Europeiska unionens råd

Bryssel den 26 november 2021
(OR. en)

14337/21

Interinstitutionellt ärende:
2020/0359(COD)

CODEC 1541
CSC 416
CSCI 147
CYBER 312
DATAPROTECT 269
JAI 1295
MI 891
TELECOM 435

NOT

från:	Rådets generalsekretariat
till:	Rådet
Föreg. dok. nr:	9583/2/21, 11724/21
Komm. dok. nr:	14150/20
Ärende:	Förslag till Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148 *– Allmän riktlinje*

I. INLEDNING

1. Den 16 december 2020 antog kommissionen förslaget till direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (*det reviderade NIS-direktivet* eller *NIS 2*)[1] i syfte att ersätta det nuvarande direktivet om säkerhet i nätverks- och informationssystem (*NIS-direktivet*)[2].

[1] Förslag till Europaparlamentets och rådets direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148.

[2] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

Förslaget var en av de åtgärder som planeras i EU:s strategi för cybersäkerhet för ett digitalt decennium[3] för att säkerställa att medborgarna och företagen kan dra nytta av tillförlitlig digital teknik.

2. Syftet med förslaget, som grundas på artikel 114 i fördraget om Europeiska unionens funktionssätt (*EUF-fördraget*), är att ytterligare förbättra motståndskraften och incidenthanteringskapaciteten hos offentliga och privata entiteter, behöriga myndigheter och unionen som helhet.

3. I Europaparlamentet är utskottet för industrifrågor, forskning och energi ansvarigt utskott för förslaget. Utskottet antog föredragandens betänkande den 28 oktober 2021.

4. Europeiska ekonomiska och sociala kommittén antog sitt yttrande den 28 april 2021.

5. Den 3 februari 2021 beslutade Coreper att höra Europeiska regionkommittén om förslaget[4]. Hittills har Europeiska regionkommittén inte yttrat sig.

6. Europeiska datatillsynsmannen antog sitt yttrande den 11 mars 2021[5].

7. I sina slutsatser[6] av den 22 mars 2021 om EU:s strategi för cybersäkerhet för ett digitalt decennium noterade rådet det nya förslaget som bygger på NIS-direktivet och upprepade sitt stöd för att stärka och harmonisera nationella cybersäkerhetsramar samt för kontinuerligt samarbete mellan medlemsstaterna.

8. I sina slutsatser av den 21–22 oktober 2021 uppmanade Europeiska rådet till fortsatt arbete med förslaget till reviderat NIS-direktiv.

---

3 Dok. 14133/20.
4 Dok. 5573/21.
5 Yttrande 5/2021 om cybersäkerhetsstrategin och NIS 2.0-direktivet.
6 Dok. 6722/21.

II. ARBETET I RÅDETS FÖRBEREDANDE ORGAN

9. I rådet har förslaget behandlats i övergripande arbetsgruppen för cyberfrågor. Behandlingen inleddes under det portugisiska ordförandeskapet den 19 januari med en noggrann genomläsning av förslaget, och medlemsstaterna gavs möjlighet att ställa frågor, lyfta fram sina främsta farhågor och få detaljerade förklaringar från kommissionen om ändringarna i det reviderade direktivet.

10. Under det portugisiska ordförandeskapet ägnade arbetsgruppen 17 möten åt presentation och genomläsning av förslaget. En lägesrapport om genomläsningen lades fram för rådet (transport, telekommunikation och energi) den 4 juni 2021.

11. Därefter har arbetet fortsatt och intensifierats under det slovenska ordförandeskapet med målet att nå fram till en allmän riktlinje vid mötet i rådet (transport, telekommunikation och energi) den 3 december 2021.Det slovenska ordförandeskapet har ägnat 15 möten åt översynen av NIS 2-förslaget och genomfört många bilaterala diskussioner på alla nivåer.

12. Arbetsgruppen fokuserade först på att omarbeta förslaget vad gäller samspelet mellan NIS 2-direktivet och den sektorsspecifika lagstiftningen samt tillämpningsområdet, framför allt med avseende på offentlig förvaltning, DNS-rotservrar och undantagsklausulen, och därefter vad gäller bland annat sakkunnigbedömningar, jurisdiktion och ömsesidigt bistånd, samordnad information om sårbarheter, databaser med domännamn och registreringsuppgifter samt internationellt samarbete.

13. Ett första kompromissförslag om förslaget till direktiv lades fram den 21 september 2021[7] på grundval av skriftliga kommentarer och icke-officiella dokument från medlemsstaterna samt tidigare kompromissförslag om samspelet mellan NIS 2-direktivet och den sektorsspecifika lagstiftningen och om NIS 2-direktivets tillämpningsområde.

[7] Dok. 12019/21.

14. Den senaste översynen[8] av ordförandeskapets kompromissförslag diskuterades på arbetsgruppsnivå den 22 november 2021. Delegationerna välkomnade i allmänhet kompromisstexten, men några anmälde fortfarande granskningsreservationer eller lämnade synpunkter på delar av kompromissförslaget. Vissa tekniska omformuleringar föreslogs alltjämt för vissa delar av texten.

III. SAKFRÅGOR

15. På grundval av diskussionerna på arbetsgruppsnivå har följande punkter identifierats som de viktigaste politiska frågorna:

a) Tillämpningsområde (artikel 2)

Sedan början av diskussionerna om NIS 2-förslaget har medlemsstaternas främsta farhåga varit den betydande ökningen av antalet entiteter som omfattas av direktivet och i synnerhet införandet av den storleksbaserade regeln, som innebär att alla medelstora och stora entiteter som är verksamma inom sektorerna eller tillhandahåller tjänster som täcks av NIS 2-direktivet omfattas av dess tillämpningsområde. Samtidigt som denna allmänna regel behålls i kompromissförslaget innehåller det ytterligare bestämmelser som ska säkerställa nödvändig proportionalitet, en högre nivå av riskhantering och tydliga kriterier för kritisk betydelse för att fastställa vilka entiteter som omfattas av direktivet. Dessutom innehåller kompromissförslaget särskilda bestämmelser om prioritering av användningen av tillsynsåtgärder enligt en riskbaserad metod.

[8] Dok. 12019/5/21 REV 5.

b) Offentlig förvaltning (artikel 2.2a)

Inkluderandet av offentlig förvaltning i NIS 2-direktivets tillämpningsområde var en mycket omdebatterad fråga, med tanke på att sektorn för offentlig förvaltning är mer differentierad än andra sektorer som omfattas av NIS 2-direktivet. Ordförandeskapet har strävat efter en balanserad strategi som tar hänsyn till särdragen i ramarna för den nationella offentliga förvaltningen och säkerställer att medlemsstaterna har en viss flexibilitet när det gäller att fastställa vilka offentliga förvaltningsentiteter som omfattas av NIS 2-direktivets tillämpningsområde. I kompromisstexten är NIS 2 följaktligen tillämpligt på offentliga förvaltningsentiteter hos nationella regeringar medan medlemsstaterna också kan fastställa att direktivet är tillämpligt på offentliga förvaltningsentiteter på regional och lokal nivå.

c) Undantagsklausulen (artikel 2.3a och 2.3aa)

Medlemsstaterna ville förtydliga undantagsklausulen ytterligare eftersom direktivet inte är tillämpligt på de entiteter som främst bedriver verksamhet på områdena försvar, nationell säkerhet, allmän säkerhet eller brottsbekämpning eller på verksamhet rörande nationell säkerhet eller försvar. Rättsväsende, parlament och centralbanker är också undantagna.

d) Samspelet med den sektorsspecifika lagstiftningen

Medlemsstaterna betonade behovet av anpassning mellan NIS 2-direktivet och den sektorsspecifika lagstiftningen, framför allt förordningen om digital operativ motståndskraft för finanssektorn och direktivet om kritiska enheters resiliens. NIS 2-direktivet, som bör vara utgångspunkten för minimiharmoniseringen av cybersäkerhet, innehåller en särskild artikel om sektorsspecifika unionsakter (artikel 2b). När det gäller samspelet med direktivet om kritiska enheters resiliens säkerställer kompromissförslaget större klarhet om ”allriskstrategin”. Andra viktiga tillägg rör samarbetsarrangemang mellan de behöriga myndigheterna enligt respektive rättsakter.

e) Peer learning (artikel 16)

Med några undantag motsatte sig medlemsstaterna kommissionens införande av obligatoriska sakkunnigbedömningar. Den föreslagna kompromissen säkerställer att den nya peer learning-mekanismen bygger på ömsesidigt förtroende och är en frivillig process som drivs av medlemsstaterna.

f) Jurisdiktion och territorialitet (artikel 24) och ömsesidigt bistånd (artikel 34)

Medlemsstaterna uttryckte oro över konsekvenserna av differentierad jurisdiktion för entiteter inom IKT-sektorn, som kommissionen föreslagit. I kompromisstexten har man klargjort jurisdiktionen på grundval av typen av entiteter och förtydligat formuleringarna om ömsesidigt bistånd.

g) Rapporteringsskyldigheter (artikel 20)

Till följd av medlemsstaternas farhågor om att detta skulle innebära en alltför stor börda för de entiteter som omfattas av NIS 2-direktivet och leda till överrapportering har obligatorisk rapportering för betydande cyberhot uteslutits i kompromisstexten.

IV. SLUTSATS

16. Den 24 november 2021 nådde Coreper en överenskommelse om kompromisstexten enligt bilagan och beslutade att överlämna den till rådet (transport, telekommunikation och energi) så att en allmän riktlinje kan antas.

17. Rådet uppmanas därför att godkänna ordförandeskapets kompromisstext enligt bilagan till denna not och att anta en allmän riktlinje vid mötet den 3 december 2021.

BILAGA

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV

om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) 912/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148

(Text av betydelse för EES)

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[9],

med beaktande av Regionkommitténs yttrande[10],

i enlighet med det ordinarie lagstiftningsförfarandet, och

[9] EUT C , , s. .
[10] EUT C , , s. .

av följande skäl:

(1) Syftet med Europaparlamentets och rådets direktiv (EU) 2016/1148[11] var att bygga upp cybersäkerhetskapaciteten i hela unionen, minska hoten mot nätverks- och informationssystem som används för att tillhandahålla samhällsviktiga tjänster i centrala sektorer och säkerställa kontinuiteten i sådana tjänster när de utsätts för cyberincidenter, och därigenom bidra till att unionens ekonomi och samhälle kan fungera effektivt.

(2) Sedan ikraftträdandet av direktiv (EU) 2016/1148 har det gjorts betydande framsteg med att öka unionens nivå av resiliens på cybersäkerhetsområdet. Översynen av det direktivet har visat att det har fungerat som katalysator för den institutionella och lagstiftningsmässiga strategin för cybersäkerhet i unionen och har banat väg för en betydande attitydförändring. Direktivet har säkerställt fullbordandet av nationella ramar genom att fastställa nationella strategier för [...] **säkerhet i nätverks- och informationssystem**, inrätta nationell kapacitet och genomföra lagstiftningsåtgärder som omfattar viktig infrastruktur och viktiga aktörer som identifierats av varje medlemsstat. Det har också bidragit till samarbete på unionsnivå genom inrättandet av samarbetsgruppen[12] och [...] nätverk**et** av nationella it-incidentcentrum (*CSIRT-nätverket*)[13]. Trots dessa framsteg har översynen av direktiv (EU) 2016/1148 avslöjat inneboende brister som hindrar det från att effektivt hantera samtida och framväxande utmaningar på cybersäkerhetsområdet.

---

11 Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (EUT L 194, 19.7.2016, s. 1).

12 Artikel 11 i direktiv (EU) 2016/1148.

13 Artikel 12 i direktiv (EU) 2016/1148.

(3) Nätverks- och informationssystem har utvecklats till att vara ett centralt inslag i vardagslivet i och med den snabba digitala omställningen och sammankopplingen av samhället, vilket även gäller vid gränsöverskridande utbyten. Denna utveckling har lett till en expansion av hotbilden mot cybersäkerheten, vilket medfört nya utmaningar som kräver anpassade, samordnade och innovativa svarsåtgärder i alla medlemsstater. Cyberincidenter, som blir att fler och mer omfattande, sofistikerade och vanliga och får allt större inverkan, utgör ett allvarligt hot mot nätverks- och informationssystemens funktion. Därför kan sådana cyberincidenter hindra utövandet av ekonomisk verksamhet på den inre marknaden, generera ekonomiska förluster, undergräva användarnas förtroende och orsaka allvarlig skada för unionens ekonomi och samhälle. Beredskap och ändamålsenlighet på cybersäkerhetsområdet är därför nu viktigare än någonsin för att den inre marknaden ska kunna fungera väl.

(4) Den rättsliga grunden för direktiv (EU) 2016/1148 var artikel 114 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget), vars mål är att upprätta den inre marknaden och säkerställa dess funktion genom att förbättra åtgärderna för tillnärmning av nationella regler. De cybersäkerhetskrav som åläggs entiteter som tillhandahåller tjänster eller ekonomiskt relevant verksamhet varierar avsevärt mellan medlemsstaterna vad gäller typen av krav, kravens utförlighet och tillsynsmetoden. Dessa skillnader medför extra kostnader och gör det svårt för företagen att erbjuda varor och tjänster över gränserna. Krav som ställs av en medlemsstat och som skiljer sig från eller rentav står i strid med krav som ställs av en annan medlemsstat, kan väsentligt påverka dessa gränsöverskridande verksamheter.

Det är dessutom sannolikt att illa utformade eller otillräckligt genomförda cybersäkerhet**såtgärder** [...] i en medlemsstat kommer att få återverkningar för cybersäkerhetsnivån i andra medlemsstater, särskilt med tanke på det intensiva utbytet över gränserna. Översynen av direktiv (EU) 2016/1148 har visat på stora skillnader i genomförandet från en medlemsstat till en annan, även vad gäller dess tillämpningsområde, då avgränsningen av detta i stor utsträckning har överlåtits på medlemsstaterna. Direktiv (EU) 2016/1148 gav också medlemsstaterna mycket stort utrymme för skönsmässig bedömning vad gäller genomförandet av de incidentrapporteringsskyldigheter som anges i det. Dessa skyldigheter genomfördes därför på väsentligt skilda sätt på nationell nivå. Liknande skillnader i genomförandet uppstod i fråga om direktivets bestämmelser om tillsyn och efterlevnadskontroll.

(5) Alla dessa skillnader medför en fragmentering av den inre marknaden och kan ha en potentiellt skadlig inverkan på dess funktion, vilket påverkar i synnerhet tillhandahållandet av tjänster över gränserna och nivån av cybersäkerhetsresiliens till följd av tillämpningen av olika [...] **åtgärder**. Direktivets mål är att undanröja dessa stora skillnader mellan medlemsstater, särskilt genom att föreskriva minimiregler för ett fungerande samordnat regelverk genom fastställande av mekanismer för effektivt samarbete mellan de ansvariga myndigheterna i varje medlemsstat, genom uppdatering av förteckningen över sektorer och verksamheter som omfattas av skyldigheter vad gäller cybersäkerhet och genom föreskrivande av effektiva rättsmedel och sanktioner, vilket är avgörande för att upprätthålla en effektiv kontroll av att dessa skyldigheter efterlevs. Därför bör direktiv (EU) 2016/1148 upphävas och ersättas av det här direktivet.

(6) [...] Medlemsstaterna **bör kunna** vidta de åtgärder som är nödvändiga för att skydda deras väsentliga säkerhetsintressen, upprätthålla allmän ordning och säkerhet och möjliggöra utredning, upptäckt och lagföring av brott [...]. […] **Direktivet bör inte tillämpas på vissa offentliga eller privata entiteter som bedriver verksamhet på dessa områden. Det bör inte heller tillämpas på entiteternas verksamhet inom dessa områden. Dessutom** bör ingen medlemsstat vara förpliktad att lämna information vars avslöjande den anser strida mot sina väsentliga säkerhetsintressen. [...] Nationella regler [...] **eller** unionsregler till skydd för säkerhetsklassificerade uppgifter, sekretessavtal, eller informella sekretessavtal såsom Traffic Light Protocol[14], är relevanta i detta sammanhang.

