P7_TA(2014)0244

Hög gemensam nivå av nät- och informationssäkerhet ***I

Europaparlamentets lagstiftningsresolution av den 13 mars 2014 om förslaget till Europaparlamentets och rådets direktiv om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen (COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

(Ordinarie lagstiftningsförfarande: första behandlingen)

Europaparlamentet utfärdar denna resolution

– med beaktande av kommissionens förslag till Europaparlamentet och rådet (COM(2013)0048),

– med beaktande av artiklarna 294.2 och 114 i fördraget om Europeiska unionens funktionssätt, i enlighet med vilka kommissionen har lagt fram sitt förslag för parlamentet (C7-0035/2013),

– med beaktande av artikel 294.3 i fördraget om Europeiska unionens funktionssätt,

– med beaktande av det motiverade yttrande från Sveriges riksdag som lagts fram i enlighet med protokoll nr 2 om tillämpning av subsidiaritets- och proportionalitetsprinciperna, och enligt vilka utkastet till lagstiftningsakt inte är förenligt med subsidiaritetsprincipen,

– med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande av den 22 maj 2013[1],

– med beaktande av sin resolution av den 12 september 2013 om EU:s strategi för it-säkerhet: en öppen, säker och trygg cyberrymd[2],

– med beaktande av artikel 55 i arbetsordningen,

– med beaktande av betänkandet från utskottet för den inre marknaden och konsumentskydd och yttrandena från utskottet för industrifrågor, forskning och energi, utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor och utskottet för utrikesfrågor (A7-0103/2014).

1. Europaparlamentet antar nedanstående ståndpunkt vid första behandlingen.

2. Europaparlamentet uppmanar kommissionen att lägga fram en ny text för parlamentet om den har för avsikt att väsentligt ändra sitt förslag eller ersätta det med ett nytt.

3. Europaparlamentet uppdrar åt talmannen att översända parlamentets ståndpunkt till rådet, kommissionen och de nationella parlamenten.

---

1 EUT C 271, 19.9.2013, s. 133.

2 Antagna texter, P7_TA(2013)0376.

P7_TC1-COD(2013)0027

Europaparlamentet ståndpunkt fastställd vid första behandlingen den 13 mars 2014 inför antagandet av Europaparlamentets och rådets direktiv 2014/.../EU om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela unionen

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA DIREKTIV

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande[1],

i enlighet med det ordinarie lagstiftningsförfarandet, och[2]

---

1 EUT C 271, 19.9.2013, s. 133.

2 Europaparlamentets ståndpunkt av den 13 mars 2014.

av följande skäl:

(1) Nät och informationssystem och nät- och informationstjänster har en viktig roll i samhället. Deras tillförlitlighet och säkerhet är en förutsättning ***för EU-medborgarnas frihet och övergripande säkerhet samt*** för ekonomisk verksamhet och social välfärd och i synnerhet för den inre marknadens funktion. **[Ändr. 1]**

(2) ~~Avsiktliga eller oavsiktliga~~ Säkerhetsincidenter blir allt mer omfattande och vanliga ***och deras inverkan allt kraftigare***, vilket utgör ett allvarligt hot mot nätens och informationssystemens funktion. ***Dessa system kan också bli ett lätt mål för avsiktligt sabotage som går ut på att skada dem eller avbryta driften.*** Sådana incidenter kan hindra genomförandet av ekonomisk verksamhet, generera omfattande finansiella förluster, undergräva användarnas ***och investerares*** förtroende och medföra allvarliga konsekvenser för unionens ekonomi ***samt i slutändan hota EU-medborgarnas välbefinnande och medlemsstaternas förmåga att skydda sig själva och säkerställa säkerheten för kritiska infrastrukturer***. **[Ändr. 2]**

(3) Som ett kommunikationsinstrument utan gränser har de digitala informationssystemen, och i synnerhet internet, en viktig funktion för att främja den gränsöverskridande rörligheten för varor, tjänster och personer. Denna transnationella natur innebär att störningar i en medlemsstat även kan påverka andra medlemsstater och EU som helhet. Nätens och informationssystemens motståndskraft och stabilitet är därför avgörande för en smidigt fungerande inre marknad.

(3a) Eftersom vanliga orsaker till systemfel fortsatt är oavsiktliga, exempelvis naturliga orsaker eller mänskliga misstag, bör infrastrukturen kunna stå emot både avsiktliga och oavsiktliga störningar, och operatörer som driver kritisk infrastruktur bör utforma motståndskraftsbaserade system. **[Ändr. 3]**

(4) En samarbetsmekanism bör inrättas på unionsnivå för att möjliggöra informationsutbyte och samordning av ***förebyggande åtgärder,*** upptäckt och ~~samordnade~~ svarsåtgärder när det gäller nät- och informationssäkerhet. För att denna mekanism ska vara effektiv och inkluderande är det viktigt att alla medlemsstater har en minimikapacitet och en strategi som säkerställer en hög nivå av nät- och informationssäkerhet på det egna territoriet. Minimikrav avseende säkerhet bör också gälla ***åtminstone*** för ~~offentliga förvaltningar och operatörer~~ ***vissa marknadsoperatörer*** av ~~kritisk~~ informationsinfrastrukturer, för att främja en riskhanteringskultur och säkerställa att de allvarligaste incidenterna rapporteras. ***Börsnoterade företag bör uppmuntras att på frivillig basis offentliggöra incidenter i sina redovisningar. Den rättsliga ramen bör baseras på behovet av att skydda medborgarens privatliv och integritet. Nätverket för varningar om hot mot kritisk infrastruktur (Ciwin) bör utvidgas till de marknadsoperatörer som omfattas av detta direktiv.*** **[Ändr. 4]**

(4a) ***Offentliga förvaltningar bör på grund av sitt allmännyttiga uppdrag förvalta och skydda sina egna nätverk och informationssystem med vederbörlig aktsamhet, medan detta direktiv bör vara inriktat på kritisk infrastruktur som är nödvändig för att upprätthålla viktig ekonomisk och samhällelig verksamhet inom områdena energi, transport, bankverksamhet, finansmarknadsinfrastrukturer samt hälso- och sjukvård. Mjukvaruutvecklare och hårdvarutillverkare bör inte omfattas av detta direktiv.*** **[Ändr. 5]**

(4b) ***Samarbete och samordning mellan de relevanta unionsmyndigheterna, den höga representanten/vice ordföranden för kommissionen – med ansvar för den gemensamma utrikes- och säkerhetspolitiken och den gemensamma säkerhets- och försvarspolitiken – och EU:s samordnare för kampen mot terrorism bör säkerställas i fall där incidenter som har en betydande inverkan förefaller uppträda i form av yttre hot och terroristverksamhet.*** **[Ändr. 6]**

(5) Detta direktiv bör tillämpas på alla nät och informationssystem, så att alla relevanta incidenter och risker täcks. De skyldigheter som införs för offentliga förvaltningar och marknadsoperatörer bör dock inte tillämpas på företag som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster enligt Europaparlamentets och rådets direktiv 2002/21/EG[1], som omfattas av de särskilda säkerhets- och integritetskrav som fastställs i artikel 13a i direktivet; direktivet bör inte heller tillämpas på tillhandahållare av betrodda tjänster.

[1] Europaparlamentets och rådets direktiv 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv) (EGT L 108, 24.4.2002, s. 33).

(6) Den befintliga kapaciteten räcker inte för att säkerställa en hög nivå av nät- och informationssäkerhet i unionen. Medlemsstaterna har väldigt olika nivåer av beredskap, vilket leder till fragmenterade angreppssätt i unionen. Resultatet blir olika grad av skydd för konsumenter och företag, vilket undergräver den allmänna nät- och informationssäkerhetsnivån i unionen. Avsaknaden av gemensamma minimikrav för ~~offentliga förvaltningar och~~ marknadsoperatörer gör det i sin tur omöjligt att inrätta en övergripande och effektiv mekanism för samarbete på unionsnivå. ***Universitet och forskningscentrum har en avgörande roll när det gäller att främja forskning, utveckling och innovation på dessa områden, och de bör ges adekvat finansiering.*** **[Ändr. 7]**

(7) Effektiva reaktioner på utmaningarna på nät- och informationssäkerhetsområdet förutsätter därför ett övergripande angreppssätt på unionsnivå, som omfattar en gemensam lägsta nivå för kapacitetsuppbyggnad och planering***, utveckling av tillräcklig kompetens inom it-säkerhet***, utbyte av information och samordning av åtgärder samt gemensamma minimikrav avseende säkerhet ~~för alla berörda marknadsoperatörer och offentliga förvaltningar~~. ***Gemensamma minimistandarder bör tillämpas i enlighet med relevanta rekommendationer från samordningsgrupper för it-säkerhet (Cyber Security Coordination Groups – CSGC).*** **[Ändr. 8]**

(8) Bestämmelserna i detta direktiv bör inte påverka varje enskild medlemsstats möjligheter att vidta de åtgärder som är nödvändiga för att skydda sina väsentliga säkerhetsintressen, för att skydda allmän ordning och säkerhet och för att möjliggöra utredning, upptäckt och åtal av brott. Enligt artikel 346 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget) ska ingen medlemsstat vara skyldig att lämna sådan information vars avslöjande den anser strida mot sina väsentliga säkerhetsintressen. ***Ingen medlemsstat är skyldig att avslöja säkerhetsskyddsklassificerade EU-uppgifter enligt rådets beslut 2011/292/EU[1], information som omfattas av sekretessavtal eller informella sekretessavtal, t.ex. Traffic Light Protocol.*** **[Ändr. 9]**

[1] ***Rådets beslut 2011/292/EU av den 31 mars 2011 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter) (EUT L 141, 27.5.2011, s. 17).***

(9) För att uppnå och bibehålla en gemensam hög säkerhetsnivå för nät och informationssystem bör alla medlemsstater ha en nationell nät- och informationssäkerhetsstrategi där de fastställer de strategiska mål och konkreta politiska åtgärder som ska genomföras. Man bör på nationell nivå ***– på grundval av de minimikrav som anges i detta direktiv och med beaktande av vikten av att respektera och skydda privatlivet och personuppgifter –*** utarbeta planer för samarbete om nät- och informationssäkerhet ~~med~~ ***vilka uppfyller*** grundläggande krav för att uppnå en kapacitet för svarsåtgärder som möjliggör ett effektivt och verkningsfullt samarbete på nationell nivå och unionsnivå vid incidenter. ***Varje medlemsstat bör därför vara skyldig att uppfylla gemensamma standarder för uppgifters format och utbytbarheten av uppgifter som ska utbytas och utvärderas. Medlemsstaterna bör kunna be om stöd från Europeiska byrån för nät- och informationssäkerhet (Enisa) i utvecklingen av sina nationella strategier för nät- och informationssäkerhet, på grundval av en gemensam grundläggande strategisk plan för nät- och informationssäkerhet.***
[Ändr. 10]

(10) För att uppnå ett effektivt genomförande av de bestämmelser som antas i enlighet med detta direktiv bör man i varje medlemsstat inrätta eller utse ett organ med ansvar för samordning av nät- och informationssäkerhetsfrågor som kan fungera som sambandspunkt för det gränsöverskridande samarbetet på unionsnivå. Dessa organ bör förses med de tekniska och finansiella resurser och personalresurser som de behöver för att på ett effektivt sätt kunna utföra de uppgifter som de tilldelas och därmed uppnå detta direktivs mål.

