydande incidenter, incidenter, cyberhot och tillbud.

25 § Den gemensamma kontaktpunkten ska senast den 17 april 2025 och därefter vartannat år underrätta kommissionen och samarbetsgruppen om antalet väsentliga och viktiga verksamhetsutövare som förtecknats för varje sektor och delsektor.

Den gemensamma kontaktpunkten ska informera kommissionen och samarbetsgruppen om antalet väsentliga och viktiga verksamhetsutövare samt deras verksamhet som identifierats enligt 1 kap. 8 § lagen om cybersäkerhet.

26 § Den gemensamma kontaktpunkten ska upprätta ett särskilt register över gränsöverskridande verksamhetsutövare och ge in det skyndsamt till Enisa. Vidare ska den gemensamma kontaktpunkten löpande underrätta Enisa om uppgifter avseende gränsöverskridande verksamhetsutövare.

CSIRT-enhet

27 § Myndigheten för samhällsskydd och beredskap ska vara CSIRT-enhet.

CSIRT-enhetens uppgifter

28 § När CSIRT-enheten utför sina uppgifter ska den,

1. säkerställa en hög nivå av tillgänglighet för sina kommunikationskanaler,
2. ha lokaler och informationssystem på säkra platser,
3. ha ett ändamålsenligt system för handläggning och dirigering av förfrågningar,
4. vara ständigt tillgänglig och säkerställa att personalen har fått lämplig utbildning,
5. ha redundanta system och reservlokaler för att säkerställa kontinuiteten i tjänsterna, och

6. ha en säker och motståndskraftig kommunikations- och informationsstruktur för utbyte av information med verksamhetsutövare och andra relevanta intressenter.

29 § CSIRT-enheten ska,

1. övervaka och analysera cyberhot, sårbarheter och incidenter på nationell nivå och tillhandahålla varningar och information,
2. erbjuda stöd avseende realtidsövervakning av nätverks- och informationssystem,
3. ta emot incidentrapporter, vidta åtgärder och erbjuda stöd,
4. om en incident kan antas ha sin grund i en brottslig gärning skyndsamt uppmana verksamhetsutövaren att anmäla incidenten till Polismyndigheten,
5. tillgängliggöra informationen i incidentrapporter utan dröjsmål för tillsynsmyndigheten,
6. samla in och analysera forensiska uppgifter,
7. tillhandahålla dynamiska risk- och incidentanalyser samt lägesuppfattning,
8. på begäran av en verksamhetsutövare utföra en proaktiv skanning av den berörda verksamhetsutövarens nätverks- och informationssystem,
9. delta i det nätverk som inrättats enligt artikel 15 i NIS2-direktivet (CSIRT-nätverket),
10. vara samordnare för samordnad delgivning av information om sårbarheter, och
11. upprätta samarbetsförbindelser med relevanta intressenter inom privat och offentlig sektor samt bidra till samverkan rörande cybersäkerhet.

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

Cyberkrishanteringsmyndighet

31 § Myndigheten för samhällsskydd och beredskap ska vara cyberkrishanteringsmyndighet.

32 § Myndigheten för samhällsskydd och beredskap ska delta i det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe).

Rätt att meddela föreskrifter

33 § Myndigheten för samhällsskydd och beredskap får i föreskrifter ange vilka verksamhetsutövare som omfattas av 1 kap. 8 § lagen om cybersäkerhet och om verksamhetsutövaren är väsentlig. Tillsynsmyndigheten ska ges tillfälle att yttra sig.

34 § Myndigheten för samhällsskydd och beredskap får meddela föreskrifter om anmälningsskyldigheten i 2 kap. 2 § lagen om cybersäkerhet.

35 § Tillsynsmyndigheten får meddela föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning enligt 3 kap. 1–3 §§ lagen om cybersäkerhet. Myndigheten för samhällsskydd och beredskap ska ges tillfälle att yttra sig.

För sektorn offentlig förvaltning och lärosäten med examenstillstånd får Myndigheten för samhällsskydd och beredskap i stället för länsstyrelserna i 8 § meddela föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning enligt 3 kap. 1–3 §§ lagen om cybersäkerhet.