(6a) Unionslagstiftningen om skydd av personuppgifter och skydd för privatlivet är tillämplig på all behandling av personuppgifter inom ramen för detta direktiv. Framför allt påverkar detta direktiv inte tillämpningen av förordning (EU) 2016/679 och Europaparlamentets och rådets direktiv 2002/58/EG och bör därför i synnerhet inte påverka uppgifterna och befogenheterna för de oberoende tillsynsmyndigheter som är behöriga att övervaka efterlevnaden av respektive unionslagstiftning om dataskydd.

---

14 Traffic Light Protocol (TLP) kan användas av någon som delar information för att informera sin publik om eventuella begränsningar av vidarespridning av denna information. Det används i de flesta CSIRT-grupper och av vissa informations- och analyscentraler.

(7) Med upphävandet av direktiv (EU) 2016/1148 bör tillämpningsområdet med avseende på olika sektorer utvidgas till en större del av ekonomin mot bakgrund av beaktandena i skälen 4–6. Täckningen av sektorer enligt direktiv (EU) 2016/1148 bör därför utvidgas så att den ger en omfattande täckning av sektorer och tjänster som är av avgörande betydelse för viktiga samhälleliga och ekonomiska verksamheter på den inre marknaden. Reglerna bör inte vara olika beroende på om entiteterna är leverantörer av samhällsviktiga tjänster eller leverantörer av digitala tjänster. En sådan differentiering har visat sig vara inaktuell eftersom den inte återspeglar den faktiska betydelse som dessa sektorer och tjänster har för samhälleliga och ekonomiska verksamheter på den inre marknaden.

(8) I enlighet med direktiv (EU) 2016/1148 hade medlemsstaterna ansvaret för att fastställa vilka entiteter som uppfyllde kriterierna för att klassificeras som leverantörer av samhällsviktiga tjänster (identifieringsförfarande). För att begränsa de stora skillnaderna mellan medlemsstater i detta avseende och säkerställa rättslig säkerhet vad gäller riskhanteringskraven och rapporteringsskyldigheterna för alla relevanta entiteter, bör det fastställas ett enhetligt kriterium för vilka entiteter som ska omfattas av tillämpningsområdet för detta direktiv. Kriteriet bör bestå i tillämpningen av en storleksbaserad regel genom vilken alla medelstora och stora företag, enligt definitionen i kommissionens rekommendation 2003/361/EG[15], som är verksamma i de sektorer eller tillhandahåller den typ av tjänster som omfattas av detta direktiv också omfattas av dess tillämpningsområde. [...]

---

15 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).

(8a) För att säkerställa en tydlig översikt över de entiteter som omfattas av detta direktivs tillämpningsområde bör medlemsstaterna kunna inrätta nationella mekanismer för självanmälan som kräver att de entiteter som omfattas av detta direktiv – till de behöriga myndigheterna enligt detta direktiv eller till de organ som utsetts för detta ändamål av medlemsstaterna – åtminstone lämnar in namn, adress och kontaktuppgifter samt information om vilken sektor de är verksamma inom eller vilken typ av tjänst de tillhandahåller och, i tillämpliga fall, en förteckning över de medlemsstater där entiteten tillhandahåller sina tjänster. Om det finns register på nationell nivå kan medlemsstaterna besluta om lämpliga mekanismer som gör det möjligt att identifiera de entiteter som omfattas av detta direktiv.

(9) [...] **Mikro**entiteter **eller** små entiteter [...] som uppfyller vissa kriterier som visar att de spelar en nyckelroll i medlemsstaternas ekonomier eller samhällen eller för särskilda sektorer eller typer av tjänster, bör emellertid också omfattas av detta direktiv. Medlemsstaterna bör ha ansvaret för att [...] till kommissionen **åtminstone** lämna [...] **relevant information om antalet identifierade entiteter, vilken sektor de tillhör eller vilken typ av tjänst de tillhandahåller och de särskilda kriterier enligt vilka de identifierades. Medlemsstaterna kan också, om det är tillåtet i enlighet med de nationella säkerhetsbestämmelserna, besluta att lämna namnen på dessa entiteter till kommissionen.**

(9a) Offentliga förvaltningsentiteter som bedriver verksamhet på områdena nationell säkerhet, försvar, allmän säkerhet och brottsbekämpning samt rättsväsende, parlament och centralbanker omfattas inte av detta direktivs tillämpningsområde. Vid tillämpning av detta direktiv bör entiteter med lagstiftningsbehörighet inte anses bedriva verksamhet på brottsbekämpningsområdet, och de är därför inte undantagna från detta direktivs tillämpningsområde på dessa grunder. Dessutom omfattas inte offentliga förvaltningsentiteter hos nationella regeringar som inrättats gemensamt med ett tredjeland i enlighet med ett internationellt avtal av detta direktivs tillämpningsområde.

(9aa) Medlemsstaterna bör kunna fastställa att entiteter som före detta direktivs ikraftträdande har identifierats som leverantörer av samhällsviktiga tjänster i enlighet med direktiv (EU) 2016/1148 ska betraktas som väsentliga entiteter.

(9aaa) Detta direktiv är inte tillämpligt på medlemsstaternas diplomatiska och konsulära beskickningar utomlands och på deras IKT-infrastruktur som används av sådana beskickningar i den mån sådan infrastruktur är belägen utomlands eller är i drift för användare utomlands.

(10) Kommissionen kan, i samarbete med samarbetsgruppen, utfärda riktlinjer om genomförandet av de kriterier som ska tillämpas på mikroföretag och små företag.

(11) [...] **Entiteter som omfattas av detta direktivs tillämpningsområde bör delas in i två kategorier – väsentliga och viktiga – som beaktar nivån av kritisk betydelse för sektorn eller den typ av tjänster de tillhandahåller samt deras storlek. I detta avseende bör vederbörlig hänsyn också tas till eventuella relevanta sektoriella riskbedömningar eller, i tillämpliga fall, vägledning från behöriga myndigheter.** Väsentliga och viktiga entiteter bör omfattas av [...] riskhanteringskraven och rapporteringsskyldigheterna. Tillsyns- och sanktionssystemen bör dock differentieras mellan dessa två kategorier i syfte att säkerställa en rättvis balans mellan **riskbaserade** krav och skyldigheter å ena sidan och den administrativa börda som följer av tillsynen av fullgörandet å den andra.

(12) **I detta direktiv fastställs referensscenariot för riskhanteringsåtgärder och rapporteringsskyldigheter för cybersäkerhet inom alla sektorer som omfattas av dess tillämpningsområde. För att undvika fragmentering av cybersäkerhetsbestämmelserna i unionsrättsakter bör kommissionen, när ytterligare sektorsspecifika bestämmelser om** riskhanteringsåtgärder **och rapporteringsskyldigheter för cybersäkerhet anses nödvändiga för att säkerställa en hög cybersäkerhetsnivå, bedöma om sådana bestämmelser skulle kunna fastställas i en genomförandeakt inom ramen för den befogenhet som föreskrivs i detta direktiv. Om sådana akter inte är lämpliga för detta ändamål skulle** sektorsspecifik lagstiftning **kunna** bidra till att säkerställa **en** hög cybersäkerhetsnivå [...], samtidigt som den fullt ut beaktar **de berörda** [...] sektorernas särdrag och komplexitet. **Anledningen till att en genomförandeakt inom ramen för den befogenhet som föreskrivs i detta direktiv inte var lämplig bör förklaras i den sektorsspecifika lagstiftningen. Samtidigt bör sådana sektorsspecifika bestämmelser i unionsrättsakter vederbörligen beakta behovet av en heltäckande och harmoniserad cybersäkerhetsram.** [...] Detta [...] påverkar inte de befintliga genomförandebefogenheter som har tilldelats [...] kommissionen med avseende på ett antal sektorer, däribland transport och energi.

(12a) Om en sektorsspecifik unionsrättsakt **innehåller bestämmelser** [...] **om** att väsentliga eller viktiga entiteter ska anta **åtgärder som har minst samma verkan som de skyldigheter som fastställs i detta direktiv i fråga om** hantering av cybersäkerhetsrisker [...] **och skyldigheter** att anmäla **betydande** incidenter eller betydande cyberhot [...] bör dessa sektorsspecifika bestämmelser, **inbegripet om tillsyn och efterlevnadskontroll**, tillämpas. **När man fastställer om de skyldigheter som föreskrivs i de sektorsspecifika bestämmelserna i en unionsrättsakt har samma verkan bör man beakta följande aspekter: i) Riskhanteringsåtgärderna för cybersäkerhet bör bestå av lämpliga och proportionella tekniska och organisatoriska åtgärder för att hantera riskerna för säkerheten i de nätverks- och informationssystem som de berörda entiteterna använder vid tillhandahållandet av sina tjänster och bör minst omfatta alla de delar som fastställs i detta direktiv. ii) Skyldigheten att anmäla betydande incidenter och cyberhot bör åtminstone motsvara de skyldigheter som fastställs i detta direktiv vad gäller innehåll, format och tidsfrister för anmälningarna. iii) Rapporteringsmetoderna för entiteterna och de berörda myndigheterna enligt de sektorsspecifika unionsrättsakterna bör åtminstone motsvara de krav som fastställs i detta direktiv vad gäller innehåll, format och tidsfrister och bör ta hänsyn till CSIRT-enheternas roll. iv) Kraven avseende gränsöverskridande samarbete för de berörda myndigheterna bör åtminstone motsvara de krav som fastställs i detta direktiv. Om de sektorsspecifika bestämmelserna i en unionsrättsakt inte omfattar alla entiteter inom en viss sektor som omfattas av detta direktivs tillämpningsområde, bör de relevanta bestämmelserna i detta direktiv fortsätta att tillämpas på de entiteter som inte omfattas av dessa sektorsspecifika bestämmelser.**

(12aa) Kommissionen **bör regelbundet se över tillämpningen av kravet om samma verkan i förhållande till sektorsspecifika bestämmelser i unionsrättsakter** [...]. **Kommissionen bör samråda med samarbetsgruppen när den förbereder den periodiska översynen.**

(12aaa) Framtida sektorsspecifika unionsrättsakter bör ta vederbörlig hänsyn till definitionerna i artikel 4 i detta direktiv och den ram för tillsyn och efterlevnadskontroll som fastställs i kapitel VI i detta direktiv.

(12ab) Om sektorsspecifika bestämmelser i unionsrättsakter kräver att väsentliga eller viktiga entiteter antar åtgärder med minst samma verkan som de rapporteringsskyldigheter som fastställs i detta direktiv, bör överlappande rapporteringsskyldigheter undvikas och samstämmig och ändamålsenlig hantering av anmälningar om cyberhot eller cyberincidenter säkerställas. För detta ändamål kan dessa sektorsspecifika bestämmelser ge medlemsstaterna möjlighet att inrätta en gemensam, automatisk och direkt rapporteringsmekanism för anmälan av betydande incidenter och cyberhot både till de myndigheter vars uppgifter anges i respektive sektorsspecifika bestämmelser och till de behöriga myndigheter, inbegripet den gemensamma kontaktpunkten och CSIRT-enheterna i förekommande fall, som ansvarar för de cybersäkerhetsuppgifter som föreskrivs i detta direktiv eller en mekanism som säkerställer ett systematiskt och omedelbart informationsutbyte och samarbete mellan de berörda myndigheterna och CSIRT-enheterna när det gäller hanteringen av sådana anmälningar. För att förenkla rapporteringen och genomföra den gemensamma, automatiska och direkta rapporteringsmekanismen får medlemsstaterna, i enlighet med den sektorsspecifika lagstiftningen, använda den gemensamma kontaktpunkt som de inrättar i enlighet med artikel 11.5a i detta direktiv. För att säkerställa harmonisering bör rapporteringsskyldigheterna i de sektorsspecifika unionsrättsakterna anpassas till de skyldigheter som anges i detta direktiv. Medlemsstaterna kan fastställa att de behöriga myndigheterna enligt detta direktiv eller de nationella CSIRT-enheterna är mottagare av rapporteringen, i enlighet med den sektorsspecifika lagstiftningen.

(13) Europaparlamentets och rådets förordning XXXX/XXXX bör betraktas som en sektorsspecifik unionsrättsakt vid tillämpning av detta direktiv med avseende på entiteter i den finansiella sektorn. Bestämmelserna i förordning XXXX/XXXX rörande riskhanteringsåtgärder för informations- och kommunikationsteknik (IKT), hantering av IKT-relaterade incidenter, särskilt incidentrapportering, samt om rapportering om testning av digital operativ motståndskraft, arrangemang för informationsutbyte och IKT-tredjepartsrisk bör tillämpas i stället för dem som fastställs i detta direktiv. Medlemsstaterna bör därför inte tillämpa detta direktivs bestämmelser om riskhanterings- och rapporteringsskyldigheter beträffande cybersäkerhet [...] och om tillsyn och efterlevnadskontroll av [...] finansiella entiteter som omfattas av förordning XXXX/XXXX. Det är samtidigt viktigt att upprätthålla starka förbindelser och informationsutbyte med finanssektorn inom ramen för detta direktiv. Därför gör förordning XXXX/XXXX det möjligt för […] de europeiska tillsynsmyndigheterna för finanssektorn och de nationella behöriga myndigheterna enligt förordning XXXX/XXXX [...] att delta i […] **arbetet** inom ramen för samarbetsgruppen, och att utbyta information och samarbeta med de gemensamma kontaktpunkter som utsetts enligt detta direktiv [...] **samt** med de nationella CSIRT-enheterna. De behöriga myndigheterna enligt förordning XXXX/XXXX bör även översända uppgifter om större IKT-relaterade incidenter **och betydande cyberhot** till de gemensamma kontaktpunkter**, de behöriga myndigheter eller de nationella CSIRT-enheter** som utsetts enligt detta direktiv. **Detta kan uppnås genom automatisk och direkt vidarebefordran av incidentanmälningar eller en gemensam rapporteringsplattform.** Vidare bör medlemsstaterna fortsätta att inkludera finanssektorn i sina strategier för cybersäkerhet, och de nationella CSIRT-enheterna kan inbegripa finanssektorn i sin verksamhet.

(13a) För att undvika luckor mellan och överlappningar av de cybersäkerhetsskyldigheter som åläggs entiteter inom luftfartssektorn enligt punkt 2 a i bilaga I bör de nationella myndigheter som utsetts enligt Europaparlamentets och rådets förordningar (EG) nr 300/2008[16] och (EU) 2018/1139[17] och de behöriga myndigheterna enligt detta direktiv samarbeta när det gäller genomförandet av riskhanteringsåtgärderna för cybersäkerhet och tillsynen av dessa åtgärder på nationell nivå. En entitets fullgörande av riskhanteringsåtgärderna för cybersäkerhet enligt detta direktiv [...] kan av de nationella myndigheter som utsetts enligt förordningarna (EG) nr 300/2008 och (EU) 2018/1139 anses uppfylla kraven i dessa förordningar och de relevanta delegerade akter och genomförandeakter som antagits i enlighet med dessa förordningar.

---

16 Europaparlamentets och rådets förordning (EG) nr 300/2008 av den 11 mars 2008 om gemensamma skyddsregler för den civila luftfarten och om upphävande av förordning (EG) nr 2320/2002 (EUT L 97, 9.4.2008, s. 72).