(10a) På grund av skillnaderna i nationella förvaltningsstrukturer och för att skydda befintliga sektorsspecifika arrangemang eller unionens tillsyns- och regleringsmyndigheter och undvika överlappning, bör medlemsstaterna kunna utse mer än en nationell behörig myndighet som ansvarar för att utföra arbetsuppgifter som rör säkerheten i marknadsoperatörernas nät och informationssystem enligt detta direktiv. För att se till att samarbetet och kommunikationen över gränserna fungerar smidigt måste emellertid varje medlemsstat, utan att det påverkar sektorsspecifika regleringsarrangemang, utse endast en nationell gemensam kontaktpunkt som ansvarar för det gränsöverskridande samarbetet på unionsnivå. Om det är nödvändigt på grund av medlemsstatens konstitutionella struktur eller andra bestämmelser bör en medlemsstat kunna utse endast en myndighet som ska utföra den behöriga myndighetens och den gemensamma kontaktpunktens uppgifter. De behöriga myndigheterna och de gemensamma kontaktpunkterna bör vara civila organ som är föremål för fullständig demokratisk kontroll, och de bör inte utföra uppgifter på underrättelse-, brottsbekämpnings- eller försvarsrelaterade områden eller på något sätt vara organisatoriskt kopplade till organ som är verksamma på de områdena. **[Ändr. 11]**

(11) Samtliga medlemsstater ***och marknadsoperatörer*** bör ha både den tekniska och organisatoriska kapacitet som krävs för att ***när som helst*** förebygga, upptäcka, reagera på och begränsa effekterna av incidenter och risker vad gäller nät och informationssystem. ***Säkerhetssystem för offentlig förvaltning bör vara säkra och stå under demokratisk kontroll och granskning. Deras gängse nödvändiga utrustning och kapacitet bör följa gemensamt överenskomna tekniska standarder samt operativa standardförfaranden.*** Välfungerade incidenthanteringsorganisationer ***(Cert)*** som uppfyller grundläggande krav bör därför inrättas i alla medlemsstater för att garantera effektiv och kompatibel kapacitet att hantera incidenter och risker och säkerställa ett effektivt samarbete på unionsnivå. ***Dessa incidenthanteringsorganisationer bör kunna interagera på grundval av gemensamma tekniska standarder och operativa standardförfaranden. Eftersom de befintliga incidenthanteringsorganisationerna har olika karaktär och svarar mot olika behov och aktörer, bör medlemsstaterna garantera att åtminstone en incidenthanteringsorganisation tillhandahåller tjänster till var och en av de sektorer som avses i listan över marknadsoperatörer i detta direktiv. Medlemsstaterna bör säkerställa att incidenthanteringsorganisationerna har tillräckliga medel för att delta i gränsöverskridande samarbete i de befintliga internationella och unionsbaserade samarbetsnätverken.*** **[Ändr. 12]**

(12) På grundval av de betydande framsteg som gjorts inom det europeiska forumet för medlemsstaterna (EFMS) när det gäller att främja diskussioner och utbyten av bästa praxis, inbegripet utarbetandet av principer för ett europeiskt samarbete vid cyberkriser bör medlemsstaterna och kommissionen bilda ett nätverk som för samman dem för kontinuerlig kommunikation och stöder deras samarbete. En sådan säker och effektiv samarbetsmekanism***, om lämpligt inklusive marknadsoperatörers deltagande,*** bör skapa förutsättningar för ett strukturerat och samordnat genomförande av informationsutbyte, upptäckt och svarsåtgärder på unionsnivå. **[Ändr. 13]**

(13) ~~Europeiska byrån för nät- och informationssäkerhet (~~Enisa~~)~~ bör bistå medlemsstaterna och kommissionen genom att tillhandahålla expertis och rådgivning och främja utbyte av bästa praxis. Vid tillämpningen av detta direktiv bör kommissionen ***och medlemsstaterna*** i synnerhet konsultera Enisa. För att medlemsstaterna och kommissionen i rätt tid ska få den information som behövs bör tidiga varningar om incidenter och risker lämnas inom samarbetsnätverket. För att bygga upp kapacitet och kunskap bland medlemsstaterna bör samarbetsnätverket också fungera som ett instrument för utbyte av bästa praxis och bistå sina medlemmar vid kapacitetsuppbyggnad samt leda organiserandet av sakkunnigbedömning och nät- och informationssäkerhetsövningar. **[Ändr. 14]**

(13a) Medlemsstaterna bör vid behov kunna använda eller anpassa befintliga organisationsstrukturer eller strategier vid tillämpningen av bestämmelserna i detta direktiv. **[Ändr. 15]**

(14) En säker infrastruktur bör upprättas för informationsutbyte så att känslig och konfidentiell information kan utbytas inom samarbetsnätverket. ***Befintliga strukturer i unionen bör utnyttjas till fullo i detta syfte.*** Utan att det påverkar medlemsstaternas skyldighet att anmäla incidenter och risker med en unionsdimension till samarbetsnätverket bör medlemsstater inte få tillgång till konfidentiell information från andra medlemsstater förrän de kan visa att deras tekniska och finansiella resurser, personalresurser och kommunikationsinfrastruktur garanterar att de kan delta i nätverket på ett effektivt, verkningsfullt och säkert sätt***, med användning av insynsvänliga metoder***. **[Ändr. 16]**

(15) Eftersom de flesta nät och informationssystem är i privat drift är det mycket viktigt med samarbete mellan offentlig och privat sektor. Marknadsoperatörer bör uppmuntras att upprätta egna informella samarbetsmekanismer för att garantera nät- och informationssäkerheten. De bör också samarbeta med den offentliga sektorn och ***sinsemellan*** utbyta information och bästa praxis ~~i~~***, inklusive ömsesidigt*** utbyte ~~mot~~ ***av relevant information,*** operativt stöd ***och strategiskt analyserad*** information vid incidenter. ***För att effektivt uppmuntra utbyte av information och bästa praxis är det mycket viktigt att se till att marknadsoperatörer som deltar i sådana utbyten inte missgynnas till följd av att de samarbetar. Tillfredsställande skyddsmekanismer behövs för att inte sådant samarbete ska utsätta dessa operatörer för högre efterlevnadsrisk eller nya ansvarsskyldigheter enligt bland annat lagstiftningen om konkurrens, immateriella rättigheter, uppgiftsskydd eller it-brottslighet, och inte heller för ökade operativa risker eller säkerhetsrisker.*** **[Ändr. 17]**

(16) För att säkra öppenhet och insyn och informera ~~EU-medborgare~~ ***unionsmedborgare*** och marknadsoperatörer ordentligt bör de ~~behöriga myndigheterna~~ ***gemensamma kontaktpunkterna*** skapa en gemensam ***unionsomfattande*** webbplats för ~~offentliggörande av~~ ***att offentliggöra*** sådan information om incidenter ~~och~~**,** risker ***och riskreduceringssätt*** som inte är konfidentiell ***och för att vid behov ge råd om lämpliga underhållsåtgärder***. ***Informationen på webbplatsen bör vara tillgänglig oberoende av vilken apparat som används. Offentliggörandet av personuppgifter på denna webbplats bör vara begränsat till vad som är nödvändigt, och uppgifterna bör vara så anonymiserade som möjligt.***
[Ändr. 18]

(17) När information anses konfidentiell enligt unionens bestämmelser och nationella bestämmelser om företagshemlighet bör denna konfidentialitet säkerställas vid genomförande av verksamheter och uppfyllande av mål enligt detta direktiv.

(18) På grundval av i synnerhet de nationella erfarenheterna av krishantering bör kommissionen och medlemsstaterna, i samarbete med Enisa, utarbeta en unionsplan för nät- och informationssäkerhetssamarbete som omfattar samarbetsmekanismer***, bästa praxis och operationsmönster*** för att ***förebygga, upptäcka, rapportera och*** bemöta risker och incidenter. Planen bör vederbörligen beaktas när tidiga varningar görs inom samarbetsnätverket. **[Ändr. 19]**

(19) Anmälan av en tidig varning inom nätverket bör endast krävas när den berörda incidenten eller risken är av sådan omfattning och så allvarlig att den är eller kan bli så betydande att det är nödvändigt med information eller samordning av svarsåtgärderna på unionsnivå. Tidiga varningar bör därför begränsas till ~~faktiska eller potentiella~~ incidenter eller risker som är av snabbt ökande omfattning, som överstiger den nationella beredskapen eller som påverkar mer än en medlemsstat. För att möjliggöra en riktig utvärdering bör all information av relevans för bedömningen av risken eller incidenten meddelas samarbetsnätverket. **[Ändr. 20]**

(20) Vid mottagandet av en tidig varning, och vid sin bedömning av den, bör de ~~behöriga myndigheterna~~ ***gemensamma kontaktpunkterna*** enas om samordnade svarsåtgärder i enlighet med unionens plan för nät- och informationssäkerhetssamarbete. ~~Behöriga myndigheter~~***De gemensamma kontaktpunkterna, Enisa och kommissionen*** bör~~, liksom kommissionen,~~ informeras om de åtgärder som vidtas på nationell nivå till följd av de samordnade svarsåtgärderna. **[Ändr. 21]**

(21) I och med att nät- och informationssäkerhetsproblemen är globala till sin natur behövs ett närmare internationellt samarbete för att förbättra säkerhetsstandarder och informationsutbyten och främja ett gemensamt sätt att hantera nät- och informationssäkerhetsfrågor. ***Varje ram för detta internationella samarbete bör omfattas av bestämmelserna i Europaparlamentets och rådets direktiv 95/46/EG[1] och Europaparlamentets och rådets förordning (EG) nr 45/2001[2].*** **[Ändr. 22]**

---

1 ***Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, 23.11.1995, s. 31).***

2 ***Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EGT L 8, 12.1.2001, s. 1).***

(22) Ansvaret för att garantera nät- och informationssäkerheten vilar i hög grad på ~~offentliga förvaltningar och marknadsoperatörer~~ ***marknadsoperatörerna***. En kultur av riskhantering, ~~som~~ ***nära samarbete och förtroende vilken*** inbegriper riskbedömning och genomförande av säkerhetsåtgärder som är anpassade till riskerna ***och incidenterna, oavsett om det rör sig om avsiktliga eller oavsiktliga sådana***, bör främjas och utvecklas genom ändamålsenliga krav i lagstiftning och frivillig branschpraxis. Lika konkurrensvillkor ***som gäller*** för alla ***på ett tillförlitligt sätt*** krävs också för ett effektivt fungerande samarbetsnätverk som kan säkerställa ett effektivt samarbete från alla medlemsstater. **[Ändr. 23]**

(23) Enligt direktiv 2002/21/EG ska företag som tillhandahåller allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster vidta lämpliga åtgärder för att skydda deras integritet och säkerhet och införa anmälningskrav avseende säkerhetsöverträdelser och integritetsförlust. Enligt Europaparlamentets och rådets direktiv 2002/58/EG [1] ska leverantören av en allmänt tillgänglig elektronisk kommunikationstjänst vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa säkerheten i sina tjänster.