36 § Myndigheten för samhällsskydd och beredskap får meddela föreskrifter om vad som utgör en betydande incident enligt 3 kap. 4 § och om incidentrapportering enligt 3 kap. 5–7 §§ lagen om cybersäkerhet. Tillsynsmyndigheten ska ges tillfälle att yttra sig.

Samarbetsforum för effektiv och likvärdig tillsyn

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

Begäran om information

38 § När tillsynsmyndigheten begär information enligt 4 kap. 4 § lagen om cybersäkerhet ska myndigheten ange syftet med begäran och precisera vilken information som krävs.

Säkerhetsrevision

39 § Ett beslut om riktad säkerhetsrevision enligt 4 kap. 8 § lagen om cybersäkerhet ska baseras på riskbedömningar som utförts av tillsynsmyndigheten, verksamhetsutövaren eller på annan tillgänglig riskrelaterad information.

Beslut om förbud

40 § När ett beslut enligt 5 kap. 8 § lagen om cybersäkerhet har fått laga kraft ska domstolen underrätta Bolagsverket och verksamhetsutövaren om beslutet och dess innehåll. Om verksamhetsutövaren är en stiftelse ska den länsstyrelse som är registreringsmyndighet för stiftelsen underrättas i stället för Bolagsverket.

Domstolen ska skicka motsvarande underrättelser om ett sådant förbud upphävs.

41 § När Bolagsverket eller en länsstyrelse som är registreringsmyndighet har fått en underrättelse enligt 40 § ska de avregistrera personen som befattningshavare hos verksamhetsutövaren i det aktuella registret.

Bolagsverket eller en länsstyrelse som är registreringsmyndighet ska säkerställa att personen inte registreras på nytt som befattningshavare hos verksamhetsutövaren under förbudstiden.

---

1. Denna förordning träder i kraft den 1 januari 2025.

2. Genom förordningen upphävs förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster. Förordningen ska dock fortfarande gälla för överträdelser som har skett före ikraftträdandet.

Bilaga

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.

1.5 Förslag till förordning om ändring i förordningen (2007:951) med instruktion för Post- och telestyrelsen

Härigenom föreskrivs i fråga om förordningen (2007:951) med instruktion för Post- och telestyrelsen att 4 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

4 §[1]

Post- och telestyrelsen har till uppgift att

1. främja tillgången till säkra och effektiva elektroniska kommunikationer, inbegripet att se till att samhällsomfattande tjänster finns tillgängliga, och att främja tillgången till ett brett urval av elektroniska kommunikationstjänster,

2. främja utbyggnaden av och följa tillgången till bredband och mobiltäckning i alla delar av landet, inbegripet att skapa förutsättningar för samverkan mellan myndigheter som kan bidra till utbyggnaden av bredband,

3. svara för att möjligheterna till radiokommunikation och andra användningar av radiovågor utnyttjas effektivt,

4. svara för att nummer ur nationella nummerplaner utnyttjas på ett effektivt sätt,

5. främja en effektiv konkurrens,

6. övervaka pris- och tjänsteutvecklingen,

7. bedriva informationsverksamhet riktad till konsumenter,

8. följa utvecklingen när det gäller säkerhet vid elektronisk kommunikation och uppkomsten av eventuella miljö- och hälsorisker,

9. pröva frågor om tillstånd och skyldigheter, fastställa och analysera marknader samt utöva tillsyn och pröva tvister enligt lagen (2022:482) om elektronisk kommunikation,

10. meddela föreskrifter enligt förordningen (2022:511) om elektronisk kommunikation,

11. upprätta och offentliggöra planer för frekvensfördelning till ledning för radioanvändningen samt offentliggöra information av allmänt intresse om rättigheter, villkor, förfaranden och avgifter som rör radiospektrumanvändningen,

[1] Senaste lydelse 2022:531.