17 Europaparlamentets och rådets förordning (EU) 2018/1139 av den 4 juli 2018 om fastställande av gemensamma bestämmelser på det civila luftfartsområdet och inrättande av Europeiska unionens byrå för luftfartssäkerhet, och om ändring av Europaparlamentets och rådets förordningar (EG) nr 2111/2005, (EG) nr 1008/2008, (EU) nr 996/2010, (EU) nr 376/2014 och direktiv 2014/30/EU och 2014/53/EU, samt om upphävande av Europaparlamentets och rådets förordningar (EG) nr 552/2004 och (EG) nr 216/2008 och rådets förordning (EEG) nr 3922/91 (EUT L 212, 22.8.2018, s. 1).

(14) Med beaktande av kopplingarna mellan cybersäkerhet och entiteters fysiska säkerhet bör man säkerställa samstämmighet mellan Europaparlamentet och rådets direktiv (EU) XXX/XXX och detta direktiv. För att uppnå detta bör medlemsstaterna säkerställa att kritiska entiteter **[**och med dessa likvärdiga entiteter**]** enligt direktiv (EU) XXX/XXX anses vara väsentliga entiteter enligt detta direktiv. Medlemsstaterna bör även säkerställa att deras strategier för cybersäkerhet tillhandahåller en politisk ram för ökat samarbete mellan den behöriga myndigheten enligt detta direktiv och den behöriga myndigheten enligt direktiv (EU) XXX/XXX när det gäller informationsutbyte om incidenter och cyberhot och utövandet av tillsynsuppgifter. **De behöriga** [...] myndigheterna enligt båda direktiven bör samarbeta och utbyta information, särskilt när det gäller identifiering av kritiska entiteter, cyberhot, cybersäkerhetsrisker och incidenter **samt icke-cyberrelaterade risker, hot och incidenter** som påverkar kritiska entiteter **[**eller entiteter som är likvärdiga med kritiska entiteter**]**, [...] **inbegripet** cybersäkerhetsåtgärder och fysiska åtgärder som vidtas av kritiska entiteter och resultatet av den tillsynsverksamhet som bedrivs med avseende på dessa entiteter. **För att effektivisera tillsynsverksamheten mellan de behöriga myndigheter som utsetts enligt båda direktiven och för att minimera den administrativa bördan för de berörda entiteterna bör de behöriga myndigheterna dessutom sträva efter att harmonisera mallarna för incidentanmälningar och tillsynsförfarandena.** [...] **Vid behov kan** de behöriga myndigheterna enligt direktiv (EU) XXXX/XXXX [...] **begära** att de behöriga myndigheterna enligt det här direktivet [...] får utöva sina tillsyns- och efterlevnadskontrollbefogenheter [...] **avseende** en väsentlig entitet som identifierats som kritisk. [...]

(14a) Entiteter som tillhör sektorn för digital infrastruktur är i huvudsak baserade på nätverks- och informationssystem, och därför bör de skyldigheter som åläggs dessa entiteter genom det här direktivet på ett övergripande sätt omfatta den fysiska säkerheten i sådana system som en del av deras riskhanterings- och rapporteringsskyldigheter för cybersäkerhet. Eftersom dessa frågor omfattas av det här direktivet är de skyldigheter som fastställs i kapitlen III–VI i direktiv (EU) XXX/XXX [direktivet om kritiska enheters resiliens] inte tillämpliga på sådana entiteter.

(15) Att upprätthålla och bevara ett tillförlitligt, resilient och säkert domännamnssystem (DNS) är en viktig faktor för att upprätthålla internets integritet och är avgörande för en kontinuerlig och stabil drift, vilket den digitala ekonomin och samhället är beroende av. Därför bör detta direktiv tillämpas på leverantörer av DNS-tjänster längs hela DNS-**leverans- och** DNS-uppslagningskedjan **som är betydelsefulla för den inre marknaden,** inbegripet [...] **registreringsenheter** för toppdomäner[…], **entiteter som tillhandahåller domännamnsregistreringstjänster, operatörer av** auktoritativa namnservrar för domännamn och **operatörer av** rekursiva resolvrar. **Termen *leverantör av DNS-tjänster* bör inte tillämpas på DNS-tjänster som den berörda entiteten och dess anknutna entiteter utför för egna ändamål. De cybersäkerhetsskyldigheter som följer av detta direktiv för denna kategori av leverantörer är strikt begränsade till riskhanteringsåtgärder för och rapportering om cybersäkerhet och påverkar därför inte flerpartssamfundets styrning av det globala DNS.**

(16) Molntjänster bör omfatta tjänster som möjliggör administration av beställtjänster och bred fjärråtkomst till en skalbar och elastisk pool av delbara och distribuerade dataresurser. Sådana dataresurser omfattar resurser såsom nätverk, servrar eller annan infrastruktur, operativsystem, programvara, lagring, applikationer och tjänster. **Tjänstemodellerna för molntjänster omfattar bland annat infrastruktur som en tjänst, plattform som en tjänst, program som nättjänst och nätverk som en tjänst.** Distribueringsmodellerna för molntjänster bör omfatta privat moln, gemensamt moln, offentligt moln och hybridmoln. De ovannämnda tjänste- och distribueringsmodellerna har samma innebörd som termerna tjänste- och distribueringsmodeller som definieras i standarden ISO/IEC 17788:2014. Molnanvändarens kapacitet att ensidigt självständigt tillhandahålla datorkapacitet, såsom servertid eller nätlagring, utan någon mänsklig medverkan från leverantören av molntjänster kan beskrivas som beställtjänster. Termen bred fjärråtkomst används för att beskriva att molnkapaciteten tillhandahålls över nätet och nås genom mekanismer som främjar användning av heterogena tunna eller tjocka klientplattformar (däribland mobiltelefoner, surfplattor, bärbara datorer och arbetsstationer).

Termen skalbar avser dataresurser som leverantören av molntjänster fördelar på ett flexibelt sätt, oberoende av resursernas geografiska läge, för att hantera fluktuationer i efterfrågan. Termen elastisk pool används för att beskriva dataresurser som avsätts och utnyttjas beroende på efterfrågan för att tillgängliga resurser snabbt ska kunna utökas och minskas i takt med arbetsbördan. Termen delbar används för att beskriva dataresurser som tillhandahålls flera användare som delar en gemensam åtkomst till tjänsten där behandlingen genomförs separat för varje användare, även om tjänsten tillhandahålls från samma elektroniska utrustning. Termen distribuerad används för att beskriva de dataresurser som finns på olika nätverksanslutna datorer eller enheter och som kommunicerar och samordnar sig sinsemellan genom meddelandepassning.

(17) Med tanke på framväxten av innovativ teknik och nya affärsmodeller, förväntas nya molntjänster och nya servicemodeller att uppstå på marknaden som svar på kundernas föränderliga behov. I detta sammanhang kan molntjänster levereras i en mycket distribuerad form, ännu närmare den plats där data genereras eller samlas in, och därmed övergå från den traditionella modellen till en mycket distribuerad modell (edge computing).

(18) Tjänster som erbjuds av leverantörer av datacentraltjänster tillhandahålls inte alltid i form av molntjänster. Därför ingår inte datacentraler alltid i en molninfrastruktur. För att hantera alla risker för säkerheten i nätverks- och informationssystem bör detta direktiv även omfatta leverantörer av datacentraltjänster som inte är molnbaserade. Vid tillämpningen av detta direktiv bör datacentraltjänstomfatta strukturer, eller grupper av strukturer, avsedda för centraliserad inkvartering, sammankoppling och drift av it- och nätutrustning som tillhandahåller datalagrings-, databehandlings- och datatransporttjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll. Termen datacentraltjänst är inte tillämplig på interna datacentraler som ägs och drivs för egen räkning av den berörda entiteten.

(19) Tillhandahållare av posttjänster i den mening som avses i Europaparlamentets och rådets direktiv 97/67/EG[18], [...] **inklusive** tillhandahållare av budtjänster, bör omfattas av detta direktiv om de tillhandahåller minst ett led i postleveranskedjan, särskilt insamling, sortering och distribution, inklusive upphämtning. Transporttjänster som inte utförs i samband med något av dessa steg bör inte omfattas av tillämpningsområdet för posttjänster.

---

18 Europaparlamentets och rådets direktiv 97/67/EG av den 15 december 1997 om gemensamma regler för utvecklingen av gemenskapens inre marknad för posttjänster och för förbättring av kvaliteten på tjänsterna (EGT L 15, 21.1.1998, s. 14).

(20) Dessa växande ömsesidiga beroendeförhållanden är resultatet av ett allt mer gränsöverskridande nätverk av tillhandahållande av tjänster, med ett inbördes beroende, som använder central infrastruktur över hela unionen inom sektorerna energi, transport, digital infrastruktur, dricks- och avloppsvatten, hälso- och sjukvård, vissa aspekter av offentlig förvaltning, samt rymden i den mån tillhandahållandet av vissa tjänster som är beroende av markbaserad infrastruktur som ägs, förvaltas och drivs av medlemsstater eller privata parter berörs; därför omfattas inte infrastruktur som ägs, förvaltas eller drivs av unionen eller på unionens vägnar som en del av dess rymdprogram. Dessa beroendeförhållanden innebär att alla störningar, även sådana som inledningsvis är begränsade till en entitet eller sektor, kan få dominoeffekter i vidare bemärkelse, vilket kan leda till långtgående och långvariga effekter på tillhandahållandet av tjänster på hela den inre marknaden. Covid-19-pandemin har visat hur sårbara våra alltmer av varandra beroende samhällen är för risker med låg sannolikhet.

(**20a**) **I syfte att uppnå och upprätthålla en hög cybersäkerhetsnivå bör de nationella strategier för cybersäkerhet som krävs enligt detta direktiv bestå av enhetliga ramar som möjliggör styrning på cybersäkerhetsområdet. Dessa strategier kan bestå av ett eller flera dokument av lagstiftningskaraktär eller av annan karaktär.**

(21) Mot bakgrund av skillnaderna i nationella förvaltningsstrukturer och för att skydda befintliga sektorsspecifika arrangemang eller unionens tillsyns- och regleringsorgan, bör medlemsstaterna kunna utse mer än en nationell behörig myndighet med ansvar för att utföra uppgifter som rör säkerheten i de nätverks- och informationssystem som används av väsentliga och viktiga entiteter enligt detta direktiv. Medlemsstaterna bör kunna tilldela en befintlig myndighet denna roll.

(22) För att underlätta gränsöverskridande samarbete och kommunikation mellan myndigheter och för att göra det möjligt att genomföra detta direktiv på ett effektivt sätt måste varje medlemsstat utse en nationell gemensam kontaktpunkt med ansvar för samordningen av frågor angående säkerhet i nätverks- och informationssystem och gränsöverskridande samarbete på unionsnivå.

(23) Behöriga myndigheter eller CSIRT-enheter bör motta anmälningar om incidenter från entiteter på ett ändamålsenligt och effektivt sätt**, även i syfte att vid behov möjliggöra en snabb reaktion på incidenter och lämna svar till den anmälande entiteten**. Den gemensamma kontaktpunkten bör ges i uppgift att vidarebefordra incidentanmälningar till de gemensamma kontaktpunkterna i andra berörda medlemsstater. [...]

(23a) De sektorsspecifika unionsrättsakter som kräver riskhanteringsåtgärder eller rapporteringsskyldigheter för cybersäkerhet med minst samma verkan som de åtgärder och skyldigheter som fastställs i detta direktiv kan föreskriva att deras utsedda behöriga myndigheter utövar sina tillsyns- och efterlevnadskontrollbefogenheter avseende sådana åtgärder eller skyldigheter med bistånd av de behöriga myndigheter som utsetts i enlighet med detta direktiv. De berörda behöriga myndigheterna kan upprätta samarbetsarrangemang för detta ändamål. Sådana samarbetsarrangemang kan bland annat specificera förfarandena för samordning av tillsynsverksamheten, inbegripet förfarandena för utredningar och inspektioner på plats i enlighet med den nationella lagstiftningen och en mekanism för utbyte av relevant information mellan de behöriga myndigheterna om tillsyn och efterlevnadskontroll, inklusive tillgång till cyberrelaterad information som begärts av de behöriga myndigheter som utsetts i enlighet med detta direktiv.

(24) Medlemsstaterna bör ha både den tekniska och organisatoriska kapacitet som krävs för att förebygga, upptäcka, vidta åtgärder mot och begränsa effekterna av incidenter och risker vad gäller nätverks- och informationssystem. Medlemsstater bör därför säkerställa att de har väl fungerande CSIRT-enheter, även kallade incidenthanteringsorganisationer (Computer Emergency Response Teams, Cert), som uppfyller grundläggande krav i syfte att garantera effektiv och kompatibel kapacitet att hantera incidenter och risker och säkerställa ett effektivt samarbete på unionsnivå. För att stärka förtroendeförhållandet mellan entiteterna och CSIRT-enheterna, i fall där en CSIRT-enhet är en del av den behöriga myndigheten, [...] **får** medlemsstaterna överväga funktionell åtskillnad mellan de operativa uppgifter som utförs av CSIRT-enheten, särskilt när det gäller informationsutbyte och stöd till entiteterna, och de behöriga myndigheternas tillsynsverksamhet.

(25) Vad gäller personuppgifter bör CSIRT-enheterna, i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679[19], på en entitets vägnar och begäran inom ramen för detta direktiv tillhandahålla en proaktiv skanning av de nätverks- och informationssystem som används för att tillhandahålla deras tjänster. **I tillämpliga fall** bör medlemsstaterna sträva efter att säkerställa en lika hög nivå av teknisk kapacitet hos alla sektoriella CSIRT-enheter. Medlemsstaterna får begära bistånd från Europeiska unionens cybersäkerhetsbyrå (Enisa) vid inrättandet av nationella CSIRT-enheter.

(26) Med tanke på vikten av internationellt samarbete på området cybersäkerhet, bör CSIRT-enheterna kunna delta i internationella samarbetsnätverk utöver det CSIRT-nätverk som inrättas genom detta direktiv. **Därför skulle CSIRT-enheterna och de behöriga myndigheterna kunna utbyta information, inbegripet personuppgifter, med CSIRT-enheterna i tredjeländer eller deras myndigheter i syfte att utföra sina uppgifter i enlighet med förordning (EU) 2016/679. Om ett beslut om adekvat skyddsnivå enligt artikel 45 i förordning (EU) 2016/679 inte har antagits eller om lämpliga skyddsåtgärder enligt artikel 46 i den förordningen inte har införts, kan det utbyte av personuppgifter som anses nödvändigt för att minska betydande cyberhot och reagera på en pågående betydande incident anses utgöra ett viktigt skäl som rör allmänintresset i den mening som avses i artikel 49.1 d i förordning (EU) 2016/679.**

---

19 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

(27) I enlighet med bilagan till kommissionens rekommendation (EU) 2017/1548 om samordnade insatser vid storskaliga cyberincidenter och cyberkriser på alla relevanta nivåer[20], bör en storskalig cyberincident anses vara en incident som påverkar två eller flera medlemsstater eller som leder till störningar som är så omfattande att den berörda medlemsstaten inte kan hantera dem på egen hand. Beroende på orsak och verkan kan storskaliga incidenter eskalera och förvandlas till fullt utvecklade kriser som hindrar den inre marknaden från att fungera korrekt. Med beaktande av sådana incidenters stora omfattning och, i de flesta fall, gränsöverskridande karaktär, bör medlemsstater och relevanta EU-institutioner, -organ och -byråer samarbeta på teknisk, operativ och politisk nivå i syfte att på lämpligt sätt samordna insatserna i hela unionen.