[1] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

(24) Dessa skyldigheter bör utvidgas bortom sektorn för elektronisk kommunikation till ***att omfatta operatörer av infrastruktur vilka är starkt beroende av informations- och kommunikationsteknik och vilka behövs för upprätthållandet av centrala ekonomiska eller samhälleliga funktioner som el och gas, transporter, kreditinstitut, finansmarknadsinfrastrukturer och hälso- och sjukvård. Störningar i dessa nät och informationssystem skulle påverka den inre marknaden. Även om skyldigheterna enligt detta direktiv inte bör utvidgas till att omfatta*** viktiga leverantörer av informationssamhällets tjänster, enligt definitionen i Europaparlamentets och rådets direktiv 98/34/EG [1], som ligger till grund för informationssamhällets tjänster i senare led eller onlineverksamhet, t.ex. e-handelsplattformar, internetbelningsslussar, sociala nät, sökmotorer, molntjänster ***i allmänhet*** och onlineförsäljning av tillämpningar. ~~Störningar i denna typ av informationssamhällestjänster hindrar tillhandahållandet av andra informationssamhällestjänster som är beroende av dem. Programutvecklare och hårdvarutillverkare är inte leverantörer av informationssamhällets tjänster och omfattas därför inte. Dessa skyldigheter bör också utvidgas till att omfatta offentliga förvaltningar och operatörer av kritisk infrastruktur som är starkt beroende av informations- och kommunikationsteknik och som behövs för upprätthållandet av centrala ekonomiska eller samhälleliga funktioner som el och gas, transporter, kreditinstitut, börser och hälso- och sjukvård. Störningar i dessa nät och informationssystem skulle påverka den inre marknaden.~~ ***, kan dessa leverantörer av informationssamhällets tjänster, på frivillig basis och om lämpligt i det specifika fallet enligt deras bedömning, informera den behöriga myndigheten eller den gemensamma kontaktpunkten om incidenter i nätverkssäkerheten***. ***Den behöriga myndigheten eller den gemensamma kontaktpunkten bör, om möjligt, till de marknadsoperatörer som informerat om incidenten lämna strategiskt analyserad information som bidrar till att avhjälpa säkerhetshotet.*** **[Ändr. 24]**

[1] Europaparlamentets och rådets direktiv 98/34/EG av den 22 juni 1998 om ett informationsförfarande beträffande tekniska standarder och föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (EGT L 204, 21.7.1998, s. 37).

(24a) Även om hårdvaru- och mjukvaruleverantörer inte är marknadsoperatörer på samma sätt som de som omfattas av detta direktiv, främjar deras produkter säkerheten för nät och informationssystem. De spelar därför en viktig roll när det gäller att göra det möjligt för marknadsoperatörer att säkra sina nät och informationsinfrastrukturer. Med tanke på att hårdvaru- och mjukvaruprodukter redan omfattas av befintliga regler om produktansvar bör medlemsstaterna se till att de reglerna tillämpas i vederbörlig ordning. **[Ändr. 25]**

(25) Tekniska och organisatoriska åtgärder som införs för ~~offentliga förvaltningar och~~ marknadsoperatörer bör inte omfatta krav på att en viss kommersiell informations- och kommunikationsteknisk produkt utformas, utvecklas eller tillverkas på ett visst sätt. **[Ändr. 26]**

(26) ~~De offentliga förvaltningarna och~~ Marknadsoperatörerna bör garantera säkerheten för de nät och system som står under deras kontroll. Det rör sig framför allt om privata nät och system som antingen förvaltas av deras interna it-personal eller vars säkerhet har lagts ut på entreprenad. Säkerheten och anmälningsskyldigheterna bör gälla för relevanta marknadsoperatörer ~~och offentliga förvaltningar~~ oavsett om de själva sköter underhållet på sina nät och informationssystem internt eller om de lägger ut uppgifterna på entreprenad. **[Ändr. 27]**

(27) För att undvika oproportionerligt stora finansiella och administrativa bördor för små operatörer och användare bör kraven stå i proportion till den risk som det berörda nätet eller informationssystemet utgör, med beaktande av de bästa sådana åtgärderna. Dessa krav bör inte gälla för mikroföretag.

(28) Behöriga myndigheter ***och gemensamma kontaktpunkter*** bör se till att upprätthålla informella och tillförlitliga kanaler för informationsutbyte mellan marknadsoperatörer och mellan offentlig och privat sektor. ***Behöriga myndigheter och gemensamma kontaktpunkter bör informera tillverkare och leverantörer av berörda IKT-produkter och IKT-tjänster om incidenter som har en betydande inverkan och som anmälts till dem.*** Vid offentliggörande av incidenter som rapporteras till de behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** bör allmänhetens intresse av att få information om hot vägas mot eventuella negativ inverkan på ryktet och affärerna för de ~~offentliga förvaltningar och~~ marknadsoperatörer som rapporterar incidenter. Vid genomförandet av anmälningsskyldigheterna bör behöriga myndigheter ***och gemensamma kontaktpunkter*** särskilt ta hänsyn till behovet av att hålla uppgifter om produkters sårbara aspekter strikt konfidentiella till dess att ändamålsenliga säkerhetslösningar ~~släpps~~ ***satts i verket***. ***Den allmänna regeln bör vara att gemensamma kontaktpunkter inte bör lämna ut personuppgifter om dem som är inblandade i incidenter. Gemensamma kontaktpunkter bör lämna ut personuppgifter endast om det är nödvändigt och proportionellt för ändamålet.*** **[Ändr. 28]**

(29) Behöriga myndigheter bör ha de medel som de behöver för att kunna fullgöra sina förpliktelser, inbegripet befogenhet att få fram tillräckligt med information från marknadsoperatörer ~~och offentliga förvaltningar~~ för att bedöma säkerhetsnivån för nät och informationssystem ***och mäta incidenters antal, storlek och omfattning,*** liksom tillförlitliga och heltäckande data om faktiska incidenter som har inverkat på nätens och informationssystemens drift. **[Ändr. 29]**

(30) I många fall är det kriminell verksamhet som ligger bakom en incident. Incidenternas kriminella art kan misstänkas även om det inte finns några entydiga bevis från början. I sådana fall bör ett lämpligt samarbete mellan behöriga myndigheter***, gemensamma kontaktpunkter*** och brottsbekämpande myndigheter ***samt samarbete med Europols it-brottscentrum (EC3) och Enisa*** ingå i effektiva och omfattande svarsåtgärder på hotet från säkerhetsincidenter. För att främja en säker, trygg och mer motståndskraftig miljö krävs i synnerhet en systematisk rapportering av incidenter som misstänks vara av kriminell art till de brottsbekämpande myndigheterna. Incidenters allvarliga kriminella art bör bedömas i ljuset av unionsrätten om it-brott. **[Ändr. 30]**

(31) Säkerheten för personuppgifter äventyras ofta till följd av incidenter. ***Medlemsstater och marknadsoperatörer bör skydda personuppgifter som lagras, behandlas eller överförs mot oavsiktlig eller olaglig förstörelse, oavsiktlig förlust eller ändring, och otillåten eller olaglig lagring, åtkomst, utlämning eller spridning, och säkerställa genomförandet av en säkerhetsstrategi för behandling av personuppgifter.*** I detta sammanhang bör de behöriga myndigheterna***, de gemensamma kontaktpunkterna*** och dataskyddsmyndigheterna samarbeta och utbyta information ~~om alla relevanta frågor~~***, vid behov även med marknadsoperatörer,*** för att ***i enlighet med tillämpliga dataskyddsregler*** hantera personuppgiftsbrott till följd av incidenter. ~~Medlemsstaterna ska genomföra~~ Skyldigheten att anmäla säkerhetsincidenter ***bör fullgöras*** på ett sätt som minimerar den administrativa bördan om säkerhetsincidenten också är ett personuppgiftsbrott ~~i linje med förslaget till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter[1]. Genom samarbete med de behöriga myndigheterna och dataskyddsmyndigheterna skulle~~ ***som ska anmälas i enlighet med unionens dataskyddslagstiftning.*** Enisa ***bör*** kunna vara till hjälp genom att utveckla mekanismer ~~och modeller~~ för informationsutbyte ~~så att det inte behövs två anmälningsmallar. Denna enda~~ ***och en gemensam*** anmälningsmall***, vilket*** skulle underlätta rapporteringen av incidenter som hotar säkerheten för personuppgifter och därigenom lätta den administrativa bördan för företag och offentliga förvaltningar.
[Ändr. 31]

~~[1] SEK(2012) 72 slutlig.~~

(32) Standardisering av säkerhetskrav är en marknadsdriven process ***av frivillig karaktär som bör möjliggöra för marknadsoperatörer att använda alternativa metoder för att uppnå åtminstone liknande resultat***. För att säkerställa en konvergerad tillämpning av säkerhetsstandarder bör medlemsstaterna främja efterlevnad eller överensstämmelse med specificerade ***interoperabla*** standarder för att garantera en hög säkerhetsnivå på unionsnivå. Därför ***behöver tillämpning av öppna internationella standarder för nät- och informationssäkerhet eller utformning av sådana verktyg övervägas. En annan nödvändig åtgärd*** kan ~~det~~ vara ~~nödvändigt~~ att utarbeta harmoniserade standarder, i enlighet med Europaparlamentets och rådets förordning (EU) nr 1025/2012[1]. ***Särskilt bör Etsi, CEN och Cenelec ges i uppdrag att föreslå effektiva och ändamålsenliga öppna säkerhetsstandarder för unionen, där tekniska preferenser undviks så långt möjligt, och som bör vara lätthanterliga för små och medelstora marknadsoperatörer. Internationella standarder för it-säkerhet bör granskas noggrant för att säkerställa att de inte har kompromitterats och att de ger en tillräcklig säkerhetsnivå, och sålunda garanterar att den föreskrivna efterlevnaden av it-säkerhetsstandarder ökar unionens it-säkerhet som helhet och inte minskar den.*** **[Ändr. 32]**

(33) Detta direktiv bör ***med jämna mellanrum*** ses över ~~med jämna mellanrum~~ ***av kommissionen***, ***i samråd med alla berörda aktörer,*** främst i syfte att avgöra behovet av modifieringar med hänsyn till ***samhällsutvecklingen,*** den ***politiska utvecklingen, den*** tekniska utvecklingen eller ändrade marknadsvillkor. **[Ändr. 33]**

---

[1] Europaparlamentets och rådets förordning (EU) nr 1025/2012 av den 25 oktober 2012 om europeisk standardisering och om ändring av rådets direktiv 89/686/EEG och 93/15/EEG samt av Europaparlamentets och rådets direktiv 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG och 2009/105/EG samt om upphävande av rådets beslut 87/95/EEG och Europaparlamentets och rådets beslut 1673/2006/EG (EUT L 316, 14.11.2012, s. 12).

(34) För att se till att samarbetsnätverket fungerar på ett korrekt sätt bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen med avseende på ~~fastställandet av de kriterier som en medlemsstat ska uppfylla för att ha rätt att delta~~ ***gemensamma standarder för samtrafik och säkerhet*** i ~~det~~ ***den*** säkra ~~informationsutbytessystemet,~~ ***informationsutbytesinfrastrukturen och*** ytterligare specificering av de händelser som utlöser tidig varning ~~och definitionen av de omständigheter då marknadsoperatörer och offentliga förvaltningar är skyldiga att anmäla incidenter~~. **[Ändr. 34]**

(35) Det är av särskild betydelse att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå. Vid förberedelse och utarbetande av delegerade akter bör kommissionen säkerställa att relevanta dokument samtidigt, utan dröjsmål och på lämpligt sätt lämnas till Europaparlamentet och rådet.