12. tillhandahålla information om frekvensanvändning till Europeiska radiokommunikationskontorets frekvensinformationssystem (EFIS),

13. vara marknadskontrollmyndighet enligt radioutrustningslagen (2016:392),

14. vara tillsynsmyndighet enligt lagen (2016:561) med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering och ge stöd och information till myndigheter och enskilda när det gäller betrodda tjänster,

15. följa utvecklingen när det gäller toppdomäner med geografiska namn som har anknytning till Sverige,

16. vara tillsynsmyndighet enligt lagen (2006:24) om nationella toppdomäner för Sverige på internet samt meddela föreskrifter enligt förordningen (2006:25) om nationella toppdomäner för Sverige på internet,

17. verka för robusta elektroniska kommunikationer och minska risken för störningar, inbegripet att upphandla förstärkningsåtgärder, och verka för ökad krishanteringsförmåga,

18. verka för ökad nät- och informationssäkerhet i fråga om elektronisk kommunikation, genom samverkan med myndigheter som har särskilda uppgifter inom informationssäkerhets-, säkerhetsskydds- och integritetsskyddsområdet samt med andra berörda aktörer,

19. lämna råd och stöd till myndigheter, kommuner och regioner och till företag, organisationer och andra enskilda i frågor om nätsäkerhet,

20. vara tvistlösnings- och tillsynsmyndighet enligt lagen (2016:534) om åtgärder för utbyggnad av bredbandsnät och ansvara för informationstjänsten för utbyggnad av bredbandsnät enligt samma lag, och

21. vara tillsynsmyndighet enligt lagen *(2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.*	21. vara tillsynsmyndighet enligt lagen *(2024:XXX) om cybersäkerhet.*

Denna förordning träder i kraft den 1 januari 2025.

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

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

Nuvarande lydelse

Bilaga[1]

Verksamheten består i	Särskilda begränsningar i sekretessen
153. tillsyn enligt *lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster*	

Föreslagen lydelse

Bilaga

Verksamheten består i	Särskilda begränsningar i sekretessen
153. tillsyn enligt *lagen (2025:000) om cybersäkerhet*	*Gäller ej beslut i ärenden*

Denna förordning träder i kraft den 1 januari 2025.

[1] Senaste lydelse 2023:742.

1.7 Förslag till förordning om ändring i förordningen (2022:511) om elektronisk kommunikation

Härigenom föreskrivs i fråga om förordningen (2022:511) om elektronisk kommunikation

dels att 1 kap. 2 § fjortonde strecksatsen ska upphöra att gälla,

dels att 8 kap. 1 och 5 §§ ska upphöra att gälla,

dels att 1 kap. 2 § femtonde strecksatsen ska ha följande lydelse,

dels att 8 kap. 4 § ska ha följande lydelse.

Nuvarande lydelse	*Föreslagen lydelse*

1 kap.

2 §[1]

– –

Nuvarande lydelse	*Föreslagen lydelse*
8 kap. *4–6 §§* i samma lag i fråga om 8 kap. 4 §,	8 kap. *5 och 6 §§* i samma lag i fråga om 8 kap. 4 §,

– –

8 kap.

4 §[2]

Post- och telestyrelsen får meddela

Nuvarande lydelse	*Föreslagen lydelse*
1. ytterligare föreskrifter om säkerhetsåtgärder enligt 8 kap. 1 § lagen (2022:482) om elektronisk kommunikation	
2. ytterligare föreskrifter om rapportering av säkerhetsincidenter enligt 8 kap. 3 § i samma lag,	
3. ytterligare föreskrifter om information till användare enligt 8 kap. 4 § i samma lag,	
4. ytterligare föreskrifter om skyddsåtgärder enligt 8 kap. 5 § i *samma lag*, och	*1.* ytterligare föreskrifter om skyddsåtgärder enligt 8 kap. 5 § i *lagen (2022:482) om elektronisk kommunikation*, och

[1] Senaste lydelse 2023:583.
[2] Senaste lydelse 2023:583.

5. föreskrifter om skyddsåtgärder enligt 8 kap. 6 § i samma lag.	*2.* föreskrifter om skyddsåtgärder enligt 8 kap. 6 § i samma lag.

1. Denna förordning träder i kraft den 1 januari 2025.
2. Äldre bestämmelser gäller fortfarande för överträdelser som skett före ikraftträdandet.