(28) Eftersom utnyttjandet av sårbarheter i nätverks- och informationssystem kan orsaka betydande störningar och skada, är snabb identifiering och snabbt åtgärdande av dessa sårbarheter en viktig faktor för att minska cybersäkerhetsrisken. Entiteter som utvecklar **eller administrerar** sådana system bör därför inrätta lämpliga förfaranden för att hantera sårbarheter när de upptäcks. Eftersom sårbarheter ofta upptäcks och rapporteras (meddelas) av tredjeparter (rapporterande entiteter) bör tillverkaren eller leverantören av IKT-produkter eller IKT-tjänster även införa nödvändiga förfaranden för att motta sårbarhetsinformation från tredjeparter. I detta avseende ger standarderna ISO/IEC 30111 och ISO/IEC [...] **29147** vägledning om sårbarhetshantering respektive meddelande av information om sårbarheter. När det gäller meddelande av information om sårbarheter är samordning mellan rapporterande entiteter och tillverkare eller leverantörer av IKT-produkter eller IKT-tjänster särskilt viktig. Samordnad information om sårbarheter specificerar en strukturerad process genom vilken sårbarheter rapporteras till organisationer på ett sätt som gör det möjligt för organisationen att diagnostisera och åtgärda sårbarheter innan detaljerad information om sårbarheten meddelas tredjeparter eller allmänheten. Samordnad information om sårbarheter bör även omfatta samordning mellan den rapporterande entiteten och organisationen vad gäller tidpunkten för åtgärdandet och offentliggörandet av sårbarheter.

---

20 Kommissionens rekommendation (EU) 2017/1584 av den 13 september 2017 om samordnade insatser vid storskaliga cyberincidenter och cyberkriser (EUT L 239, 19.9.2017, s. 36).

(29) Medlemsstaterna bör därför vidta åtgärder för att underlätta samordnad information om sårbarheter genom att fastställa en relevant nationell policy. **Som en del av den nationella politiken bör medlemsstaterna sträva efter att i största möjliga utsträckning ta itu med de utmaningar som sårbarhetsforskare ställs inför, inbegripet deras potentiella utsatthet för straffrättsligt ansvar, i enlighet med den nationella rättsordningen.** [...] Medlemsstaterna bör utse en CSIRT-enhet i rollen som samordnare, och som vid behov ska fungera som mellanhand mellan den rapporterande entiteten och tillverkarna eller tillhandahållarna av IKT-produkter eller IKT-tjänster. CSIRT-samordnarens uppgifter bör särskilt omfatta att identifiera och kontakta berörda entiteter, stödja rapporterande entiteter, förhandla om tidsramar för meddelande av information och hantera samordnad information om sårbarheter som påverkar flera organisationer (**samordnad** information om sårbarheter omfattande flera parter). Om **de rapporterade** sårbarheterna **skulle kunna ha en betydande påverkan på entiteter** [...] i fler än en medlemsstat bör den utsedda CSIRT-enheten **i förekommande fall** samarbeta inom CSIRT-nätverket.

(30) Tillträde till korrekt och läglig information om sårbarheter som påverkar IKT-produkter och -tjänster bidrar till en förbättrad riskhantering på cybersäkerhetsområdet. I detta avseende är källor till offentligt tillgänglig information om sårbarheter ett viktigt verktyg för entiteter och deras användare, men även nationella myndigheter och CSIRT-enheter. Av denna anledning bör Enisa upprätta ett sårbarhetsregister där väsentliga och viktiga entiteter och deras leverantörer, samt entiteter som inte omfattas av detta direktivs tillämpningsområde **eller utsedda CSIRT-enheter**, på frivillig basis kan meddela information om sårbarheter och tillhandahålla sårbarhetsinformation som möjliggör för användarna att vidta lämpliga riskreducerande åtgärder.

(31) Även om liknande sårbarhetsregister och databaser faktiskt finns, förvaltas och underhålls dessa av entiteter som inte är etablerade i unionen. Ett europeiskt sårbarhetsregister som upprätthålls av Enisa skulle ge förbättrad insyn i processen för offentliggörande innan sårbarheten offentliggjorts officiellt, samt motståndskraft i händelse av störningar eller avbrott i tillhandahållandet av liknande tjänster. För att undvika dubbelarbete och i så hög grad som möjligt eftersträva komplementaritet bör Enisa undersöka möjligheten att ingå avtal om strukturerat samarbete med liknande register i tredjelandsjurisdiktioner. **Enisa bör framför allt undersöka möjligheten till ett nära samarbete med operatörerna för systemet för gemensamma sårbarheter och exponeringar (Common Vulnerabilities and Exposures – CVE), inbegripet möjligheten att bli en CVE-rotnumreringsmyndighet (root CVE numbering authority).**

(32) **Samarbetsgruppen bör fortsätta att stödja och underlätta strategiskt samarbete och utbyte av information samt att stärka förtroende och tillit mellan medlemsstaterna.** Samarbetsgruppen bör vartannat år upprätta ett arbetsprogram som omfattar de åtgärder som ska vidtas av gruppen för att genomföra dess mål och uppgifter. Tidsramen för det första program som antas enligt detta direktiv bör anpassas till tidsramen för det senaste program som antas enligt direktiv (EU) 2016/1148, i syfte att undvika potentiella avbrott i gruppens arbete.

(33) Vid utarbetandet av vägledningsdokument bör samarbetsgruppen konsekvent kartlägga nationella lösningar och erfarenheter, bedöma hur samarbetsgruppens resultat påverkar nationella strategier, diskutera utmaningar i samband med genomförandet och formulera särskilda rekommendationer som ska beaktas för ett bättre genomförande av befintliga bestämmelser.

(34) Samarbetsgruppen bör förbli ett flexibelt forum och kunna reagera på föränderliga och nya politiska prioriteringar och utmaningar samtidigt som tillgången till resurser beaktas. Den bör anordna regelbundna gemensamma möten med relevanta privata intressenter från hela unionen för att diskutera gruppens verksamhet och inhämta synpunkter på framväxande politiska frågor. För att stärka samarbetet på unionsnivå, bör gruppen överväga att bjuda in unionsorgan och -byråer som arbetar med frågor som rör cybersäkerhetspolitiken, såsom Europeiska it-brottcentrumet (EC3), Europeiska unionens byrå för luftfartssäkerhet (Easa) och Europeiska unionens rymdprogrambyrå (EUSPA) att delta i samarbetet.

(35) De behöriga myndigheterna och CSIRT-enheterna bör ha befogenhet att delta i utbytesprogram för tjänstemän från andra medlemsstater i syfte att förbättra samarbetet. De behöriga myndigheterna bör vidta nödvändiga åtgärder för att tjänstemän från andra medlemsstater ska kunna spela en faktisk roll i verksamheten inom den behöriga värdmyndigheten.

(35a) CSIRT-nätverket bör fortsätta att bidra till att stärka förtroende och tillit och främja snabbt och effektivt operativt samarbete mellan medlemsstaterna. För att stärka det operativa samarbetet på unionsnivå bör CSIRT-nätverket överväga att bjuda in unionsorgan och -byråer som arbetar med frågor som rör cybersäkerhetspolitiken, såsom Europol, att delta i dess arbete.

(36) [...]

(36a) För att underlätta ett effektivt genomförande av bestämmelserna i detta direktiv om bland annat hantering av sårbarheter, riskhanteringsåtgärder för cybersäkerhet, rapporteringsåtgärder och arrangemang för utbyte av information får medlemsstaterna samarbeta med tredjeländer och vidta åtgärder som anses lämpliga för detta ändamål, inbegripet informationsutbyte om hot, incidenter, sårbarheter, verktyg och metoder, taktik, tekniker och förfaranden, beredskapsåtgärder och övningar för cyberkrishantering, utbildning, förtroendeskapande åtgärder och strukturerade arrangemang för informationsutbyte. Sådana samarbetsavtal bör vara förenliga med unionsrätten om dataskydd.

(37) Medlemsstaterna bör bidra till inrättandet av en EU-ram för hantering av cyberkriser enligt rekommendation (EU) 2017/1584 genom de befintliga samarbetsnätverken, särskilt **Europeiska** kontaktnätverket för cyberkriser (EU-CyCLONe), CSIRT-nätverket och samarbetsgruppen. EU-CyCLONe och CSIRT-nätverket bör samarbeta på grundval av förfaranden som fastställer formerna för detta samarbete **och undvika dubbelarbete**. Arbetsordningen för EU-CyCLONe bör ytterligare specificera de förutsättningar enligt vilka nätverket ska fungera, inbegripet men inte begränsat till roller, samarbetsformer, samverkan med andra relevanta aktörer och mallar för informationsutbyte, samt kommunikationsmedel. För krishantering på **politisk** unionsnivå bör berörda parter stödja sig på EU:s integrerade arrangemang för politisk krishantering (IPCR). Kommissionen bör använda Argus-förfarandet för gränsöverskridande krissamordning på hög nivå för detta ändamål. Om krisen har en yttre dimension eller en dimension som rör den gemensamma säkerhets- och försvarspolitiken (GSFP) och denna dimension är betydande, bör Europeiska utrikestjänstens krishanteringsmekanism aktiveras.

(37a) EU-CyCLONe bör fungera som ett förmedlande nätverk mellan den tekniska och politiska nivån vid storskaliga cyberincidenter och cyberkriser. Det bör stärka samarbetet på operativ nivå genom att bygga på CSIRT-nätverkets resultat och använda egen kapacitet för att göra konsekvensanalyser av storskaliga incidenter och kriser samt ge stöd till beslutsfattandet på politisk nivå. EU:s institutioner, organ och byråer bör utse en behörig myndighet med ansvar för hantering av storskaliga cyberincidenter och cyberkriser till medlem av EU-CyCLONe.

(38) [...]

(39) [...]

(39a) Ansvaret för att säkerställa säkerheten i nätverks- och informationssystemen vilar i hög grad på väsentliga och viktiga entiteter. En riskhanteringskultur, som inbegriper riskbedömning och genomförande av säkerhetsåtgärder som är anpassade till riskerna, bör främjas och utvecklas.

(40) Åtgärder för riskhantering bör **ta hänsyn till hur beroende av nätverks- och informationssystem entiteten är och** omfatta åtgärder för att identifiera alla incidentrisker, för att förebygga, upptäcka och hantera incidenter och för att begränsa deras inverkan. Säkerheten i nätverks- och informationssystem bör omfatta lagrade, överförda och behandlade uppgifters säkerhet.

(40a) Eftersom hot mot säkerheten i nätverks- och informationssystem kan ha olika ursprung tillämpas i detta direktiv en ”allriskstrategi” som omfattar skydd av nätverks- och informationssystem och deras fysiska miljö mot alla händelser såsom stöld, brand, översvämning och telekommunikations- eller elavbrott och mot all obehörig fysisk åtkomst till och skada eller störning på entitetens information och informationsbehandlingsresurser som kan undergräva tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem. Riskhanteringsåtgärderna bör därför också omfatta fysisk säkerhet och miljösäkerhet genom att inbegripa åtgärder för att skydda entitetens nätverks- och informationssystem mot systemfel, mänskliga misstag, skadliga handlingar eller naturfenomen i linje med europeiska eller internationellt erkända standarder såsom de som ingår i ISO 27000-serien. I detta avseende bör entiteter som ett led i sina riskhanteringsåtgärder också ägna sig åt personalsäkerhet och inrätta lämpliga strategier för åtkomstkontroll. Dessa åtgärder bör vara förenliga med direktiv XXXX [direktivet om kritiska entiteters motståndskraft].

(40b) I avsaknad av lämpliga europeiska ordningar för cybersäkerhetscertifiering som antagits i enlighet med förordning (EU) 2019/881 kan medlemsstaterna kräva att entiteter använder certifierade IKT-produkter, IKT-tjänster och IKT-processer eller erhåller ett certifikat i enlighet med tillgängliga nationella ordningar för cybersäkerhet i syfte att uppfylla riskhanteringskraven för cybersäkerhet enligt detta direktiv.

(41) För att undvika oproportionella finansiella och administrativa bördor för väsentliga och viktiga entiteter bör riskhanteringskraven för cybersäkerhet stå i proportion till **risken för** [...] det berörda nätverks- och informationssystemet, med beaktande av bästa praxis för sådana åtgärder **och kostnaden för deras genomförande**. **Vederbörlig hänsyn bör också tas till entitetens storlek liksom till sannolikheten för att en incident inträffar och incidentens allvarlighetsgrad.**

(41a) I syfte att minska regelbördan bör kraven vad gäller genomförande av riskhanteringsåtgärder för cybersäkerhet i princip vara lättare för små och medelstora entiteter eller mikroentiteter, såvida inte kriterier för kritisk betydelse eller nationella riskbedömningar skulle motivera strängare krav, särskilt med avseende på entiteter som uppfyller de kriterier för kritisk betydelse som fastställs i detta direktiv.

(42) Väsentliga och viktiga entiteter bör säkerställa säkerheten i de nätverks- och informationssystem som de använder i sin verksamhet. Det rör sig framför allt om privata nätverks- och informationssystem som antingen förvaltas av deras interna it-personal eller vilkas säkerhet har lagts ut på entreprenad. Riskhanterings- och rapporteringskraven för cybersäkerhet enligt detta direktiv bör tillämpas på de relevanta väsentliga och viktiga entiteterna oavsett om de sköter underhållet av sina nätverks- och informationssystem internt eller lägger ut uppgifterna på entreprenad.

(42aa) Med beaktande av deras gränsöverskridande karaktär bör leverantörer av DNS-tjänster, registreringsenheter för toppdomäner och entiteter som tillhandahåller domännamnsregistreringstjänster för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för innehållsleverans, leverantörer av hanterade tjänster och leverantörer av hanterade säkerhetstjänster omfattas av en högre nivå av harmonisering på unionsnivå. Genomförandet av cybersäkerhetsåtgärder bör därför underlättas genom en genomförandeakt.

(43) Det är särskilt viktigt att hantera cybersäkerhetsrisker som härrör från en entitets leveranskedja och dess förhållande till sina leverantörer, med tanke på förekomsten av incidenter där entiteter har fallit offer för cyberattacker och där illvilliga aktörer har kunnat äventyra säkerheten i en entitets nätverks- och informationssystem genom att utnyttja sårbarheter som påverkar tredje parts produkter och tjänster. Entiteterna bör därför bedöma och beakta sina leverantörers och tjänsteleverantörers övergripande produktkvalitet och cybersäkerhetspraxis, inbegripet deras förfaranden för säker utveckling.

(44) Bland tjänsteleverantörerna har leverantörer av hanterade säkerhetstjänster (managed security services providers, MSSP) på områden som incidenthantering, penetrationstester, säkerhetsrevisioner och konsulttjänster en särskilt viktig roll när det gäller att bistå entiteter i deras arbete med att upptäcka och reagera på incidenter. Dessa MSSP har dock också själva varit mål för cyberattacker, och genom att de är nära integrerade i operatörernas verksamhet utgör de en särskild cybersäkerhetsrisk. Entiteterna bör därför visa större noggrannhet vid valet av en MSSP.

(44a) De nationella behöriga myndigheterna får också inom ramen för sina tillsynsuppgifter dra nytta av cybersäkerhetstjänster såsom säkerhetsrevisioner och penetrationstester eller incidenthantering. För att hjälpa entiteter och nationella behöriga myndigheter att välja kvalificerade och tillförlitliga leverantörer av cybersäkerhetstjänster bör kommissionen, med bistånd av samarbetsgruppen och Enisa, överväga möjligheten att begära europeiska ordningar för cybersäkerhetscertifiering i enlighet med artikel 48 i förordning (EU) 2019/881.

(45) Entiteterna bör också hantera cybersäkerhetsrisker som härrör från deras samverkan och förbindelser med andra intressenter inom ett vidare ekosystem. I synnerhet bör entiteterna vidta lämpliga åtgärder för att säkerställa att deras samarbete med akademiska institutioner och forskningsinstitut sker i linje med deras cybersäkerhetstrategier och följer god praxis när det gäller säker tillgång till och spridning av information i allmänhet och skydd av immateriella rättigheter i synnerhet. Likaså, med tanke på hur viktiga och värdefulla data är för entiteternas verksamhet, bör entiteterna, när de förlitar sig på dataomvandlings- och dataanalystjänster från tredje parter, vidta alla lämpliga cybersäkerhetsåtgärder.