(36) För att säkerställa enhetliga villkor för genomförandet av direktivet bör kommissionen ges genomförandebefogenheter när det gäller samarbetet mellan ~~behöriga myndigheter~~ ***gemensamma kontaktpunkter*** och kommissionen inom samarbetsnätverket***, dock utan att det påverkar befintliga nationella samarbetsmekanismer***, ~~tillträdet till den säkra infrastrukturen för informationsutbyte,~~ unionens samarbetsplan för nät- och informationssäkerhet, formaten och förfarandena för att ~~informera allmänheten~~ ***rapportera*** om incidenter ~~samt standarderna och/eller de tekniska specifikationerna av betydelse för nät- och informationssäkerhet~~ ***som har en betydande inverkan***. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011[1]. **[Ändr. 35]**

[1] Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

(37) Vid tillämpningen av direktivet bör kommissionen på lämpligt sätt samarbeta med relevanta sektorskommittéer och organ som inrättas på EU-nivå, i synnerhet ~~inom energi-, transport- och~~ ***på områdena e-förvaltning, energi***, ***transport,*** hälso- och ~~sjukvårdsområdet~~ ***sjukvård och försvar***. **[Ändr. 36]**

(38) Information som ~~den nationella regleringsmyndigheten~~ ***en behörig myndighet eller en gemensam kontaktpunkt*** anser vara konfidentiell i enlighet med unionslagstiftning och nationell lagstiftning om affärshemligheter, får ~~endast~~ utbytas med kommissionen ~~och~~***, kommissionens relevanta organ, gemensamma kontaktpunkter och/eller*** andra behöriga ***nationella*** myndigheter ***endast*** när sådant utbyte är absolut nödvändigt för att tillämpa bestämmelserna i detta direktiv. Den information som utbyts bör begränsas till vad som är relevant***, nödvändigt*** och proportionellt för ändamålet med utbytet***, och den bör respektera på förhand fastställda kriterier för konfidentialitet och säkerhet – i enlighet med beslut 2011/292/EU –, för information som omfattas av sekretessavtal och för informella sekretessavtal, t.ex. Traffic Light Protocol***. **[Ändr. 37]**

(39) Utbytet av information om risker och incidenter inom samarbetsnätverket och uppfyllandet av kravet att anmäla incidenter till de behöriga nationella myndigheterna ***eller gemensamma kontaktpunkterna*** kan förutsätta behandling av personuppgifter. Sådan behandling av personuppgifter är nödvändig för att tillgodose detta direktivs syfte av allmänintresse och är därmed berättigad enligt artikel 7 i direktiv 95/46/EG. I förhållande till detta legitima syfte utgör den inte ett oproportionerligt och oacceptabelt ingripande som påverkar själva kärnan i rätten till skydd av personuppgifter som garanteras enligt artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Vid tillämpningen av detta direktiv bör Europaparlamentets och rådets förordning (EG) nr 1049/2001[1] gälla i tillämpliga fall. När uppgifter behandlas av unionens institutioner och organ bör bearbetning i samband med till genomförandet av detta direktiv ske i enlighet med Europaparlamentets och rådets förordning (EG) nr 45/2001. **[Ändr. 38]**

[1] Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar (EGT L 145, 31.5.2001, s. 43).

(40) Eftersom målet för denna förordning, det vill säga att garantera en hög nivå av nät- och informationssäkerhet i unionen, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna och eftersom det därför, på grund av åtgärdens verkningar, bättre kan uppnås på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går detta direktiv inte utöver vad som är nödvändigt för att uppnå dessa mål.

(41) Förslaget överensstämmer med de grundläggande rättigheterna och de principer som erkänns i Europeiska unionens stadga om de grundläggande rättigheterna, i synnerhet rätten till skydd för privatliv och kommunikation, skyddet av personuppgifter, näringsfriheten, äganderätten, rätten till ett effektivt rättsmedel och rätten att höras. Detta direktiv måste tillämpas i enlighet med dessa rättigheter och principer.

(41a) I enlighet med den gemensamma politiska förklaringen av den 28 september 2011 från medlemsstaterna och kommissionen om förklarande dokument har medlemsstaterna åtagit sig att i motiverade fall låta anmälan av införlivandeåtgärder åtföljas av ett eller flera dokument som förklarar förhållandet mellan de olika delarna i ett direktiv och motsvarande delar i nationella instrument för införlivande. När det gäller detta direktiv anser lagstiftaren det vara motiverat att sådana dokument översänds. **[Ändr. 39]**

(41b) Europeiska datatillsynsmannen har hörts i enlighet med artikel 28.2 i förordning (EG) nr 45/2001 och avgav ett yttrande den 14 juni 2013[1],

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

[1] EUT C 32, 4.2.2014, s. 19.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Syfte och tillämpningsområde

1. Direktivet omfattar åtgärder som ska säkerställa en hög gemensam nivå av nät- och informationssäkerhet (NIS) inom EU.

2. Direktivet omfattar därför följande:

(a) Det fastställer skyldigheter för alla medlemsstater när det gäller förebyggande åtgärder, hantering och svarsåtgärder vid risker och incidenter som påverkar nät och informationssystem.

(b) Det inrättar en samarbetsmekanism mellan medlemsstaterna som ska säkerställa en enhetlig tillämpning av detta direktiv inom unionen och, vid behov, en samordnad ~~och~~ effektiv ***och ändamålsenlig*** hantering och samordnade ~~och~~***,*** effektiva ***och ändamålsenliga*** svarsåtgärder vid risker och incidenter som påverkar nät och informationssystem***, med deltagande av relevanta aktörer***. **[Ändr. 40]**

(c) Det fastställer säkerhetskrav för ~~marknadsaktörer och offentliga förvaltningar~~ ***marknadsoperatörer***. **[Ändr. 41]**

3. Säkerhetskraven enligt artikel 14 i detta direktiv ska inte tillämpas på företag som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster enligt direktiv 2002/21/EG, då dessa ska uppfylla de säkerhets- och integritetskrav som fastställs i artiklarna 13a och 13b i det direktivet, eller på leverantörer av betrodda tjänster.

4. Detta direktiv påverkar inte tillämpningen av unionslagstiftning om it-brottslighet och rådets direktiv 2008/114/EG[1]

[1] Rådets direktiv 2008/114/EG av den 8 december 2008 om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna (EUT L 345, 23.12.2008, s. 75).

5. Detta direktiv påverkar inte heller tillämpningen av Europaparlamentets och rådets direktiv 95/46/EG och direktiv 2002/58/EGoch förordning ***(EG) nr 45/2001*** **.** ***Användningen av personuppgifter ska begränsas till vad som är absolut nödvändigt för syftena med detta direktiv, och uppgifterna ska vara så anonyma som möjligt, om inte fullständigt anonyma.*** **[Ändr. 42]**

6. Informationsutbytet inom samarbetsnätverket enligt kapitel III och anmälan av nät- och informationssäkerhetsincidenter enligt artikel 14 kan förutsätta behandling av personuppgifter. Sådan behandling, som är nödvändig för att tillgodose detta direktivs syfte av allmänintresse ska godkännas av medlemsstaten i enlighet med artikel 7 i direktiv 95/46/EG och direktiv 2002/58/EG, såsom dessa har genomförts i nationell lagstiftning.

Artikel 1a

Skydd och behandling av personuppgifter

1. *All behandling av personuppgifter i medlemsstaterna med tillämpning av detta direktiv ska ske i enlighet med direktiven 95/46/EG och 2002/58/EG.*

2. *All behandling av personuppgifter som utförs av kommissionen och Enisa med tillämpning av detta direktiv ska ske i enlighet med förordning (EG) nr 45/2001.*

3. *All behandling av personuppgifter som utförs av Europeiska it-brottscentrumet inom Europol med tillämpning av detta direktiv ska ske i enlighet med rådets beslut 2009/371/RIF*[1]*.*

4. *Behandlingen av personuppgifter ska vara rättvis och laglig och ska strikt begränsas till de minimiuppgifter som krävs för det syfte för vilket de behandlas. Personuppgifterna ska lagras på ett sätt som förhindrar identifiering av de registrerade under en längre tid än vad som är nödvändigt för det ändamål för vilket personuppgifterna behandlas.*

5. *De anmälningar av incidenter som avses i artikel 14 i detta direktiv ska inte påverka tillämpningen av de bestämmelser och skyldigheter i fråga om att anmäla personuppgiftsbrott som fastställs i artikel 4 i direktiv 2002/58/EG och i kommissionens förordning (EU) nr 611/2013*[2]*.* **[Ändr. 43]**

---

1 *Rådets beslut 2009/371/RIF av den 6 april 2009 om inrättande av Europeiska polisbyrån (Europol) (EUT L 121, 15.5.2009, s. 37).*

2 *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 (EUT L 173, 26.6.2013, s. 2).*

Artikel 2

Minimiharmonisering

Medlemsstaterna ska inte vara förhindrade att anta eller behålla bestämmelser som garanterar en högre säkerhetsnivå, utan att det påverkar deras skyldigheter enligt unionslagstiftningen.

Artikel 3

Definitioner

I detta direktiv gäller följande definitioner:

(1) nät och informationssystem:

(a) elektroniskt kommunikationsnät enligt direktiv 2002/21/EG, och

(b) apparat eller en grupp av sammankopplade apparater eller apparater som hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av ~~datorbehandlade~~ ***digitala*** uppgifter, samt **[Ändr. 44]**

(c) ~~datorbehandlade~~ ***digitala*** uppgifter som lagras, behandlas, hämtas eller överförs med hjälp av element som omfattas av led a och b för att de skall kunna drivas, användas, skyddas och underhållas. **[Ändr. 45]**

(2) säkerhet: förmågan hos ett nät eller ett informationssystem att, vid en viss tillförlitlighetsnivå, tåla olyckshändelser, olagliga handlingar eller illvilligt uppträdande som äventyrar tillgängligheten, autenticiteten, integriteten och konfidentialiteten hos lagrade eller överförda data eller hos besläktade tjänster som tillhandahålls av eller är tillgängliga via dessa nät och informationssystem***; ”säkerhet” inkluderar lämplig teknisk apparatur samt lämpliga lösningar och driftsförfaranden som säkerställer att de säkerhetskrav som anges i detta direktiv är uppfyllda***. **[Ändr. 46]**

(3) risk: en ***rimligen identifierbar*** omständighet eller händelse som har en potentiell negativ inverkan på säkerheten. **[Ändr. 47]**

(4) incident: en ~~omständighet eller~~ händelse som har en faktisk negativ inverkan på säkerheten. **[Ändr. 48]**

~~(5) informationssamhällestjänst: tjänst enligt artikel 1.2 i direktiv 98/34/EG.~~ **[Ändr. 49]**

(6) NIS-samarbetsplan: en plan som fastställer en ram för organisatoriska roller, ansvarsområden och förfaranden för att bibehålla eller återställa driften av nät och informationssystem som påverkas av en risk eller incident.

(7) incidenthantering: alla förfaranden som stöder ***upptäckt, förebyggande,*** analys och begränsning av effekterna av en incident samt svarsåtgärder. **[Ändr. 50]**

(8) marknadsoperatör:

~~(a) Leverantör av informationssamhällestjänster som möjliggör tillhandahållandet av andra informationssamhällestjänster; en ej uttömmande förteckning över sådana tjänster finns i bilaga II.~~ **[Ändr. 51]**

(b) Operatör av kritisk infrastruktur som är nödvändig för upprätthållandet av viktig ekonomisk och samhällelig verksamhet inom områdena energi, transport, bankverksamhet, ***finansmarknadsinfrastrukturer***, ***internetknutpunkter, försörjningskedjan för livsmedel*** samt hälso- och ~~sjukvårdsverksamhet~~ ***sjukvård, och då störningar eller förstörelse som gör att dessa funktioner inte kan upprätthållas skulle ha en betydande inverkan i en medlemsstat***; en ej uttömmande förteckning över sådana verksamheter finns i bilaga II***, i den mån det berörda nätet och de berörda informationssystemen har en anknytning till verksamheternas kärntjänster***. **[Ändr. 52]**

(8a) incident som har en betydande inverkan: en incident som påverkar säkerheten och kontinuiteten för ett informationsnät eller informationssystem och som leder till betydande störning av centrala ekonomiska eller samhälleliga funktioner. **[Ändr. 53]**

(9) standard: standard som avses i förordning (EU) nr 1025/2012.

(10) specifikation: specifikation som avses i förordning (EU) nr 1025/2012.