(46) För att ytterligare hantera centrala risker i leveranskedjan och hjälpa entiteter som är verksamma i sektorer som omfattas av detta direktiv att på lämpligt sätt hantera cybersäkerhetsrisker i leveranskedjan och leverantörsrelaterade cybersäkerhetsrisker bör samarbetsgruppen tillsammans med relevanta nationella myndigheter, i samarbete med kommissionen och Enisa, utföra samordnade sektorsvisa riskbedömningar av leveranskedjan, vilket redan gjorts för 5G-nät efter rekommendation (EU) 2019/534 om it-säkerhet i 5G-nät[21], i syfte att per sektor identifiera kritiska IKT-tjänster, IKT-system eller IKT-produkter, relevanta hot och sårbarheter.

[21] Kommissionens rekommendation (EU) 2019/534 av den 26 mars 2019 om it-säkerhet i 5G-nät (EUT L 88, 29.3.2019, s. 42).

(47) Riskbedömningar av leveranskedjan bör, mot bakgrund av den berörda sektorns särdrag, ta hänsyn till både tekniska och när så är lämpligt icke-tekniska faktorer, inbegripet de som anges i rekommendation (EU) 2019/534, i den EU-omfattande samordnade riskbedömningen av säkerhet i 5G-nät och i EU:s verktygslåda för 5G-cybersäkerhet som samarbetsgruppen enats om. För att identifiera de leveranskedjor som bör bli föremål för en samordnad riskbedömning bör följande kriterier beaktas: i) i vilken utsträckning väsentliga och viktiga entiteter använder och förlitar sig på specifika kritiska IKT-tjänster, IKT-system eller IKT-produkter, ii) specifika kritiska IKT-tjänsters, IKT-systems eller IKT-produkters relevans för att utföra kritiska eller känsliga funktioner, inbegripet behandling av personuppgifter, iii) tillgången till alternativa IKT-tjänster, IKT-system eller IKT-produkter, iv) motståndskraften i hela leveranskedjan för IKT-tjänster, IKT-system eller IKT-produkter mot störningar, och v) för framväxande IKT-tjänster, IKT-system eller IKT-produkter, deras potentiella framtida betydelse för entiteternas verksamhet.

(48) För att rationalisera de rättsliga skyldigheter som åläggs tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster, och tillhandahållare av betrodda tjänster med anknytning till säkerheten i deras nätverks- och informationssystem, samt för att göra det möjligt för dessa entiteter och deras respektive behöriga myndigheter att dra nytta av den rättsliga ram som inrättas genom detta direktiv (inbegripet utnämning av CSIRT-enheter med ansvar för risk- och incidenthantering, deltagande av behöriga myndigheter och organ i samarbetsgruppens och CSIRT-nätverkets arbete) bör de omfattas av tillämpningsområdet för detta direktiv. De motsvarande bestämmelser som anges i Europaparlamentets och rådets förordning (EU) nr 910/2014[22] och Europaparlamentets och rådets direktiv (EU) 2018/1972[23] och som gäller införande av säkerhets- och anmälningskrav för sådana typer av entiteter bör därför upphävas.

---

[22] 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 (EUT L 257, 28.8.2014, s. 73).

[23] Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (EUT L 321, 17.12.2018, s. 36).

(48a) De säkerhetsskyldigheter som fastställs i detta direktiv bör anses komplettera de krav som åläggs tillhandahållare av betrodda tjänster enligt förordning (EU) nr 910/2014 (eIDA-förordningen). Tillhandahållare av betrodda tjänster bör vara skyldiga att vidta alla lämpliga och proportionella åtgärder för att hantera riskerna för deras tjänster, även med avseende på kunder och tredje parter som förlitar sig på dessa tjänster, och rapportera säkerhetsincidenter enligt detta direktiv. Sådana säkerhets- och rapporteringsskyldigheter bör också avse det fysiska skyddet av den tjänst som tillhandahålls. Artikel 24 i förordning (EU) nr 910/2014 bör fortsätta att tillämpas.

(48aa) Medlemsstaterna får utse eIDA:s tillsynsorgan till behöriga myndigheter för betrodda tjänster för att säkerställa att nuvarande praxis upprätthålls och för att bygga vidare på den kunskap och erfarenhet som förvärvats genom tillämpningen av eIDA-förordningen. Om den rollen tilldelas ett annat organ bör de nationella behöriga myndigheterna enligt detta direktiv samarbeta nära och i god tid genom att utbyta relevant information i syfte att säkerställa att tillsynen är effektiv och att tillhandahållare av betrodda tjänster uppfyller kraven i detta direktiv och i förordning [XXXX/XXXX].

I förekommande fall bör den nationella behöriga myndigheten enligt detta direktiv omedelbart informera eIDA:s tillsynsorgan om anmälda betydande cyberhot eller anmälda betydande cyberincidenter som påverkar betrodda tjänster samt ifall en tillhandahållare av betrodda tjänster inte uppfyller kraven enligt detta direktiv. Medlemsstaterna får för rapporteringsändamål i tillämpliga fall använda den gemensamma kontaktpunkt som inrättats för att uppnå en gemensam och automatisk rapportering av incidenter till både eIDA:s tillsynsorgan och den behöriga myndigheten enligt detta direktiv. Reglerna om rapporteringsskyldigheter bör inte påverka tillämpningen av förordning (EU) 2016/679 och Europaparlamentets och rådets direktiv 2002/58/EG[24].

[24] 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).

(49) När så är lämpligt och för att undvika onödiga störningar **bör** befintliga nationella riktlinjer [...] som antagits för införlivandet av bestämmelserna om säkerhetsåtgärder i artik**larna** 40[...] och 41 i direktiv (EU) 2018/1972[...] **beaktas i de bestämmelser om införlivande som medlemsstaterna tillämpar med avseende på detta direktiv, så att man bygger vidare på den kunskap och kompetens som redan har förvärvats inom ramen för direktiv (EU) 2018/1972 i fråga om åtgärder för hantering av säkerhetsrisker eller incidentanmälningar. Enisa kan också ta fram vägledning om säkerhets- och rapporteringskrav för tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster för att underlätta harmonisering och övergång och minimera störningar. Medlemsstaterna kan utse de nationella regleringsmyndigheterna till behöriga myndigheter för elektronisk kommunikation för att säkerställa att nuvarande praxis upprätthålls och för att bygga vidare på den kunskap och erfarenhet som förvärvats inom ramen för direktiv (EU) 2018/1972.**

(50) Mot bakgrund av den ökande betydelsen av nummeroberoende interpersonella kommunikationstjänster är det nödvändigt att säkerställa att sådana tjänster också omfattas av lämpliga säkerhetskrav med tanke på deras särskilda karaktär och ekonomiska betydelse. Tillhandahållare av sådana tjänster bör därför också säkerställa en nivå på säkerheten i nätverks- och informationssystem som är lämplig i förhållande till den föreliggande risken. Eftersom tillhandahållare av nummeroberoende interpersonella kommunikationstjänster i allmänhet inte utövar någon faktisk kontroll över överföringen av signaler via nät kan graden av risk för sådana tjänster i vissa avseenden anses lägre än för traditionella elektroniska kommunikationstjänster. Detsamma gäller för interpersonella kommunikationstjänster som använder nummer och som inte utövar faktisk kontroll över signalöverföringen.

(51) Den inre marknaden är mer beroende av ett fungerande internet än någonsin tidigare. Tjänster från praktiskt taget alla väsentliga och viktiga entiteter är beroende av tjänster som tillhandahålls via internet. För att säkerställa ett smidigt tillhandahållande av tjänster som levereras från väsentliga och viktiga entiteter är det viktigt att allmänna elektroniska kommunikationsnät, t.ex. stamnät för internet eller sjökablar för telekommunikation, har infört lämpliga cybersäkerhetsåtgärder och rapporterar incidenter i samband med dessa.

(52) I [...] **tillämpliga fall** bör entiteterna informera sina tjänstemottagare om särskilda [...] åtgärder dessa kan vidta för att minska den åtföljande risken för dem själva **från ett betydande cyberhot**. **Entiteterna bör, när så är lämpligt och i synnerhet i fall där det betydande cyberhotet kan förverkligas, utöver de behöriga myndigheterna eller CSIRT-enheterna även informera sina tjänstemottagare om själva hotet.** Kravet på att informera mottagarna om sådana hot bör inte befria entiteter från skyldigheten att på egen bekostnad vidta lämpliga och omedelbara åtgärder för att förebygga eller avhjälpa cyberhot och återställa tjänstens normala säkerhetsnivå. Mottagarna bör kostnadsfritt tillhandahållas sådan information om **cyber**[...]hot.

(53) Särskilt bör tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster informera tjänstemottagarna om särskilda och betydande cyberhot och om åtgärder de kan vidta för att säkerställa säkerheten för sin kommunikation, t.ex. genom att använda särskilda typer av programvara eller krypteringsteknik.

(54) För att trygga säkerheten för elektroniska kommunikationsnät och kommunikationstjänster bör användningen av kryptering, särskilt totalsträckskryptering, främjas och vid behov vara obligatorisk för tillhandahållare av sådana tjänster och nät i enlighet med principerna om automatisk och inbyggd säkerhet och automatiskt och inbyggt integritetsskydd vid tillämpningen av artikel 18. Användningen av totalsträckskryptering bör förenas med medlemsstaternas befogenheter att säkerställa skyddet av sina väsentliga säkerhetsintressen och sin allmänna säkerhet och att möjliggöra utredning, avslöjande och lagföring av brott i enlighet med unionsrätten. Lösningar för laglig åtkomst till information i totalsträckskrypterad kommunikation bör upprätthålla krypteringens effektivitet när det gäller att skydda den personliga integriteten och kommunikationssäkerheten, och samtidigt möjliggöra en effektiv brottsbekämpning.

(55) I detta direktiv fastställs en tvåstegsstrategi för incidentrapportering för att hitta rätt balans mellan, å ena sidan, snabb rapportering som bidrar till att minska den potentiella spridningen av incidenter och gör det möjligt för entiteter att söka stöd, och, å andra sidan, ingående rapportering som drar värdefulla lärdomar av enskilda incidenter och med tiden förbättrar enskilda företags och hela sektorers motståndskraft mot cyberhot. Om entiteter får kännedom om en incident bör de vara skyldiga att lämna in en första anmälan inom 24 timmar, följt av en slutrapport senast en månad därefter. Den första anmälan bör endast innehålla den information som är absolut nödvändig för att göra de behöriga myndigheterna medvetna om incidenten och för att entiteten vid behov ska kunna söka hjälp. En sådan anmälan bör, i tillämpliga fall, ange om incidenten sannolikt har orsakats av olagliga eller avsiktligt skadliga handlingar. Medlemsstaterna bör säkerställa att kravet att lämna in denna första anmälan inte avleder den rapporterande entitetens resurser från verksamheter i samband med incidenthantering som bör prioriteras. För att ytterligare förhindra att incidentrapporteringsskyldigheter avleder resurser från incidenthantering eller på annat sätt kan äventyra entiteternas ansträngningar i detta avseende, bör medlemsstaterna också föreskriva att den berörda entiteten, i vederbörligen motiverade fall och efter överenskommelse med de behöriga myndigheterna eller CSIRT-enheten, får avvika från tidsfristerna på 24 timmar för den första anmälan och en månad för slutrapporten.

(55a) En proaktiv strategi mot cyberhot är en viktig del av hanteringen av cybersäkerhetsrisker som bör göra det möjligt för behöriga myndigheter att effektivt förhindra att cyberhot blir verkliga incidenter som kan vålla betydande materiella eller immateriella förluster. Det är därför av avgörande vikt att betydande cyberhot anmäls.

(56) Väsentliga och viktiga entiteter befinner sig ofta i en situation där en viss incident på grund av sina särdrag måste rapporteras till flera olika myndigheter till följd av anmälningsskyldigheter enligt olika rättsliga instrument. Sådana fall skapar ytterligare bördor och kan också leda till osäkerhet om format och förfaranden för sådana anmälningar. Mot bakgrund av detta och, i syfte att förenkla rapporteringen av säkerhetsincidenter, [...] **kan** medlemsstaterna inrätta en gemensam kontaktpunkt för alla anmälningar som krävs enligt detta direktiv och även enligt annan unionslagstiftning, t.ex. förordning (EU) 2016/679 och direktiv 2002/58/EG. Enisa bör i samarbete med samarbetsgruppen utarbeta gemensamma mallar för anmälningar med hjälp av riktlinjer som skulle förenkla och rationalisera den rapporteringsinformation som krävs enligt unionsrätten och minska företagens bördor.

(57) Om en incident misstänks ha samband med allvarlig brottslig verksamhet enligt unionsrätt eller nationell rätt, bör medlemsstaterna uppmuntra väsentliga och viktiga entiteter att, på grundval av tillämpliga straffrättsliga bestämmelser i enlighet med unionsrätten, rapportera incidenter som misstänks vara av allvarlig brottslig art till de relevanta rättsvårdande myndigheterna. Där så är lämpligt, och utan att det påverkar de bestämmelser om skydd av personuppgifter som gäller för Europol, är det önskvärt att samordning mellan behöriga myndigheter och rättsvårdande myndigheter i olika medlemsstater underlättas av EC3 och Enisa.

(58) Säkerheten för personuppgifter undergrävs ofta till följd av incidenter. I detta sammanhang bör de behöriga myndigheterna samarbeta och utbyta information om alla relevanta frågor med dataskyddsmyndigheterna och tillsynsmyndigheterna i enlighet med direktiv 2002/58/EG.

(59) Att upprätthålla korrekta och fullständiga databaser med domännamn och registreringsuppgifter (WHOIS-data) och ge laglig åtkomst till sådana uppgifter är avgörande för att säkerställa domännamnssystemets säkerhet, stabilitet och resiliens, vilket i sin tur bidrar till en hög gemensam nivå av cybersäkerhet inom unionen. Om behandlingen inbegriper personuppgifter ska sådan behandling vara förenlig med unionens dataskyddslagstiftning.

(60) Dessa uppgifters tillgänglighet och offentliga myndigheters möjlighet att få åtkomst till dem i rätt tid, inbegripet behöriga myndigheter enligt unionslagstiftning eller nationell lagstiftning för förebyggande, utredning eller lagföring av brott, incidenthanteringsorganisationer (Cert), [...]CSIRT-enheter, och när det gäller uppgifter om deras klienter för tillhandahållare av elektroniska kommunikationsnät och kommunikationstjänster och tillhandahållare av cybersäkerhetsteknik och cybersäkerhetstjänster som agerar för dessa klienters räkning, är avgörande för att förebygga och bekämpa missbruk av domännamnssystem, särskilt för att förebygga, upptäcka och reagera på cybersäkerhetsincidenter. Sådan åtkomst bör vara förenlig med unionens dataskyddslagstiftning i den mån den rör personuppgifter.

(61) För att säkerställa tillgången till korrekta och fullständiga registreringsuppgifter för domännamn bör registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster för toppdomäner (så kallade ombud) samla in och garantera integriteten och tillgängligheten för registreringsuppgifterna för domännamn. **När det gäller registreringsuppgifterna bör entiteterna särskilt kontrollera registrantens namn och e-postadress.** [...] Registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster för toppdomäner bör fastställa policyer och förfaranden för insamling och lagring av korrekta och fullständiga registreringsuppgifter samt för att förhindra och korrigera felaktiga registreringsuppgifter i enlighet med unionens dataskyddsregler.