(11) leverantör av betrodd tjänst: fysisk eller juridisk person som tillhandahåller en elektronisk tjänst som består av skapande, kontroll, validering, hantering och bevarande av elektroniska signaturer, elektroniska sigill, elektroniska tidsmärkningar, elektroniska dokument, elektroniska leveranstjänster, autentisering av webbplatser och elektroniska certifikat, inklusive certifikat för elektroniska signaturer och för elektroniska sigill.

(11a) reglerad marknad: reglerad marknad enligt definitionen i artikel 4.14 i Europaparlamentets och rådets direktiv 2004/39/EG[1]. **[Ändr. 54]**

(11b) multilateral handelsplattform (MTF-plattform): multilateral handelsplattform enligt definitionen i artikel 4.15 i direktiv 2004/39/EG. **[Ändr. 55]**

(11c) organiserad handelsplattform: ett multilateralt system eller en multilateral facilitet – dock inte en reglerad marknad, en multilateral handelsplattform eller en central motpart – som drivs av ett värdepappersföretag eller en marknadsoperatör och där flera tredje parters köp- och säljintressen i obligationer, strukturerade finansiella produkter, utsläppsrätter eller derivat kan interagera inom systemet så att detta leder till ett avtal i enlighet med avdelning II i direktiv 2004/39/EG. **[Ändr. 56]**

---

1 ***Europaparlamentets och rådets direktiv 2004/39/EG av den 21 april 2004 om marknader för finansiella instrument (EUT L 45, 16.2.2005, s. 18).***

KAPITEL II

NATIONELLA RAMVERK FÖR NÄT- OCH INFORMATIONSSÄKERHET

Artikel 4

Princip

Medlemsstaterna ska säkerställa en hög säkerhetsnivå för nät och informationssystem på deras territorium i enlighet med detta direktiv.

Artikel 5

Nationell NIS-strategi och nationell NIS-samarbetsplan

1. Varje medlemsstat ska anta en nationell NIS-strategi som fastställer de strategiska målen och de konkreta politiska åtgärderna och lagstiftningsåtgärderna för att uppnå och upprätthålla en hög nivå av nät- och informationssäkerhet. Den nationella NIS-strategin ska i synnerhet omfatta följande:

   (a) Definitionen av mål och prioriteringar för strategin baserat på en aktuell risk- och incidentanalys.

   (b) En styrelseram för att uppnå de strategiska målen och prioriteringarna, inklusive en tydlig definition av roller och ansvarsområden för offentliga organ och andra berörda aktörer.

(c) Identifiering av allmänna beredskaps-, svars- och återhämtningsåtgärder, inklusive mekanismer för samarbete mellan offentlig och privat sektor.

(d) Angivelse av utbildnings- och informationsprogram.

(e) Forsknings- och utvecklingsplaner och en beskrivning av hur dessa planer speglar de angivna prioriteringarna.

(ea) Medlemsstaterna kan begära hjälp av Enisa när det gäller att utveckla de nationella strategierna och nationella samarbetsplanerna för nät- och informationssäkerhet, på grundval av en gemensam grundläggande strategi i fråga om nät- och informationssäkerhet. **[Ändr. 57]**

2. Den nationella NIS-strategin ska innehålla en nationell NIS-samarbetsplan som minst uppfyller följande krav:

(a) En ~~riskbedömningsplan~~ ***riskhanteringsram*** för ***att utveckla en metod för*** kartläggning***, rangordning, utvärdering och åtgärdande*** av risker ~~och~~***,*** bedömning av verkningarna av potentiella incidenter***, handlingsalternativ för förebyggande och kontroll samt för att fastställa kriterier för valet av möjliga motåtgärder***.
[Ändr. 58]

(b) Definition av roller och ansvarsområden för olika ***myndigheter och övriga*** aktörer som deltar i genomförandet av ~~planen~~ ***ramen***. **[Ändr. 59]**

(c) Definition av samarbets- och kommunikationsprocesser som säkerställer förebyggande, upptäckt, svarsåtgärder, reparation och återhämtning och som anpassas till larmnivån.

(d) En plan för nät- och informationssäkerhetsövningar och -utbildning för att stärka, validera och testa planen. Lärdomar ska dokumenteras och föras in när planen uppdateras.

3. Den nationella NIS-strategin och den nationella NIS-samarbetsplanen ska meddelas kommissionen inom ~~en månad~~ ***tre månader*** från antagandet. **[Ändr. 60]**

Artikel 6

~~Nationell behörig myndighet~~ ***Nationella behöriga myndigheter och gemensamma kontaktpunkter*** för säkerheten i nät och informationssystem **[Ändr. 61]**

1. Varje medlemsstat ska utse en ~~behörig nationell myndighet~~ ***eller flera civila behöriga nationella myndigheter*** för säkerheten i nät och informationssystem (den ***eller de*** behöriga ~~myndigheten~~ ***myndigheterna***). **[Ändr. 62]**

2. De behöriga myndigheterna ska övervaka tillämpningen av detta direktiv på nationell nivå och bidra till en konsekvent tillämpning i hela unionen.

2a. Om en medlemsstat utser mer än en behörig myndighet ska den utse en civil nationell myndighet, t.ex. en behörig myndighet, som nationell gemensam kontaktpunkt för säkerheten i nät och informationssystem (nedan kallad gemensam kontaktpunkt). Om en medlemsstat utser endast en behörig myndighet ska denna behöriga myndighet också vara den gemensamma kontaktpunkten. **[Ändr. 63]**

2b. De behöriga myndigheterna och den gemensamma kontaktpunkten i en medlemsstat ska ha ett nära samarbete när det gäller skyldigheterna enligt detta direktiv. **[Ändr. 64]**

2c. ***Den gemensamma kontaktpunkten ska se till att det finns ett gränsöverskridande samarbete med andra gemensamma kontaktpunkter.*** **[Ändr. 65]**

3. Medlemsstaterna ska se till att de behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** har tillräckliga tekniska och finansiella resurser samt personalresurser för att på ett effektivt sätt kunna utföra de uppgifter de tilldelas och därigenom uppnå detta direktivs syften. Medlemsstaterna ska se till att de ~~behöriga myndigheterna~~ ***gemensamma kontaktpunkterna*** samarbetar på ett ***ändamålsenligt,*** effektivt och säkert sätt via det nätverk som avses i artikel 8. **[Ändr. 66]**

4. Medlemsstaterna ska se till att de behöriga myndigheterna ***och de gemensamma kontaktpunkterna, i tillämpliga fall i enlighet med punkt 2a i denna artikel,*** får de anmälningar av incidenter som görs av ~~offentliga förvaltningar och~~ marknadsoperatörer såsom anges i artikel 14.2 och att de tilldelas de genomförande- och verkställighetsbefogenheter som avses i artikel 15. **[Ändr. 67]**

4a. ***Om det i unionsrätten föreskrivs ett sektorsspecifikt tillsyns- eller regleringsorgan på unionsnivå, bland annat för säkerheten i nät och informationssystem, ska detta organ ta emot anmälningarna av incidenter i enlighet med artikel 14.2 från berörda marknadsoperatörer i sektorn och tilldelas de befogenheter för genomförande och efterlevnad som avses i artikel 15. Unionsorganet ska ha ett nära samarbete med de behöriga myndigheterna och den gemensamma kontaktpunkten i värdmedlemsstaten när det gäller dessa skyldigheter. Den gemensamma kontaktpunkten i värdmedlemsstaten ska företräda unionsorganet när det gäller de skyldigheter som fastställs i kapitel III.*** **[Ändr. 68]**

5. De behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** ska när så är lämpligt samråda och samarbeta med de relevanta nationella rättsvårdande myndigheterna och dataskyddsmyndigheterna. **[Ändr. 69]**

6. Varje medlemsstat ska utan dröjsmål meddela kommissionen ***de behöriga myndigheter och*** den ~~behöriga myndighet~~ ***gemensamma kontaktpunkt*** som utses, denna myndighets uppgifter och alla senare ändringar av detta. Varje medlemsstat ska offentliggöra utnämningen av ~~den~~ ***de*** behöriga ~~myndigheten~~ ***myndigheterna***. **[Ändr. 70]**

Artikel 7

Incidenthanteringsorganisation

1. Varje medlemsstat ska inrätta ***åtminstone*** en incidenthanteringsorganisation (Computer Emergency Response Team, Cert) ***för var och en av de sektorer*** som ~~ansvarar~~ ***anges i bilaga II, med ansvar*** för hanteringen av incidenter och risker i enlighet med ett tydligt fastställt förfarande som ska uppfylla kraven i bilaga I punkt 1. En incidenthanteringsorganisation får inrättas inom den behöriga myndigheten. **[Ändr. 71]**

2. Medlemsstaterna ska se till att incidenthanteringsorganisationerna har de tekniska och finansiella resurser och personalresurser som behöver för att effektivt utföra sina uppgifter som anges i bilaga I punkt 2.

3. Medlemsstaterna ska se till att incidenthanteringsorgansationer förlitar sig på en säker och motståndskraftig kommunikations- och informationsinfrastruktur på nationell nivå, och den ska vara förenlig och interoperabel med det säkra system för informationsutbyte som avses i artikel 9.

4. Medlemsstaterna ska underrätta kommissionen om incidenthanteringsorganisationernas resurser och mandat samt om deras förfarande för incidenthantering.

5. ~~Incidenthanteringsorganisationen~~ ***Incidenthanteringsorganisationerna*** ska bedriva sin verksamhet under tillsyn av den behöriga myndigheten ***eller den gemensamma kontaktpunkten***, som regelbundet ska bedöma om resurserna är tillräckliga, om ~~mandatet är ändamålsenligt~~ ***mandaten är ändamålsenliga*** och om incidenthanteringsförfarandet är effektivt. **[Ändr. 72]**

5a. Medlemsstaterna ska se till att incidenthanteringsorganisationerna har tillräckliga personalresurser och ekonomiska resurser för att aktivt delta i internationella samarbetsnätverk, särskilt sådana nätverk på unionsnivå. **[Ändr. 73]**

5b. Incidenthanteringsorganisationerna ska ges möjlighet och uppmuntras att inleda och delta i gemensamma övningar med andra incidenthanteringsorganisationer, med alla incidenthanteringsorganisationer i medlemsstaterna och med lämpliga institutioner i icke-medlemsstater samt med incidenthanteringsorganisationer inom multinationella och internationella institutioner såsom Nato och FN. **[Ändr. 74]**

5c. Medlemsstaterna får be om stöd från Enisa eller från andra medlemsstater i utvecklingen av sina nationella incidenthanteringsorganisationer. **[Ändr. 75]**

KAPITEL III

SAMARBETE MELLAN BEHÖRIGA MYNDIGHETER

Artikel 8

Samarbetsnätverk

1. De ~~behöriga myndigheterna och~~ ***gemensamma kontaktpunkterna,*** kommissionen ***och Enisa*** ska bilda ett nätverk (***nedan kallat*** samarbetsnätverk) för att samarbeta om risker och incidenter som påverkar nät och informationssystem. **[Ändr. 76]**

2. Samarbetsnätverket ska föra samman kommissionen och de ~~behöriga myndigheterna~~ ***gemensamma kontaktpunkterna*** i kontinuerlig kommunikation. På begäran ska ~~Europeiska byrån för nät- och informationssäkerhet (~~Enisa~~)~~ bistå samarbetsnätverket med expertis och råd. ***Vid behov får även marknadsoperatörer och leverantörer av it-säkerhetslösningar inbjudas att delta i verksamheten i det samarbetsnätverk som avses i punkt 3 g och i.***

Samarbetsnätverket ska, när så är lämpligt, samarbeta med dataskyddsmyndigheterna.

Kommissionen ska regelbundet informera samarbetsnätverket om säkerhetsforskning och andra relevanta program inom Horisont 2020. **[Ändr. 77]**

3. Inom samarbetsnätverket ska de ~~behöriga myndigheterna~~ ***gemensamma kontaktpunkterna*** göra följande:

(a) Sprida tidiga varningar om risker och incidenter i enlighet med artikel 10.

(b) Säkerställa samordnade svarsåtgärder i enlighet med artikel 11.

(c) Regelbundet offentliggöra ej konfidentiell information om pågående tidiga varningar och samordnade svarsåtgärder på en gemensam webbplats.

(d) ~~På en begäran av en medlemsstat eller kommissionen~~ gemensamt diskutera och bedöma en eller leda nationella NIS-strategier och nationella NIS-samarbetsplaner enligt artikel 5, inom detta direktivs räckvidd.

(e) ~~På begäran av en medlemsstat eller kommissionen~~ gemensamt diskutera och bedöma incidenthanteringsorganisationernas effektivitet, i synnerhet när NIS-övningar genomförs på unionsnivå.

(f) Samarbeta och utbyta ~~information~~ ***sakkunskap*** om ~~alla~~ relevanta frågor ~~med Europeiska it-brottscentrumet inom Europol och med andra relevanta europeiska organ~~ ***rörande nät- och informationssäkerhet***, i synnerhet inom områdena dataskydd, energi, transport, bankverksamhet, ***finansmarknader*** börs och hälso- och sjukvård***, med Europeiska it-brottscentrumet inom Europol och med andra relevanta europeiska organ***.

(fa) Vid behov informera EU:s samordnare för kampen mot terrorism, genom en rapport, och eventuellt be denne om stöd i samband med samarbetsnätverkets analyser, förberedande arbeten och åtgärder.

(g) Utbyta information och bästa praxis med varandra och med kommissionen och bistå varandra i uppbyggnaden av NIS-kapacitet.

~~(h) Anordna regelbundna kollegiala granskningar av kapacitet och beredskap.~~

(i) Anordna NIS-övningar på unionsnivå och delta, såsom lämpligt, i internationella NIS-övningar.

(ia) Involvera, samråda med och vid behov utbyta information med marknadsoperatörer med avseende på risker och incidenter som påverkar deras nät och informationssystem.

(ib) I samarbete med Enisa utarbeta riktlinjer för sektorsspecifika kriterier för anmälan av betydande incidenter, utöver de faktorer som anges i artikel 14.2, i syfte att uppnå en gemensam tolkning, en enhetlig tillämpning och ett enhetligt genomförande inom unionen. **[Ändr. 78]**

3a. ***Samarbetsnätverket ska offentliggöra en årlig rapport som grundar sig på nätverkets verksamhet under de senaste tolv månaderna och på den sammanfattande rapport som ska lämnas in i enlighet med artikel 14.4 i detta direktiv.*** **[Ändr. 79]**

4. Kommissionen ska genom genomförandeakter anta de bestämmelser som är nödvändiga för att underlätta samarbetet mellan ~~behöriga myndigheter och~~ ***gemensamma kontaktpunkter,*** kommissionen ***och Enisa*** enligt punkterna 2 och 3. Dessa genomförandeakter ska antas i enlighet med det ~~samrådsförfarande~~ ***granskningsförfarande*** som avses i artikel ~~19.2~~ ***19.3***. **[Ändr. 80]**

Artikel 9

Säkert system för informationsutbyte

1. Känslig och konfidentiell information inom samarbetsnätverket ska utbytas via en säker infrastruktur.

1a. Deltagare i den säkra infrastrukturen ska agera i överensstämmelse med bland annat lämpliga åtgärder för sekretess och säkerhet i enlighet med direktiv 95/46/EG och förordning (EG) nr 45/2001 under alla steg av behandlingen. **[Ändr. 81]**

~~2. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet med artikel 18 när det gäller definitionen av de kriterier som en medlemsstat ska uppfylla för att godkännas för deltagande i det säkra systemet för informationsutbyte, vad gäller följande:~~

~~(a) Medlemsstaten ska ha tillgång till en säker och motståndskraftig kommunikations- och informationsinfrastruktur på nationell nivå, som ska vara förenlig och interoperabel med samarbetsnätverkets säkra infrastruktur i enlighet med artikel 7.3.~~

~~(b) Den behöriga myndigheten och incidenthanteringsorganisationen ska ha tillräckliga tekniska och finansiella resurser samt personalresurser för att på ett effektivt och säkert sätt kunna delta i det säkra systemet för informationsutbyte i enlighet med artiklarna 6.3, 7.2 och 7.3.~~ **[Ändr. 82]**

3. Kommissionen ska genom ~~genomförandeakter besluta om medlemsstaternas tillträde till denna säkra infrastruktur, i enlighet med de kriterier som avses i punkterna 2 och 3. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 19~~ ***delegerade akter i enlighet med artikel 18 anta gemensamma standarder för samtrafik och säkerhet som de gemensamma kontaktpunkterna ska uppfylla innan de utbyter känslig och konfidentiell information inom samarbetsnätverket***. **[Ändr. 83]**

Artikel 10

Tidig varning

1. De ~~behöriga myndigheterna~~ ***gemensamma kontaktpunkterna*** eller kommissionen ska lämna tidiga varningar inom samarbetsnätverket om de risker eller incidenter som uppfyller minst ett av följande villkor:

~~(a) De ökar snabbt i omfattning eller kan öka snabbt i omfattning.~~

(b) ~~De överstiger~~ ***Den gemensamma kontaktpunkten bedömer att risken*** eller ~~kan~~ ***incidenten skulle kunna*** överstiga den nationella kapaciteten för svarsåtgärder.

(c) De ***gemensamma kontaktpunkterna eller kommissionen bedömer att risken eller incidenten*** påverkar ~~eller kan påverka~~ mer än en medlemsstat. **[Ändr. 84]**

2. I de tidiga varningarna ska de ~~behöriga myndigheterna~~ ***gemensamma kontaktpunkterna*** eller kommissionen ***utan onödigt dröjsmål*** meddela all relevant information som de förfogar över och som kan vara till nytta för att bedöma risken eller incidenten. **[Ändr. 85]**

~~3. På begäran av en medlemsstat eller på eget initiativ kan kommissionen begära att en medlemsstat inkommer med relevant information om en specifik risk eller incident.~~ **[Ändr. 86]**

4. Om den risk eller incident som är föremål för en tidig varning misstänks vara av brottslig art ***och om den berörda marknadsoperatören har rapporterat incidenter som misstänks vara av allvarlig brottslig art enligt artikel 15.4*** ska ~~de behöriga myndigheterna eller kommissionen underrätta~~ ***medlemsstaterna i tillämpliga fall se till att*** Europeiska it-brottscentrumet inom Europol ***underrättas***. **[Ändr. 87]**

4a. Medlemmarna i samarbetsnätverket får inte offentliggöra den mottagna informationen om risker och incidenter enligt punkt 1 utan att först ha erhållit godkännande från den anmälande gemensamma kontaktpunkten.

Innan informationen utbyts inom samarbetsnätverket ska den anmälande gemensamma kontaktpunkten dessutom informera den marknadsoperatör som informationen avser om sin avsikt, och, i den mån den anser att det är lämpligt, anonymisera informationen. **[Ändr. 88]**

4b. Om den risk eller incident som är föremål för en tidig varning misstänks vara av allvarlig gränsöverskridande teknisk art ska de gemensamma kontaktpunkterna eller kommissionen underrätta Enisa. **[Ändr. 89]**

5. Kommissionen ska ges befogenhet att anta delegerade akter i enlighet med artikel 18 när det gäller ytterligare specificering av risker och incidenter som utlöser en tidig varning enligt punkt 1 i den här artikeln.

Artikel 11

Samordnade svarsåtgärder

1. Efter en tidig varning enligt artikel 10 ska de ~~behöriga myndigheterna~~ ***gemensamma kontaktpunkterna***, efter att gjort en bedömning av den relevanta informationen ***och utan onödigt dröjsmål,*** enas om samordnade svarsåtgärder i enlighet med unionens NIS-samarbetsplan enligt artikel 12. **[Ändr. 90]**

2. De olika åtgärder som antas på nationell nivå till följd av de samordnade svarsåtgärderna ska meddelas samarbetsnätverket.

Artikel 12

Unionens NIS-samarbetsplan

1. Kommissionen ska ha befogenhet att genom genomförandeakter anta unionens NIS-samarbetsplan. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 19.3.

2. Unionens NIS-samarbetsplan ska omfatta följande:

(a) För de syften som avses i artikel 10:

– En definition av format och förfaranden för de ~~behöriga myndigheternas~~ ***gemensamma kontaktpunkternas*** insamling och utbyte av kompatibla och jämförbara uppgifter om risker och incidenter. **[Ändr. 91]**

– En definition av förfarandena och kriterierna för samarbetsnätverkets bedömning av risker och incidenter.

(b) Förfarandena för samordnade svarsåtgärder enligt artikel 11, inklusive definition av roller, ansvarsområden och samarbetsförfaranden.

(c) En plan för NIS-övningar och NIS-utbildning för att stärka, validera och testa planen.

(d) Ett program för överföring av kunskap mellan medlemsstater när det gäller kapacitetsuppbyggnad och ömsesidigt lärande.

(e) Ett program för medvetandehöjande och utbildning mellan medlemsstaterna.

3. Unionens NIS-samarbetsplan ska antas senast ett år efter detta direktivs ikraftträdande och regelbundet revideras. ***Resultaten av varje revidering ska rapporteras till Europaparlamentet.*** **[Ändr. 92]**

3a. Det ska säkerställas att det råder samstämdhet mellan unionens NIS-samarbetsplan och de nationella NIS-strategier och NIS-samarbetsplaner som föreskrivs i artikel 5. **[Ändr. 93]**

Artikel 13

Internationellt samarbete

Utan att det påverkar samarbetsnätverkets möjlighet att ha informella internationella samarbeten får unionen ingå internationella avtal med tredjeländer eller internationella organisationer som tillåter och organiserar deras deltagande i vissa av samarbetsnätverkets verksamheter. Sådana avtal ska beakta behovet av ändamålsenligt skydd för personuppgifter som förmedlas via samarbetsnätverket ***samt ange det kontrollförfarande som ska tillämpas för att garantera skyddet av sådana personuppgifter***. ***Europaparlamentet ska informeras om avtalsförhandlingarna. Om personuppgifter överförs till mottagare i länder utanför unionen ska det ske i enlighet med artiklarna 25 och 26 i direktiv 95/46/EG och artikel 9 i förordning (EG) nr 45/2001.*** **[Ändr. 94]**

Artikel 13a

Marknadsoperatörernas kritikalitet

Medlemsstaterna får fastställa marknadsoperatörernas kritikalitet, med hänsyn till de särskilda förhållandena i sektorn, faktorer såsom den berörda marknadsoperatörens betydelse för att upprätthålla en tillräcklig service i sektorn, antalet parter som marknadsoperatören levererar tjänster till och den tid det tar innan avbrottet i marknadsoperatörens kärntjänster får en negativ inverkan på upprätthållandet av viktig ekonomisk och samhällelig verksamhet. **[Ändr. 95]**