(62) Registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster för dem bör offentliggöra registreringsuppgifter för domännamn som inte omfattas av unionens dataskyddsregler, till exempel uppgifter som rör juridiska personer[25]. Registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster för toppdomäner bör också möjliggöra för legitima åtkomstsökande att få laglig åtkomst till specifika registreringsuppgifter för domännamn som rör fysiska personer, i enlighet med unionens dataskyddslagstiftning. Medlemsstaterna bör säkerställa att registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster för dem utan onödigt dröjsmål besvarar ansökningar [...] om utlämnande av registreringsuppgifter för domännamn **från legitima åtkomstsökande såsom behöriga myndigheter enligt unionslagstiftning eller nationell lagstiftning på området nationell säkerhet och straffrätt eller CSIRT-enheter**. Registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster för dem bör fastställa riktlinjer och förfaranden för offentliggörande och utlämnande av registreringsuppgifter, inbegripet servicenivåavtal för att hantera ansökningar om åtkomst från legitima åtkomstsökande. Åtkomstförfarandet kan också omfatta användning av ett gränssnitt, en portal eller ett annat tekniskt verktyg som ett effektivt system för att begära och få tillgång till registreringsuppgifter. **Medlemsstaterna bör säkerställa att all slags åtkomst till domänregistreringsuppgifter (både personuppgifter och andra uppgifter) är kostnadsfri.** I syfte att främja harmoniserad praxis på hela den inre marknaden får kommissionen anta riktlinjer för sådana förfaranden utan att det påverkar Europeiska dataskyddsstyrelsens befogenheter **i enlighet med och som komplement till internationella standarder som utvecklats av flerpartssamfundet**.

---

25 Enligt skäl 14 i Europaparlamentets och rådets förordning (EU) 2016/679: ”Denna förordning omfattar inte behandling av personuppgifter rörande juridiska personer, särskilt företag som bildats som juridiska personer, exempelvis uppgifter om namn på och typ av juridisk person samt kontaktuppgifter”.

(63) [...] **De v**äsentliga och viktiga entiteterna enligt detta direktiv bör omfattas av jurisdiktionen i den medlemsstat där de tillhandahåller sina tjänster. **De entiteter som avses i punkterna 1–7 och 10 i bilaga I samt de tillhandahållare av betrodda tjänster och de leverantörer av internetknutpunkter som avses i punkt 8 i bilaga I och punkterna 1–5 i bilaga II till detta direktiv bör omfattas av jurisdiktionen i den medlemsstat där de är etablerade.** Om entiteten tillhandahåller tjänster **eller är etablerad** i mer än en medlemsstat bör den omfattas av dessa medlemsstaters separata och parallella jurisdiktioner samtidigt. De behöriga myndigheterna i dessa medlemsstater bör samarbeta, ge varandra ömsesidigt bistånd och vid behov genomföra gemensamma tillsynsåtgärder. **Om medlemsstaterna beslutar att utöva jurisdiktion bör de undvika att samma beteende bestraffas mer än en gång för överträdelser av de skyldigheter som fastställs i detta direktiv.**

(64) För att ta hänsyn till den gränsöverskridande karaktären hos de tjänster och den verksamhet som bedrivs av leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, **entiteter som tillhandahåller domännamnsregistreringstjänster för toppdomäner,** tillhandahållare av nätverk för innehållsleverans, leverantörer av molntjänster, leverantörer av datacentraltjänster och digitala leverantörer bör endast en medlemsstat ha jurisdiktion över dessa entiteter. Jurisdiktion bör tilldelas den medlemsstat där respektive entitet har sitt huvudsakliga etableringsställe i unionen. Kriteriet för etableringsställe i detta direktiv förutsätter att verksamhet faktiskt bedrivs genom en stabil struktur. Den rättsliga formen för en sådan struktur, oavsett om det är en filial eller ett dotterföretag med status som juridisk person, bör inte vara den avgörande faktorn i detta avseende.

Huruvida kriteriet är uppfyllt bör inte vara beroende av om nätverks- och informationssystemen är fysiskt belägna på en viss plats. Förekomsten och användningen av sådana system utgör inte i sig en sådan huvudsaklig etablering och är därför inte avgörande kriterier för att fastställa det huvudsakliga etableringsstället. Det huvudsakliga etableringsstället bör vara den plats där besluten om åtgärder för att hantera cybersäkerhetsrisker **i huvudsak** fattas i unionen. Detta motsvarar vanligtvis platsen för företagens huvudkontor i unionen. Om **platsen där sådana beslut i huvudsak fattas inte kan fastställas eller om** sådana beslut inte fattas i unionen bör det huvudsakliga etableringsstället anses vara beläget i den medlemsstat där entiteten har ett etableringsställe med flest anställda i unionen. Om tjänsterna utförs av en koncern bör det kontrollerande företagets huvudsakliga etableringsställe betraktas som koncernens huvudsakliga etableringsställe.

(64a) När en rekursiv DNS-tjänst tillhandahålls av en tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster endast som en del av internetanslutningstjänsten, bör entiteten anses omfattas av jurisdiktionen i alla de medlemsstater där dess tjänster tillhandahålls.

(64aa) För att säkerställa en tydlig översikt över leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, entiteter som tillhandahåller domännamnsregistreringstjänster för toppdomäner, leverantörer av nätverk för innehållsleverans, leverantörer av molntjänster, leverantörer av datacentraltjänster och digitala leverantörer som tillhandahåller tjänster i hela unionen inom ramen för detta direktivs tillämpningsområde, bör Enisa skapa och upprätthålla ett register över sådana entiteter på grundval av de anmälningar som mottagits från medlemsstaterna, i tillämpliga fall genom deras nationella mekanismer för självanmälan. För att säkerställa att den information som bör ingå i registret är korrekt och fullständig bör medlemsstaterna till Enisa lämna in den information som finns tillgänglig i deras nationella register om dessa entiteter. Enisa och medlemsstaterna bör vidta åtgärder för att underlätta kompatibilitet mellan sådana register, samtidigt som skydd av sekretessbelagda och säkerhetsskyddsklassificerade uppgifter säkerställs.

(65) I de fall där en leverantör av DNS-tjänster, registreringsenhet för toppdomäner, tillhandahållare av nätverk för innehållsleverans, leverantör av molntjänster, leverantör av datacentraltjänster eller digital leverantör som inte är etablerad i unionen erbjuder tjänster inom unionen, bör den utse en företrädare. I syfte att fastställa om en sådan entitet erbjuder tjänster inom unionen bör det kontrolleras om det är uppenbart att entiteten planerar att erbjuda tjänster till personer i en eller flera medlemsstater. Enbart den omständigheten att en entitets eller en mellanhands webbplats, eller en e-postadress och andra kontaktuppgifter, är tillgängliga i unionen, eller att ett språk används som allmänt används i det tredjeland där entiteten är etablerad, är inte tillräcklig för att fastställa en sådan avsikt. Emellertid kan faktorer som att det används ett visst språk eller en viss valuta som allmänt används i en eller flera medlemsstater med möjligheten att beställa tjänster på detta andra språk, eller att kunder eller användare i unionen omnämns, göra det uppenbart att entiteten planerar att erbjuda tjänster inom unionen. Företrädaren bör agera på entitetens vägnar och det bör vara möjligt för behöriga myndigheter eller CSIRT-enheterna att kontakta företrädaren. Företrädaren bör utses uttryckligen genom en skriftlig fullmakt från entiteten att agera på dess vägnar med avseende på dess skyldigheter enligt detta direktiv, inklusive incidentrapportering.

(66) Om uppgifter som anses vara säkerhetsskyddsklassificerade enligt nationell rätt eller unionsrätt utbyts, rapporteras eller på annat sätt delas enligt bestämmelserna i detta direktiv, bör motsvarande särskilda regler för hantering av säkerhetsskyddsklassificerade uppgifter tillämpas.

(67) I och med att cyberhoten blir mer komplexa och sofistikerade är goda åtgärder för upptäckt och förebyggande i stor utsträckning beroende av ett regelbundet utbyte av underrättelser om hot och sårbarhet mellan entiteter. Informationsutbyte bidrar till ökad medvetenhet om cyberhot, vilket i sin tur ökar entiteternas förmåga att förhindra att hot blir verkliga incidenter och gör det möjligt för entiteterna att bättre begränsa effekterna av incidenter och återhämta sig mer effektivt. I avsaknad av vägledning på unionsnivå verkar flera faktorer ha hindrat sådant utbyte av underrättelser, särskilt osäkerheten om förenligheten med konkurrens- och ansvarsreglerna.

(68) Entiteter bör uppmuntras att kollektivt utnyttja sina individuella kunskaper och praktiska erfarenheter på strategisk, taktisk och operativ nivå i syfte att förbättra förmågan att på lämpligt sätt bedöma, övervaka, försvara sig mot och reagera på cyberhot. Det är därför nödvändigt att på unionsnivå möjliggöra framväxten av mekanismer för frivilligt informationsutbyte. I detta syfte bör medlemsstaterna aktivt stödja och uppmuntra även relevanta entiteter som inte omfattas av detta direktivs tillämpningsområde att delta i sådana mekanismer för informationsutbyte. Dessa mekanismer bör genomföras helt i enlighet med unionens konkurrensregler och unionens regler om uppgiftsskydd.

(69) [...] I den utsträckning som är absolut nödvändig och proportionell för att säkerställa nät- och informationssäkerhet **skulle behandling av personuppgifter som utförs** av **väsentliga och viktiga** entiteter […] och tillhandahållare av säkerhetsteknik och säkerhetstjänster **kunna betraktas som nödvändig för att fullgöra en rättslig förpliktelse eller** […] utgöra ett berättigat intresse för den personuppgiftsansvarige i fråga**[…]**, i enlighet med förordning (EU) 2016/679. Detta **skulle kunna** […] inbegripa åtgärder som rör förebyggande, upptäckt, analys och hantering av incidenter, åtgärder för att öka enheten om specifika cyberhot, informationsutbyte i samband med åtgärdande av och samordnat utlämnande av information om sårbarhet samt frivilligt informationsutbyte om dessa incidenter, […] cyberhot och sårbarheter, angreppsindikatorer, taktik, tekniker och förfaranden, cybersäkerhetsvarningar och konfigurationsverktyg. Sådana åtgärder kan kräva behandling av […] **olika** typer av personuppgifter, **såsom** ip-adresser, webbadresser (URL), domännamn och e-postadresser. **De behöriga myndigheternas, de gemensamma kontaktpunkternas och CSIRT-enheternas behandling av personuppgifter bör fastställas i den nationella lagstiftningen och betraktas som nödvändig för att fullgöra en rättslig förpliktelse eller för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning i enlighet med artikel 6.1 c eller e i förordning (EU) 2016/679.**

(69a) Medlemsstaterna får i sin lagstiftning fastställa regler som gör det möjligt för de behöriga myndigheterna, de gemensamma kontaktpunkterna och CSIRT-enheterna att – i den mån det är strikt nödvändigt och proportionellt för att säkerställa säkerhet i de väsentliga och viktiga entiteternas nätverks- och informationssystem – behandla särskilda kategorier av personuppgifter i enlighet med artikel 9 [...] i förordning (EU) 2016/679, framför allt genom att föreskriva lämpliga och särskilda åtgärder för att säkerställa fysiska personers grundläggande rättigheter och intressen, inbegripet tekniska begränsningar för vidareutnyttjandet av sådana uppgifter och användningen av säkerhetsåtgärder och integritetsbevarande åtgärder på aktuell teknisk nivå, såsom pseudonymisering, eller kryptering om avidentifiering avsevärt kan påverka det eftersträvade ändamålet.

(70) För att stärka de tillsynsbefogenheter och tillsynsåtgärder som bidrar till att säkerställa ett effektivt fullgörande av skyldigheter bör detta direktiv innehålla en minimiförteckning över tillsynsåtgärder och tillsynsmedel genom vilka behöriga myndigheter kan utöva tillsyn över väsentliga och viktiga entiteter. Dessutom bör detta direktiv fastställa en differentiering av tillsynssystemet mellan väsentliga och viktiga entiteter i syfte att säkerställa en rättvis balans vad gäller skyldigheterna för både entiteter och behöriga myndigheter. Väsentliga entiteter bör därför omfattas av ett fullständigt tillsynssystem (förhandstillsyn och efterhandstillsyn), medan viktiga entiteter bör omfattas av enklare tillsyn, endast i efterhand. För de senare innebär detta att viktiga entiteter inte systematiskt måste dokumentera uppfyllande av riskhanteringskraven för cybersäkerhet, och att de behöriga myndigheterna bör tillämpa en reaktiv efterhandstillsyn och därmed inte ha någon allmän skyldighet att utöva tillsyn över dessa entiteter. **För viktiga entiteter kan efterhandstillsyn utlösas av bevis eller indikationer eller uppgifter som har kommit till de behöriga myndigheternas kännedom och som enligt dessa myndigheter tyder på potentiellt bristande fullgörande av de skyldigheter som fastställs i detta direktiv. Sådana bevis, indikationer eller uppgifter kan exempelvis vara av den typ som de behöriga myndigheterna mottar från andra myndigheter, entiteter, medborgare, medier eller andra källor eller offentligt tillgänglig information eller härröra från annan verksamhet som de behöriga myndigheterna bedriver i samband med fullgörandet av sina uppgifter.**

(70a) Vid genomförandet av förhandstillsyn bör de behöriga myndigheterna kunna besluta att prioritera användningen av de tillsynsåtgärder och tillsynsmedel som står till deras förfogande på ett proportionellt sätt. Detta innebär att de behöriga myndigheterna kan besluta om en sådan prioritering på grundval av tillsynsmetoder som bör bygga på en riskbaserad metod. Mer specifikt kan sådana metoder omfatta kriterier eller riktmärken för klassificering av väsentliga entiteter i riskkategorier och motsvarande tillsynsåtgärder och tillsynsmedel som rekommenderas per riskkategori, såsom användning av, frekvens för eller typ av inspektioner på plats eller riktade säkerhetsrevisioner eller säkerhetsskanningar, vilken typ av information som ska begäras och detaljnivån på denna information. Sådana tillsynsmetoder kan också åtföljas av arbetsprogram och utvärderas och ses över regelbundet, inklusive med avseende på aspekter som resursfördelning och resursbehov.

(70aa) När det gäller offentliga förvaltningsentiteter bör tillsynsbefogenheterna utövas i enlighet med de nationella ramarna och den nationella rättsordningen. Medlemsstaterna bör kunna besluta att införa lämpliga, proportionella och effektiva tillsyns- och efterlevnadskontrollåtgärder med avseende på dessa entiteter.

(70aaa) För att visa att vissa riskhanteringsåtgärder för cybersäkerhet har vidtagits kan medlemsstaterna kräva att väsentliga och viktiga entiteter använder kvalificerade betrodda tjänster eller anmälda system för elektronisk identifiering i enlighet med förordning (EU) nr 910/2014.

(71) För att efterlevnadskontrollen ska bli effektiv bör det fastställas en minimiförteckning över administrativa sanktioner för brott mot de riskhanterings- och rapporteringsskyldigheter för cybersäkerhet som föreskrivs i detta direktiv, med en tydlig och konsekvent ram för sådana sanktioner i hela unionen. Vederbörlig hänsyn bör tas till överträdelsens art, allvarlighetsgrad och varaktighet, de faktiska skador eller förluster som orsakats eller potentiella skador eller förluster som kunde ha uppstått, om överträdelsen är avsiktlig eller beror på försumlighet, vidtagna åtgärder för att förhindra eller begränsa skadorna och/eller förlusterna, graden av ansvar eller relevanta tidigare överträdelser, graden av samarbete med den behöriga myndigheten och andra försvårande eller förmildrande omständigheter. Påförandet av sanktioner, inbegripet administrativa sanktionsavgifter, bör omfattas av lämpliga rättssäkerhetsgarantier i överensstämmelse med de allmänna principerna inom unionsrätten och Europeiska unionens stadga om de grundläggande rättigheterna, vilket inbegriper ett effektivt rättsligt skydd och korrekt rättsligt förfarande.

(71a) Bestämmelserna om ansvar för fysiska personer som har vissa ansvarsområden inom en entitet i samband med brott mot deras plikt att säkerställa att de skyldigheter som fastställs i detta direktiv fullgörs innebär inte att medlemsstaterna är skyldiga att säkerställa lagföring eller civilrättsligt ansvar för skador som sådana brott har medfört för tredje parter.

(72) För att säkerställa en effektiv efterlevnadskontroll av de skyldigheter som fastställs i detta direktiv bör varje behörig myndighet ha befogenhet att påföra eller begära påförande av administrativa sanktionsavgifter.

(73) Om administrativa sanktionsavgifter påförs ett företag, bör ett företag i detta sammanhang anses vara ett företag i den mening som avses i artiklarna 101 och 102 i EUF-fördraget. Om administrativa sanktionsavgifter påförs personer som inte är ett företag, bör tillsynsmyndigheten ta hänsyn till den allmänna inkomstnivån i medlemsstaten och personens ekonomiska situation, när den överväger lämplig sanktionsavgift. Medlemsstaterna bör fastställa om och i vilken utsträckning myndigheter ska omfattas av administrativa sanktionsavgifter. Föreläggande av en administrativ sanktionsavgift påverkar inte de behöriga myndigheternas tillämpning av andra befogenheter eller andra sanktioner som fastställs i de nationella bestämmelser som införlivar detta direktiv.

(74) Medlemsstaterna […] **får** fastställa bestämmelser om straffrättsliga påföljder för överträdelser av de nationella bestämmelser som införlivar detta direktiv. Påförandet av straffrättsliga påföljder för överträdelser av sådana nationella bestämmelser och relaterade administrativa sanktioner bör dock inte medföra ett åsidosättande av principen *ne bis in idem* enligt domstolens tolkning.

(75) När detta direktiv inte harmoniserar administrativa sanktioner eller när så är nödvändigt i andra fall, till exempel vid fall av allvarliga överträdelser av de skyldigheter som fastställs i detta direktiv, bör medlemsstaterna genomföra ett system med effektiva, proportionella och avskräckande sanktioner. Dessa sanktioners art, straffrättsliga eller administrativa, bör fastställas i medlemsstaternas nationella rätt.

(76) För att de sanktioner som är tillämpliga på överträdelser av de skyldigheter som fastställs i detta direktiv ska bli mer effektiva och avskräckande bör de behöriga myndigheterna ges befogenhet att tillämpa sanktioner i form av tillfälligt upphävande av en certifiering eller auktorisation för en del av eller alla tjänster som tillhandahålls av en väsentlig entitet och införande av ett tillfälligt förbud för en fysisk person att utöva ledande funktioner. Med tanke på sanktionernas stränghet och påverkan på entiteternas verksamheter och i sista hand deras konsumenter bör sådana sanktioner endast tillämpas proportionellt mot överträdelsens allvarlighetsgrad och med beaktande av de särskilda omständigheterna i varje enskilt fall, inbegripet om överträdelsen är avsiktlig eller beror på försumlighet samt vidtagna åtgärder för att förhindra eller begränsa skadorna och/eller förlusterna. Sådana sanktioner bör endast tillämpas som sista utväg, dvs. först efter det att de andra relevanta åtgärder för efterlevnadskontroll som fastställs i detta direktiv har uttömts, och endast fram till dess att de entiteter som omfattas av sanktionerna vidtar nödvändiga åtgärder för att avhjälpa de brister eller uppfylla de krav från den behöriga myndigheten för vilka sanktionerna tillämpades. Påförandet av sådana sanktioner måste omfattas av lämpliga rättssäkerhetsgarantier i enlighet med de allmänna principerna i unionsrätten och Europeiska unionens stadga om de grundläggande rättigheterna, inbegripet effektivt rättsligt skydd, korrekt rättsförfarande, oskuldspresumtion och rätten till försvar.

(76a) För att säkerställa effektiv tillsyn och efterlevnadskontroll, framför allt i fall med en gränsöverskridande dimension, bör de medlemsstater som har mottagit en begäran om ömsesidigt bistånd, inom ramen för begäran, vidta lämpliga tillsyns- och efterlevnadskontrollåtgärder med avseende på den berörda entitet som tillhandahåller tjänster eller som har ett nätverks- och informationssystem inom deras territorium.

(77) Detta direktiv bör fastställa regler för samarbete mellan de behöriga myndigheterna och tillsynsmyndigheterna i enlighet med förordning (EU) 2016/679 för att hantera överträdelser som rör personuppgifter.

(78) Detta direktiv bör syfta till att säkerställa en hög ansvarsnivå för riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter på organisationsnivå. Av dessa skäl bör ledningsorganen för de entiteter som omfattas av detta direktiv godkänna riskåtgärderna för cybersäkerhet och övervaka deras genomförande.

(79) Ett **peer** [...]**learning-system** […] bör införas **för att bidra till att stärka det ömsesidiga** förtroendet **och dra lärdom av god praxis och erfarenheter**, vilket möjliggör […] **kollegiala utbyten** för experter utsedda av medlemsstaterna […] om genomförandet av cybersäkerhetsstrategier […]. **Vid genomförandet av peer learning-systemet bör särskild hänsyn ägnas åt att säkerställa att det inte medför onödiga eller oproportionerliga bördor för medlemsstaternas berörda myndigheter. Kommissionen bör utforska alla möjligheter att potentiellt garantera ekonomisk täckning av de kostnader som kan uppstå till följd av anordnandet av peer learning-uppdrag. Dessutom bör peer learning-systemet beakta resultatet av liknande mekanismer, såsom systemet för sakkunnigbedömning inom ramen för CSIRT-nätverket, tillföra mervärde och undvika dubbelarbete. Genomförandet av peer learning-systemet bör inte påverka tillämpningen av den nationella lagstiftningen eller unionslagstiftningen om skydd av sekretessbelagda och säkerhetsskyddsklassificerade uppgifter. Innan peer learning-omgångarna inleds kan medlemsstaterna göra en självbedömning av de relevanta aspekterna. På begäran av samarbetsgruppen kan Enisa vid behov ge vägledning om självbedömningen och de relevanta mallarna. Medlemsstaterna kan besluta att offentliggöra sina respektive rapporter.**

(80) [...]

(81) I syfte att säkerställa enhetliga villkor för genomförandet av de relevanta bestämmelserna i detta direktiv med avseende på de förfaranden som krävs för samarbetsgruppens verksamhet, de tekniska aspekterna av riskhanteringsåtgärder eller typen av information i incidentanmälningar samt formatet och förfarandet för sådana anmälningar och **de kategorier av entiteter som är skyldiga att använda vissa certifierade IKT-produkter, IKT-tjänster och IKT-processer**, bör kommissionen tilldelas genomförandebefogenheter. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011[26].

(82) Detta direktiv bör med jämna mellanrum ses över av kommissionen i samråd med berörda parter, främst i syfte att avgöra behovet av ändringar med hänsyn till samhällsutvecklingen, den politiska utvecklingen, den tekniska utvecklingen eller ändrade marknadsvillkor.

---

26 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).

(83) Eftersom målet för detta direktiv, nämligen att uppnå en hög gemensam cybersäkerhetsnivå i unionen, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens verkningar, kan uppnås bättre 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 detta mål.

(84) Detta direktiv respekterar de grundläggande rättigheterna och iakttar de principer som erkänns i Europeiska unionens stadga om de grundläggande rättigheterna, i synnerhet rätten till respekt för privatliv och kommunikationer, skydd av personuppgifter, näringsfriheten, rätten till egendom, rätten till ett effektivt rättsmedel och rätten att yttra sig. Detta direktiv bör genomföras i enlighet med dessa rättigheter och principer.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

Allmänna bestämmelser

Artikel 1

Innehåll

1. I detta direktiv fastställs åtgärder för att säkerställa en hög gemensam cybersäkerhetsnivå inom unionen**, i syfte att förbättra den inre marknadens funktion**.

2. Direktivet fastställer i detta syfte följande:

   a) Skyldigheter för medlemsstaterna att anta nationella strategier för cybersäkerhet och utse behöriga nationella myndigheter, gemensamma kontaktpunkter och enheter för hantering av it-säkerhetsincidenter (*CSIRT-enheter*).

   b) Riskhanterings- och rapporteringsskyldigheter beträffande cybersäkerhet för entiteter av den typ som betecknas […] i bilag**orna I och II** […].

   c) **Regler och** skyldigheter när det gäller informationsutbyte om cybersäkerhet.

Artikel 2

Tillämpningsområde

1. Detta direktiv är tillämpligt på offentliga och privata entiteter av de typer **som förtecknas** […] i […] bilag**orna I och II** […] **och som uppnår eller överstiger trösklarna för medelstora företag** […] i den mening som avses i kommissionens rekommendation 2003/361/EG[27]. **Artiklarna 3.4 och 6.2 andra och tredje styckena i bilagan till den rekommendationen ska inte gälla vid tillämpning av detta direktiv.**

2. […] Oberoende av […] storleken **på de entiteter som avses i punkt 1** är detta direktiv också tillämpligt **i följande fall**: [...]

   a) Om tjänsterna tillhandahålls av en av följande entiteter:

      i) De tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster som avses i punkt 8 i bilaga I.

      ii) De tillhandahållare av betrodda tjänster som avses i punkt XX i bilaga I.

      iii) De icke kvalificerade tillhandahållare av betrodda tjänster som avses i punkt XX i bilaga I.

      iv) De registreringsenheter för toppdomäner […] som avses i punkt 8 i bilaga I.

   b) [...]

27 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).

c) Om entiteten är den enda leverantören **i en medlemsstat** av en tjänst […] **som är väsentlig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet**.

d) Om en potentiell störning av den tjänst som entiteten tillhandahåller skulle kunna […] ha en **betydande** påverkan på skyddet för människors liv och hälsa, den allmänna säkerheten eller folkhälsan.

e) Om en potentiell störning av den tjänst som entiteten tillhandahåller skulle kunna medföra […] **betydande** systemrisker, särskilt för de sektorer där sådana störningar skulle kunna få gränsöverskridande konsekvenser.

f) [...].

g) Om entiteten identifieras som en kritisk entitet enligt Europaparlamentets och rådets direktiv (EU) XXXX/XXXX[28] [direktivet om kritiska entiteters motståndskraft] **[**eller som en entitet likvärdig med en kritisk entitet i enlighet med artikel 7 i det direktivet**]**.

2a. **Oberoende av deras storlek är detta direktiv också tillämpligt på de offentliga förvaltningsentiteter hos nationella regeringar som är erkända som sådana i en medlemsstat i enlighet med den nationella lagstiftningen och som avses i punkt 9 i bilaga I. Medlemsstaterna får fastställa att detta direktiv också är tillämpligt på offentliga förvaltningsentiteter på regional och lokal nivå.**

28 [ange fullständig titel och EUT-hänvisning om detta är känt]

3. [...]

Detta direktiv påverkar inte medlemsstaternas ansvar att skydda den nationella säkerheten eller deras befogenhet att skydda andra väsentliga statliga funktioner, inbegripet att säkerställa statens territoriella integritet och upprätthålla lag och ordning.

3a. 1. Detta direktiv ska inte tillämpas på följande:

a) Entiteter som inte omfattas av unionslagstiftningen och under alla omständigheter alla entiteter som främst bedriver verksamhet på områdena försvar, nationell säkerhet, allmän säkerhet eller brottsbekämpning oberoende av vilken entitet som bedriver denna verksamhet och huruvida det är en offentlig eller privat entitet, utan att det påverkar tillämpningen av punkt 2.

b) Entiteter som bedriver verksamhet inom rättsväsende, parlament eller centralbanker. […]

2. Om offentliga förvaltningsentiteter bedriver verksamhet på dessa områden endast som en del av sin samlade verksamhet ska de undantas i sin helhet från direktivets tillämpningsområde.

3aa. Detta direktiv ska inte tillämpas på följande:

i) Verksamhet som bedrivs av entiteter som inte omfattas av unionslagstiftningen och under alla omständigheter all verksamhet som rör nationell säkerhet eller försvar, oberoende av vilken entitet som bedriver denna verksamhet och huruvida det är en offentlig eller privat entitet.

ii) Verksamhet som bedrivs av entiteter inom rättsväsende, parlament och centralbanker och på området allmän säkerhet, inbegripet offentliga förvaltningsentiteter som bedriver brottsbekämpande verksamhet för att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder.

3aaa. De skyldigheter som fastställs i detta direktiv medför inte tillhandahållande av information vars utlämnande strider mot medlemsstaternas väsentliga intressen i fråga om nationell säkerhet, allmän säkerhet eller försvar.

3aaaa. Detta direktiv påverkar inte tillämpningen av unionslagstiftningen om skydd av personuppgifter, i synnerhet förordning (EU) 2016/679 och direktiv 2002/58/EG.

3b. Detta direktiv är inte tillämpligt på entiteter som är undantagna från Europaparlamentets och rådets förordning (EU) XXXX/XXXX [DORA-förordningen] i enlighet med artikel 2.4 i den förordningen.

4. Detta direktiv påverkar inte tillämpningen av […][29] [...] Europaparlamentets och rådets direktiv 2011/93/EU[30] och 2013/40/EU[31].

5. Utan att det påverkar tillämpningen av artikel 346 i EUF-fördraget ska information som är konfidentiell enligt unionsbestämmelser och nationella bestämmelser, såsom bestämmelser om affärshemligheter, utbytas med kommissionen och andra berörda myndigheter **i enlighet med detta direktiv** endast när ett sådant utbyte är nödvändigt för att tillämpa detta direktiv. Den information som utbyts ska begränsas till vad som är relevant och proportionellt för ändamålet med utbytet. Vid utbytet ska informationens konfidentialitet bevaras och väsentliga eller viktiga entiteters säkerhets- och affärsintressen skyddas.

---

29 [...]

30 Europaparlamentets och rådets direktiv 2011/93/EU av den 13 december 2011 om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi samt om ersättande av rådets rambeslut 2004/68/RIF (EUT L 335, 17.12.2011, s. 1).

31 Europaparlamentets och rådets direktiv 2013/40/EU av den 12 augusti 2013 om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF (EUT L 218, 14.8.2013, s. 8).

Artikel 2a

Väsentliga och viktiga entiteter

1. Av de entiteter som detta direktiv är tillämpligt på ska följande betraktas som väsentliga:

i) Entiteter av en av de typer som anges i punkterna 1–8a och 10 i bilaga I till detta direktiv och som överstiger trösklarna för medelstora företag såsom de definieras i kommissionens rekommendation 2003/361/EG.

ii) De medelstora entiteter som avses i artikel 2.2 a i.

iii) De entiteter som avses i artikel 2.2 a ii och iv i detta direktiv, oavsett storlek.

iv) De entiteter som avses i artikel 2.2 g och 2.2a i detta direktiv, oavsett storlek.

v) Entiteter som medlemsstaterna före detta direktivs ikraftträdande har identifierat som leverantörer av samhällsviktiga tjänster i enlighet med direktiv (EU) 2016/1148 eller den nationella lagstiftningen, om sådana entiteter har inrättats av medlemsstaterna.

vi) Entiteter som överstiger trösklarna för medelstora företag såsom de definieras i kommissionens rekommendation 2003/361/EG av den typ som anges i bilaga II, vilka medlemsstaterna fastslår är väsentliga på grundval av de kriterier som anges i artikel 2.2 c–e.

vii) Medelstora entiteter i den mening som avses i kommissionens rekommendation 2003/361/EG, vilka medlemsstaterna fastslår är väsentliga på grundval av de kriterier som anges i artikel 2.2 c–e.

viii) Mikroentiteter eller små entiteter i den mening som avses i kommissionens rekommendation 2003/361/EG, som anges i punkt 2 a i eller identifieras i enlighet med punkt 2 c–e i denna artikel, vilka medlemsstaterna fastslår är väsentliga på grundval av nationella riskbedömningar.