KAPITEL IV

SÄKERHET FÖR OFFENTLIGA FÖRVALTNINGARS OCH MARKNADSOPERATÖRERS NÄT OCH INFORMATIONSSYSTEM

Artikel 14

Säkerhetskrav och anmälan av incidenter

1. Medlemsstaterna ska se till att ~~offentliga förvaltningar och~~ marknadsoperatörer vidtar ändamålsenliga ***och proportionella*** tekniska och organisatoriska åtgärder för att ***upptäcka och effektivt*** hantera risker som hotar säkerheten för de nät och informationssystem som de kontroller och använder i sin verksamhet. Med beaktande av den senaste tekniken ska dessa åtgärder ~~garantera~~***säkerställa*** en säkerhetsnivå som är anpassad till den aktuella risken. I synnerhet ska åtgärder vidtas för att förebygga och minimera de effekter som incidenter som påverkar ***säkerheten för*** deras nät och informationssystem har på de kärntjänster som de tillhandahåller och därmed säkerställa kontinuiteten för de tjänster som använder dessa nät och informationssystem. **[Ändr. 96]**

2. Medlemsstaterna ska säkerställa att ~~offentliga förvaltningar och~~ marknadsoperatörer ***utan onödigt dröjsmål*** underrättar den behöriga myndigheten ***eller den gemensamma kontaktpunkten*** om incidenter som har en betydande inverkan på ~~säkerheten~~ ***kontinuiteten*** för de kärntjänster som de tillhandahåller. ***Anmälan ska inte medföra ökad ansvarsskyldighet för den anmälande parten.***

För att avgöra om en incident har en betydande inverkan ska man ta hänsyn till bl.a. följande faktorer: **[Ändr. 97]**

(a) Hur många användares kärntjänster som påverkas. **[Ändr. 98]**

(b) Hur länge incidenten varar. **[Ändr. 99]**

(c) Hur stort geografiskt område som påverkas av incidenten. **[Ändr. 100]**

Dessa faktorer ska anges närmare enligt artikel 8.3 ib. **[Ändr. 101]**

2a. ***Marknadsoperatörerna ska anmäla de incidenter som avses i punkterna 1 och 2 till den behöriga myndigheten eller den gemensamma kontaktpunkten i den medlemsstat där kärntjänsten påverkas. Om kärntjänster påverkas i mer än en medlemsstat, ska den gemensamma kontaktpunkt som har mottagit anmälan meddela övriga berörda gemensamma kontaktpunkter med utgångspunkt i informationen från marknadsoperatören. Marknadsoperatörer ska så snart som möjligt få veta vilka andra gemensamma kontaktpunkter som underrättats om incidenten, samt om eventuella vidtagna åtgärder, resultat och all annan information av relevans för incidenten.*** **[Ändr. 102]**

2b. ***Om anmälan innehåller personuppgifter ska den lämnas ut enbart till mottagare inom den underrättade behöriga myndigheten eller gemensamma kontaktpunkten vilka behöver behandla uppgifterna i fråga för att kunna utföra sina uppdrag i enlighet med dataskyddsbestämmelserna. De uppgifter som lämnas ut ska begränsas till vad som är nödvändigt för att dessa personer ska kunna utföra sina uppdrag.*** **[Ändr. 103]**

2c. ***Marknadsoperatörer som inte omfattas av bilaga II får på frivillig basis rapportera incidenter av det slag som anges i artikel 14.2.*** **[Ändr. 104]**

3. Punkterna 1 och 2 gäller för alla marknadsoperatörer som tillhandahåller tjänster inom Europeiska unionen.

4. ***Efter samråd med*** den ***underrättade*** behöriga myndigheten ***och den berörda marknadsoperatören*** får ***den gemensamma kontaktpunkten*** informera allmänheten ~~eller kräva att de offentliga myndigheterna och marknadsoperatörerna informerar allmänheten~~, ***om enskilda incidenter*** om den ~~fastställer~~ ***bedömer*** att ~~det ligger i allmänhetens intresse~~ ***allmänheten behöver känna till dessa för*** att ***man ska kunna förhindra en incident eller åtgärda en pågående incident, eller om den marknadsoperatör som drabbats av en incident har avböjt att utan onödigt dröjsmål åtgärda en allvarlig strukturell sårbarhet i samband med den*** incidenten ~~röjs~~.

Innan information lämnas ut till allmänheten ska den underrättade behöriga myndigheten se till att den berörda marknadsoperatören ges tillfälle att höras och att beslutet om att lämna ut information till allmänheten är välavvägt i förhållande till allmänhetens intresse.

Om information om enskilda incidenter offentliggörs ska den underrättade behöriga myndigheten eller gemensamma kontaktpunkten se till att informationen är så anonymiserad som möjligt.

Den behöriga myndigheten eller den gemensamma kontaktpunkten ska, om det rimligen är möjligt, ge den berörda marknadsoperatören information som möjliggör en effektiv hantering av den anmälda incidenten.

En gång om året ska den ~~behöriga myndigheten~~ ***gemensamma kontaktpunkten*** lämna in en sammanfattande rapport till samarbetsnätverket om de anmälningar som kommit in – ***inklusive antalet anmälningar och med avseende på de incidentfaktorer som anges i punkt 2 i denna artikel*** – och de åtgärder som vidtagits i enlighet med denna punkt. **[Ändr. 105]**

4a. Medlemsstaterna ska uppmuntra marknadsoperatörer att på frivillig basis offentliggöra incidenter som involverar deras företag i sina redovisningar. **[Ändr. 106]**

~~5. Kommissionen ska ha befogenhet att anta delegerade akter i enlighet artikel 18 när det gäller definition av de omständigheter då offentliga förvaltningar och marknadsoperatörer är skyldiga att anmäla incidenter.~~ **[Ändr. 107]**

6. ~~Utan att det påverkar tillämpningen av delegerade akter som antas enligt punkt 5 får~~De behöriga myndigheterna ***eller den gemensamma kontaktpunkten får*** anta riktlinjer ~~och, om nödvändigt, utfärda anvisningar~~ avseende de omständigheter då ~~offentliga förvaltningar och~~ marknadsoperatörer är skyldiga att anmäla incidenter. **[Ändr. 108]**

7. Kommissionen ska ha befogenhet att genom genomförandeakter definiera format och förfaranden för tillämpningen av punkt 2. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 19.

8. Punkterna 1 och 2 ska inte tillämpas på mikroföretag enligt definitionen i kommissionens rekommendation 2003/361/EG[1]***, såvida inte mikroföretaget är ett dotterföretag till en marknadsoperatör enligt definitionen i artikel 3.8 b***. **[Ändr. 109]**

8a. Medlemsstaterna får besluta att tillämpa denna artikel och artikel 15 på offentliga förvaltningar i tillämpliga delar. **[Ändr. 110]**

[1] Kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36).

Artikel 15

Genomförande och efterlevnad

1. Medlemsstaterna ska säkerställa att de behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** har de befogenheter de behöver för att ~~utreda fall då offentliga förvaltningar eller~~ ***säkerställa att*** marknadsoperatörer ~~inte uppfyllt~~ ***uppfyller*** sina skyldigheter enligt artikel 14 ~~och~~***, med*** de effekter som detta har på nätens och informationssystemens säkerhet. **[Ändr. 111]**

2. Medlemsstaterna ska se till att de behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** har befogenhet att ålägga att marknadsoperatörer ~~och offentliga förvaltningar~~ **[Ändr. 112]**

   (a) tillhandahåller den information som behövs för en bedömning av säkerheten i deras nät och informationssystem, inbegripet dokumenterade säkerhetsprinciper, och

   (b) ~~genomgår~~ ***tillhandahåller dokumentation som visar att säkerhetsåtgärderna genomförts effektivt, t.ex. resultaten av*** en säkerhetsrevision som utförs av ett kvalificerat oberoende organ eller av en nationell myndighet och ~~ge~~ ***ger*** den behöriga myndigheten ***eller den gemensamma kontaktpunkten*** tillgång till ~~resultaten~~ ***dokumentationen***. **[Ändr. 113]**

I en sådan begäran ska de behöriga myndigheterna och de gemensamma kontaktpunkterna uppge syftet med begäran och ange tillräckligt tydligt vilken information som begärs. **[Ändr. 114]**

3. Medlemsstaterna ska se till att de behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** har befogenhet att utfärda bindande anvisningar för marknadsoperatörer ~~och offentliga förvaltningar~~. **[Ändr. 115]**

3a. Genom undantag från punkt 2 b i denna artikel får medlemsstaterna besluta att de behöriga myndigheterna eller de gemensamma kontaktpunkterna i förekommande fall ska tillämpa ett annat förfarande på vissa marknadsoperatörer, baserat på deras kritikalitet, fastställd i enlighet med artikel 13a. Om medlemsstaterna fattar ett sådant beslut gäller följande:

(a) De behöriga myndigheterna eller i förekommande fall den gemensamma kontaktpunkten ska ha behörighet att rikta en tillräckligt specifik begäran till marknadsoperatörerna och kräva att de tillhandahåller dokumentation som visar att säkerhetsåtgärderna genomförts effektivt, t.ex. resultaten av en säkerhetsrevision som utförs av en kvalificerad internrevisor, och ger den behöriga myndigheten eller den gemensamma kontaktpunkten tillgång till dokumentationen.

(b) När marknadsoperatören har gjort den begäran som avses i led a får den behöriga myndigheten eller den gemensamma kontaktpunkten vid behov begära ytterligare dokumentation eller kräva att en ytterligare revision utförs av ett kvalificerat oberoende organ eller av en nationell myndighet.

3b. ***Medlemsstaterna får besluta att minska antalet revisioner och intensiteten i dessa för en berörd marknadsoperatör, om den säkerhetsrevision som operatören varit föremål för konsekvent visar på överensstämmelse med kapitel IV.*** **[Ändr. 116]**

4. De behöriga myndigheterna ***och de gemensamma kontaktpunkterna*** ska ***informera de berörda marknadsoperatörerna om möjligheten att*** anmäla incidenter som misstänks vara av allvarlig brottslig art till de rättsvårdande myndigheterna. **[Ändr. 117]**

5. ***Utan att det påverkar tillämpliga dataskyddsregler ska*** de behöriga myndigheterna ~~ska~~ ***och de gemensamma kontaktpunkterna*** ha ett nära samarbete med de myndigheter som ansvarar för skydd av personuppgifter när de åtgärdar incidenter som medför personuppgiftsbrott. ***De gemensamma kontaktpunkterna och dataskyddsmyndigheterna ska i samarbete med Enisa utforma mekanismer för informationsutbyte och en gemensam mall för anmälningar både enligt artikel 14.2 i detta direktiv och enligt annan unionsrätt om dataskydd.*** **[Ändr. 118]**

6. Medlemsstaterna ska säkerställa att alla skyldigheter som införs för ~~offentliga förvaltningar och~~ marknadsoperatörer i enlighet med detta kapitel kan bli föremål för rättslig prövning. **[Ändr. 119]**

6a. ***Medlemsstaterna får besluta att tillämpa artikel 14 och denna artikel på offentliga förvaltningar i tillämpliga delar.*** **[Ändr. 120]**

Artikel 16

Standardisering

1. För att säkerställa en enhetlig tillämpning av artikel 14.1 ska medlemsstaterna***, utan att föreskriva användning av särskild teknik,*** främja användningen av ***interoperabla europeiska eller internationella*** standarder och/eller specifikationer av relevans för nät- och informationssäkerheten. **[Ändr. 121]**

2. Kommissionen ska ~~i genomförandeakter~~ ***uppdra åt ett relevant europeiskt standardiseringsorgan att under samråd med relevanta aktörer*** utarbeta en lista över de standarder ***och/eller specifikationer*** som avses i punkt 1. Listan ska kungöras i *Europeiska unionens officiella tidning*. **[Ändr. 122]**

KAPITEL V

SLUTBESTÄMMELSER

Artikel 17

Sanktioner

1. Medlemsstaterna ska föreskriva sanktioner för överträdelser av nationella bestämmelser som har utfärdats med tillämpning av detta direktiv och ska vidta de åtgärder som krävs för att se till att dessa sanktioner tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska anmäla dessa bestämmelser till kommissionen senast det datum då direktivet införlivas med nationell lagstiftning och skall utan dröjsmål anmäla alla senare ändringar som påverkar dem.

1a. Medlemsstaterna ska se till att de sanktioner som avses i punkt 1 i denna artikel är tillämpliga endast om en marknadsoperatör avsiktligt eller till följd av allvarlig försumlighet har underlåtit att fullgöra sina skyldigheter enligt kapitel IV. **[Ändr. 123]**

2. När säkerhetsincidenter rör personuppgifter ska medlemsstaterna säkerställa att de sanktioner som föreskrivs överensstämmer med de sanktioner som föreskrivs i Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter[1].

[1] SEK(2012) 72 slutlig.

Artikel 18

Utövande av delegeringen

1. Kommissionens rätt att anta delegerade akter gäller på de villkor som fastställs i denna artikel.

2. Befogenhet att anta de delegerade akter som avses i artiklarna 9.3 och 10.5 ska ges till kommissionen. Kommissionen ska utarbeta en rapport om delegeringen av befogenhet senast nio månader före utgången av femårsperioden. Delegeringen av befogenhet ska genom tyst medgivande förlängas med perioder av samma längd, såvida inte Europaparlamentet eller rådet motsätter sig en sådan förlängning senast tre månader före utgången av perioden i fråga.

3. Den delegering av befogenhet som avses i ~~artiklarna 9.2,~~ ***artikel 9.3*** och 10.5 ~~and 14.5~~ får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft. **[Ändr. 124]**

4. När kommissionen antagit en delegerad akt ska den samtidigt underrätta Europaparlamentet och rådet.

5. En delegerad akt som antas i enlighet med ~~artiklarna 9.2,~~ ***artikel 9.3*** och 10.5 ~~and 14.5~~ ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period av två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.
[Ändr. 125]

Artikel 19

Kommittéförfarande

1. Kommissionen ska bistås av en kommitté (kommittén för nät- och informationssäkerhet). Denna ska vara en kommitté enligt förordning (EU) nr 182/2011.

2. När det hänvisas till denna punkt ska artikel 4 i förordning (EU) nr 182/2011 tillämpas.

3. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.

Artikel 20

Översyn

Kommissionen ska regelbundet se över hur detta direktiv fungerar***, i synnerhet listan i bilaga II,*** och rapportera resultaten till Europaparlamentet och rådet. Den första rapporten ska lämnas senast tre år efter den införlivandedag som avses i artikel 21. För detta syfte kan kommissionen begära att medlemsstaterna utan dröjsmål tillhandahåller information. **[Ändr. 126]**

Artikel 21

Införlivande

1. Medlemsstaterna ska senast [ett och ett halvt år efter antagandet] anta och offentliggöra de lagar och andra författningar som är nödvändiga för att följa detta direktiv. De ska till kommissionen genast överlämna texten till dessa bestämmelser.

   De ska tillämpa dessa bestämmelser från och med [ett och ett halvt år efter antagandet].

   När en medlemsstat antar dessa bestämmelser ska de innehålla en hänvisning till detta direktiv eller åtföljas av en sådan hänvisning när de offentliggörs. Närmare föreskrifter om hur hänvisningen ska göras ska varje medlemsstat själv utfärda.

2. Medlemsstaterna ska till kommissionen överlämna texterna till de bestämmelser i nationell lagstiftning som de antar inom det område som omfattas av detta direktiv.

Artikel 22

Ikraftträdande

Detta direktiv träder i kraft den [tjugonde dagen] efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Artikel 23

Adressater

Detta direktiv riktar sig till medlemsstaterna.

Utfärdat i

På Europaparlaments vägnar	*På rådets vägnar*
Ordförande	*Ordförande*

BILAGA I

Krav och uppgifter för ~~incidenthanteringsorganisationen~~ ***incidenthanteringsorganisationerna*** (Cert) **[Ändr. 127]**

Incidenthanteringsorganisationens krav och uppgifter ska på lämpligt och entydigt sätt fastställas och stödjas genom nationell politik och/eller lagstiftning. Följande ska ingå:

(1) Krav för incidenthanteringsorganisationen

(a) ~~Incidenthanteringsorganisationen~~ ***Incidenthanteringsorganisationerna*** ska säkerställa god tillgång till sina kommunikationstjänster genom att undvika felkritiska systemdelar (single points of failure) och ***alltid*** kunna kontaktas och kontakta andra på flera olika sätt. Kommunikationskanalerna ska vara tydligt specificerade och välkända för användargruppen och samarbetspartner. **[Ändr. 128]**

(b) Incidenthanteringsorganisationen ska genomföra och förvalta säkerhetsåtgärder för att säkra konfidentialiteten, integriteten, åtkomligheten och äktheten för den information som den får in och behandlar.

(c) ~~Incidenthanteringsorganisationens~~ ***Incidenthanteringsorganisationernas*** kontor och de informationssystem som ~~den~~ ***de*** använder sig av ska vara lokaliserade till säker plats ***med säkra nät och informationssystem***. **[Ändr. 129]**

(d) Ett kvalitetssystem för tjänsteförvaltningen ska skapas för att följa upp kvaliteten på incidenthanteringsorganisationens arbete och säkerställa kontinuerliga förbättringar. Det ska baseras på tydligt definierade kvalitetsmått som omfattar formella tjänstenivåer och resultatindikatorer.

(e) Kontinuitetsplanering:

– Incidenthanteringsorganisationen ska ha ett ändamålsenligt system för handläggning och dirigering av ansökningar, för att underlätta överlämnanden.

– Incidenthanteringsorganisationen ska ha tillräckligt med personal för att ständigt vara tillgänglig.

– Incidenthanteringsorganisationen ska förlita sig på en infrastruktur vars kontinuitet är säkerställd. Därför måste det finnas redundans vad gäller system och reservlokaler så att incidenthanteringsorganisationen kan säkerställa permanent åtkomst till kommunikationskanalerna.

(2) Incidenthanteringsorganisationens uppgifter

(a) Incidenthanteringsorganisationens uppgifter ska omfatta minst följande:

– ***Upptäckt och*** övervakning av incidenter på nationell nivå. **[Ändr. 130]**

– Tidiga varningar, larm, meddelanden och informationsspridning till relevanta aktörer om risker och incidenter.

– Svarsåtgärder på incidenter.

– Tillhandahållande av dynamisk risk- och incidentanalys och situationsmedvetenhet.

– Uppbyggnad av bred medvetenhet hos allmänheten om de risker som är förbundna med onlineaktivitet.

– ***Aktivt deltagande i samarbetsnätverk för incidenthanteringsorganisationer på EU-nivå och internationell nivå.*** **[Ändr. 131]**

– Anordnande av kampanjer för nät- och informationssäkerhet.

(b) Incidenthanteringsorganisationen ska bygga upp samarbetsrelationer med den privata sektorn.

(c) För att underlätta samarbete ska incidenthanteringsorganisationen främja antagandet och användningen av gemensam eller standardiserad praxis för

– förfaranden för hantering av incidenter och risker,

– klassificeringssystem för incidenter, risker och information,

– systematiserade kvalitetsmått,

– format för informationsutbyte om risker och incidenter samt konventioner för namngivningssystem.

BILAGA II

Lista över marknadsoperatörer

~~Enligt artikel 3.8 a:~~

~~1. E-handelsplattformar.~~

~~2. Internetbetalningsslussar.~~

~~3. Sociala medier.~~

~~4. Sökmotorer~~

~~5. Molntjänster.~~

~~6. Onlineförsäljning av tillämpningar.~~

~~Enligt artikel 3.8 b~~ **[Ändr. 132]**

1. Energi.

(a) ***Elektricitet***.

~~– El- och gasleverantörer.~~ ***Leverantörer***.

– Systemansvariga för ~~el- och/eller gasdistributionssystem~~ ***distributionssystem*** och återförsäljare till slutkunderna.

~~– Systemansvariga för gasöverföringssystem, naturgaslager och LNG.~~

– Systemansvariga för elöverföringssystem.

(b) Olja.

– Oljeledningar och oljelager.

– Operatörer av oljeproduktion, raffinaderier, bearbetningsanläggningar, lagring och överföring.

(c) Gas.

~~– El- och gasmarknadsaktörer.~~

– ***Leverantörer***.

– Systemansvariga för distributionssystem och återförsäljare till slutkunderna.

– Systemansvariga för gasöverföringssystem, naturgaslager och flytande naturgas – LNG.

– Operatörer av ~~olje- och~~ naturgasproduktion, raffinaderier**,** ***bearbetningsanläggningar, lagring*** och ~~bearbetningsanläggningar~~ ***överföring***.

– Gasmarknadsoperatörer. **[Ändr. 133]**

2. Transporter.

~~– Lufttrafikföretag (gods- och persontransporter).~~

~~– Sjötransportföretag (transportföretag som bedriver persontrafik till havs och längs kuster samt transportföretag som bedriver godstrafik till havs och längs kuster).~~

~~– Järnväg (infrastrukturförvaltare, integrerade företag och järnvägstransportföretag).~~

~~– Flygplatser.~~

~~– Hamnar~~

~~– Trafikstyrning och trafikledning.~~

~~– Logistiska stödtjänster a) lager- och magasineringstjänster, b) godshantering och c) andra stödverksamheter för transporter).~~

(a) Vägtransport

(i) Trafikstyrning och trafikledning.

(ii) Logistiska stödtjänster:

– ***Lager- och magasineringstjänster***.

– ***Godshantering.***

– ***Andra stödverksamheter för transporter***.

(b) Järnvägstransport

(i) Järnväg (infrastrukturförvaltare, integrerade företag och järnvägstransportföretag).

(ii) Trafikstyrning och trafikledning.

(iii) Logistiska stödtjänster:

– *Lager- och magasineringstjänster.*

– *Godshantering.*

– *Andra stödverksamheter för transporter.*

(c) Luftfart.

(i) Lufttrafikföretag (gods- och persontransporter).

(ii) Flygplatser.

(iii) Trafikstyrning och trafikledning.

(iv) Logistiska stödtjänster:

– *Lagertjänster.*

– *Godshantering.*

– *Andra stödverksamheter för transporter.*

(d) Sjötransporter.

(i) Sjötransportföretag (transportföretag som bedriver persontrafik på inre vattenvägar, till havs och längs kuster samt transportföretag som bedriver godstrafik på inre vattenvägar, till havs och längs kuster). **[Ändr. 134]**

3. Bankverksamhet: Kreditinstitut i enlighet med artikel 4.1 i Europaparlamentets och rådets direktiv 2006/48/EG[1].

4. Finansmarknadsinfrastruktur: ~~börser~~ ***reglerade marknader, multilaterala handelsplattformar, organiserade handelsplattformar*** och organisationer för central motpartsclearing. **[Ändr. 135]**

5. Hälso- och sjukvårdssektorn: Hälso- och sjukvårdsmiljöer (inklusive sjukhus och privata kliniker) och andra enheter som tillhandahåller hälso- och sjukvårdsverksamhet.

5a. Vattenproduktion och vattenförsörjning. **[Ändr. 136]**

5b. Försörjningskedjan för livsmedel. **[Ändr. 137]**

5c. Internetknutpunkter. **[Ändr. 138]**

---

[1] Europaparlamentets och rådets direktiv 2006/48/EG av den 14 juni 2006 om rätten att starta och driva verksamhet i kreditinstitut (EUT L 177, 30.6.2006, s. 1)