2. Av de entiteter som detta direktiv är tillämpligt på ska följande betraktas som viktiga:

i) Entiteter av en av de typer som anges i bilaga I till detta direktiv och som anses vara medelstora företag i den mening som avses i kommissionens rekommendation 2003/361/EG samt entiteter av den typ som anges i bilaga II och som uppnår eller överstiger trösklarna för medelstora företag i den mening som avses i kommissionens rekommendation 2003/361/EG[32].

ii) De entiteter som avses i artikel 2.2 iii i detta direktiv, oavsett storlek.

iii) De små entiteter och mikroentiteter som avses i artikel 2.2 a i.

iv) De små entiteter och mikroentiteter som medlemsstaterna fastslår är viktiga på grundval av artikel 2.2 c–e.

---

32 **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 2a

Anmälningsmekanismer

1. **Medlemsstaterna får inrätta nationella mekanismer för självanmälan som kräver att alla entiteter som omfattas av detta direktiv – till de behöriga myndigheterna enligt detta direktiv eller till de organ som utsetts för detta ändamål av medlemsstaterna – åtminstone lämnar in namn, adress och kontaktuppgifter samt information om vilken sektor de är verksamma inom eller vilken typ av tjänst de tillhandahåller och, i tillämpliga fall, en förteckning över de medlemsstater där de tillhandahåller tjänster som omfattas av detta direktiv.**

2. **Senast den [12 månader efter tidsfristen för införlivande av detta direktiv]** ska medlemsstaterna […], **med avseende på de entiteter som de har identifierat i enlighet med artikel 2.2 b–e**, till kommissionen **åtminstone** lämna **relevant information om antalet identifierade entiteter, vilken sektor de tillhör eller vilken typ av tjänst de tillhandahåller enligt bilagorna och de särskilda bestämmelser i artikel 2.2 på grundval av vilka de identifierades.** Medlemsstaterna ska regelbundet och minst vartannat år därefter se över […] **denna information** […] och vid behov uppdatera den.

Artikel 2b

Sektorsspecifika unionsakter

1. Om det […] i sektorsspecifika **unionsrätts**akter […] föreskrivs att väsentliga eller viktiga entiteter […] ska anta åtgärder för att hantera cybersäkerhetsrisker eller anmäla **betydande** incidenter eller […] cyberhot, och om dessa krav har minst samma verkan som de skyldigheter som fastställs i detta direktiv, ska de relevanta bestämmelserna i detta direktiv**, inbegripet bestämmelserna om tillsyn och efterlevnadskontroll i kapitel VI,** inte tillämpas på **sådana entiteter**. **Om de sektorsspecifika unionsrättsakterna inte omfattar alla entiteter inom en viss sektor som omfattas av detta direktivs tillämpningsområde, ska de relevanta bestämmelserna i detta direktiv fortsätta att tillämpas på de entiteter som inte omfattas av dessa sektorsspecifika bestämmelser.**

2. De krav som avses i punkt 1 i denna artikel ska anses ha samma verkan som de skyldigheter som fastställs i detta direktiv om respektive sektorsspecifik unionsakt föreskriver omedelbar, och i förekommande fall automatisk och direkt, tillgång till incidentanmälningarna från de behöriga myndigheterna enligt detta direktiv eller de utsedda CSIRT-enheterna och om

a) riskhanteringsåtgärderna för cybersäkerhet åtminstone har samma verkan som de åtgärder som föreskrivs i artikel 18.1 och 18.2 i detta direktiv eller

b) kraven på anmälan av betydande incidenter åtminstone har samma verkan som de krav som fastställs i artikel 20.1–20.6.

3. Kommissionen ska regelbundet se över tillämpningen av kraven om samma verkan enligt punkterna 1 och 2 i denna artikel med avseende på sektorsspecifika bestämmelser i unionsrättsakter. Kommissionen ska samråda med samarbetsgruppen och Enisa när den förbereder de periodiska översynerna.

Artikel 3

Minimiharmonisering

Utan att det påverkar tillämpningen av deras övriga skyldigheter enligt unionsrätten får medlemsstaterna – **på de områden som omfattas av detta direktiv** – […] anta eller behålla bestämmelser som säkerställer en högre cybersäkerhetsnivå.

Artikel 4

Definitioner

I detta direktiv gäller följande definitioner:

1. *nätverks- och informationssystem*:

   a) Ett elektroniskt kommunikationsnät i den mening som avses i artikel 2.1 i direktiv (EU) 2018/1972.

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

   c) Digitala uppgifter som lagras, behandlas, hämtas eller överförs med sådana hjälpmedel som omfattas av leden a och b för att de ska kunna drivas, användas, skyddas och underhållas. säkerhet i nätverks- och informationssystem:

2. *säkerhet i nätverks- och informationssystem*: nätverks- och informationssystems förmåga att med en viss tillförlitlighetsnivå motstå **händelser** som **kan** undergräva **[…]** tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller **hos** de tjänster som erbjuds genom eller är tillgängliga via dessa nätverks- och informationssystem.

2a. *elektronisk kommunikationstjänst*: elektroniska […] kommunikationstjänster i den mening som avses i artikel 2.4 i direktiv (EU) 2018/1972.

3. *cybersäkerhet*: cybersäkerhet i den mening som avses i artikel 2.1 i Europaparlamentets och rådets förordning (EU) 2019/881[33].

4. *nationell strategi för **cybersäkerhet***: […] en enhetlig ram i en medlemsstat som tillhandahåller styrning för att uppnå strategiska mål och prioriteringar på […] **cybersäkerhetsområdet** […] i den medlemsstaten.

5. *incident*: varje händelse som undergräver tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de […] tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem.

5a. *storskalig cyberincident*: en incident som har betydande påverkan på två eller flera medlemsstater eller som leder till störningar som är så omfattande att den berörda medlemsstaten inte kan hantera dem på egen hand.

---

33 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 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15).

6. *incidenthantering*: alla åtgärder och förfaranden som syftar till att upptäcka, analysera, begränsa och reagera på en incident.

6a. *risk*: risken 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.

7. *cyberhot*: cyberhot i den mening som avses i artikel 2.8 i förordning (EU) 2019/881.

7a. ***betydande cyberhot*: ett cyberhot som, på grund av dess tekniska egenskaper, kan antas ha potential att ha en allvarlig påverkan på nätverks- och informationssystemen för en entitet eller dess användare genom att vålla betydande materiella eller immateriella förluster.**

8. *sårbarhet*: en svaghet, känslighet eller brist hos en IKT-tillgång eller ett system […] som kan utnyttjas genom ett cyberhot.

8a. *tillbud*: en händelse som potentiellt skulle ha kunnat orsaka skada på nätverks- och informationssystemen för en entitet eller dess användare, men som framgångsrikt hindrades från att utvecklas fullt ut.

9. *företrädare*: en i unionen etablerad fysisk eller juridisk person som uttryckligen har utsetts att agera för i) en leverantör av DNS-tjänster, en registreringsenhet för toppdomäner, en leverantör av molntjänster, en leverantör av datacentraltjänster eller en leverantör av nätverk för innehållsleverans enligt punkt 8 i bilaga I eller ii) ej i unionen etablerade entiteter enligt punkt […] **6** i bilaga II till vilka en nationell behörig myndighet eller en CSIRT-enhet kan vända sig i stället för entiteten, i frågor som gäller de skyldigheter som den entiteten har enligt detta direktiv.

10. *standard*: en standard i den mening som avses i artikel 2.1 i Europaparlamentets och rådets förordning (EU) nr 1025/2012[34].

11. *teknisk specifikation*: en teknisk specifikation i den mening som avses i artikel 2.4 i förordning (EU) nr 1025/2012.

12. *internetknutpunkt (IXP)*: en nätfacilitet som möjliggör sammankoppling av mer än två oberoende nät (autonoma system), främst i syfte att underlätta utbytet av internettrafik; en IXP tillhandahåller sammankoppling enbart för autonoma system och kräver inte att den internettrafik som passerar mellan två deltagande autonoma system ska passera genom ett tredje autonomt system och ändrar inte heller trafiken eller påverkar den på något annat sätt.

13. *domännamnssystem (DNS)*: ett hierarkiskt distribuerat namngivningssystem som gör det möjligt för slutanvändare att nå tjänster och resurser på internet.

14. *leverantör av DNS-tjänster*: en entitet som tillhandahåller rekursiva eller auktoritativa tjänster för att lösa domännamnsfrågor **för** […] **tredjepartsanvändning, med undantag för rotnamnsservrar** […].

---

34 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).

15. *registreringsenhet för toppdomäner*: en enhet som har delegerats en specifik toppdomän och som ansvarar för administrationen av toppdomänen, inbegripet registreringen av domännamn under toppdomänen och den tekniska driften av toppdomänen, inbegripet drift av dess namnservrar, underhåll av dess databaser och distribution av zonfiler för toppdomänen mellan namnservrar**, med undantag för situationer där toppdomänen används av ett register endast för eget bruk**.

15a. *entiteter som tillhandahåller domännamnsregistreringstjänster för toppdomäner*: registreringsenheter för toppdomäner, ombud för toppdomäner och företrädare för ombud, såsom återförsäljare och leverantörer av proxytjänster.

16. *digital tjänst*: en tjänst i den mening som avses i artikel 1.1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535[35].

16a. *betrodda tjänster*: betrodda tjänster i den mening som avses i artikel 3.16 i förordning (EU) nr 910/2014.

[35] Europaparlamentets och rådets direktiv (EU) 2015/1535 av den 9 september 2015 om ett informationsförfarande beträffande tekniska föreskrifter och beträffande föreskrifter för informationssamhällets tjänster (EUT L 241, 17.9.2015, s. 1).

16b. ***kvalificerad tillhandahållare av betrodda tjänster*****: en kvalificerad tillhandahållare av betrodda tjänster i den mening som avses i artikel 3.20 i förordning (EU) nr 910/2014.**

17. *marknadsplats online*: en digital tjänst i den mening som avses i artikel 2 n i Europaparlamentets och rådets direktiv 2005/29/EG[36].

18. *sökmotor*: en digital tjänst i den mening som avses i artikel 2.5 i Europaparlamentets och rådets förordning (EU) 2019/1150[37].

19. *molntjänst*: en digital tjänst som möjliggör administration av beställtjänster och bred fjärråtkomst till en skalbar och elastisk pool av delbara […] dataresurser**, inbegripet när de är distribuerade på flera platser**.

20. *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 datatransporttjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll.

---

36 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) (EUT L 149, 11.6.2005, s. 22).

37 Europaparlamentets och rådets förordning (EU) 2019/1150 av den 20 juni 2019 om främjande av rättvisa villkor och transparens för företagsanvändare av onlinebaserade förmedlingstjänster (EUT L 186, 11.7.2019, s. 57).

21. *nätverk för innehållsleverans*: 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.

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

23. *offentlig förvaltningsentitet*: en entitet **som erkänts som sådan i en medlemsstat enligt nationell rätt** [...] och som uppfyller följande kriterier:

    a) Den har inrättats för att tillgodose behov i det allmännas intresse och har inte industriell eller kommersiell karaktär.

    b) Den har ställning som juridisk person **eller har lagstadgad rätt att agera för en annan entitet som har ställning som juridisk person**.

    c) Den finansieras till största delen av staten, en regional myndighet eller andra offentligrättsliga organ, eller står under administrativ tillsyn av sådana myndigheter eller organ, eller har ett förvaltnings-, lednings- eller kontrollorgan där mer än hälften av ledamöterna utses av staten, regionala myndigheter eller andra offentligrättsliga organ.

    d) Den har befogenhet att rikta administrativa eller reglerande beslut till fysiska eller juridiska personer som påverkar deras rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital.

24. *entitet*: varje fysisk eller juridisk person som bildats och erkänts som sådan enligt nationell rätt där den etablerats och som i eget namn får utöva rättigheter och ha skyldigheter.

25. *väsentlig entitet*: varje entitet av en typ [...] **som anges i bilaga I och som anses vara ”väsentlig” i enlighet med artikel 2a.1**.

26. *viktig entitet*: varje entitet av den typ [...] **som anges i bilagorna I och II och som anses vara ”viktig” i enlighet med artikel 2a.2**.

26a. ***IKT-produkt*****: en IKT-produkt i den mening som avses i artikel 2.12 i förordning (EU) 2019/881.**

26aa. ***IKT-tjänst*****: en IKT-tjänst i den mening som avses i artikel 2.13 i förordning (EU) 2019/881.**

26ab. ***IKT-process*****: en IKT-process i den mening som avses i artikel 2.14 i förordning (EU) 2019/881.**

26ac. ***leverantör av hanterade tjänster*****: en entitet som tillhandahåller tjänster, såsom nätverk, tillämpningar, infrastruktur och säkerhet, genom löpande och regelbunden förvaltning, stöd och aktiv administration i kundernas lokaler, i den egna datacentralen (värdtjänst) eller i en tredje parts datacentral.**

26ad. ***leverantör av hanterade säkerhetstjänster*****: en entitet som tillhandahåller övervakning och förvaltning på entreprenad av säkerhetsanordningar och säkerhetssystem; vanliga tjänster inbegriper förvaltade brandväggstjänster, intrångsdetektering, virtuella privata nätverk, sårbarhetsskanning och antivirustjänster.**

Detta omfattar även användning av säkerhetscentrum med hög tillgänglighet (antingen från de egna anläggningarna eller från andra datacentralleverantörer) i syfte att tillhandahålla tjänster dygnet runt sju dagar i veckan, vilka är avsedda att minska mängden operativ säkerhetspersonal som ett företag behöver anställa, utbilda och behålla i syfte att upprätthålla en acceptabel säkerhetsstatus.

KAPITEL II

Samordnade regelverk för cybersäkerhet

Artikel 5

Nationell strategi för cybersäkerhet

1. Varje medlemsstat ska anta en nationell strategi för cybersäkerhet som anger strategiska mål och relevanta politiska och reglerande åtgärder, i syfte att uppnå och upprätthålla en hög cybersäkerhetsnivå. Den nationella strategin för cybersäkerhet ska särskilt inbegripa följande:

   a) [...] Mål och prioriteringar för medlemsstatens strategi för cybersäkerhet.

   b) En styrningsram för att uppnå dessa mål och prioriteringar, inbegripet de politiska åtgärder som avses i punkt 2 och roller och ansvarsområden för de olika myndigheter och aktörer som är involverade i genomförandet av strategin [...].

   c) [...] **Vägledning** för att identifiera relevanta tillgångar och **bedöma** cybersäkerhetsrisker i den medlemsstaten[...].

   d) En identifiering av åtgärder som säkerställer beredskap inför, svar på och återställande efter incidenter, inklusive samarbete mellan offentlig och privat sektor.

   e) [...]

f) En politisk ram för förbättrad samordning mellan de behöriga myndigheterna enligt detta direktiv och enligt Europaparlamentets och rådets direktiv (EU) XXXX/XXXX[38] [direktivet om kritiska entiteters motståndskraft], i syfte att utbyta information om **cybersäkerhetsrisker,** [...] cyberhot **och cyberincidenter samt om icke-cyberrelaterade risker, hot och incidenter** och utföra tillsynsuppgifter **när så är lämpligt**.

fa) En politisk ram för samordning och samarbete mellan de behöriga myndigheterna enligt detta direktiv och behöriga myndigheter som utsetts i enlighet med den sektorsspecifika lagstiftningen.

2. Som en del av den nationella strategin för cybersäkerhet ska medlemsstaterna särskilt anta följande:

a) En politik för cybersäkerhet i leveranskedjan för IKT-produkter och IKT-tjänster som används av [...] entiteter när de tillhandahåller sina tjänster.

b) **En politik** [...] för att inkludera och specificera cybersäkerhetsrelaterade krav för IKT-produkter och IKT-tjänster vid offentlig upphandling**, inbegripet cybersäkerhetscertifiering**.

c) En politik **för hantering av sårbarheter, inbegripet främjande och underlättande av** [...] **frivillig** samordnad information om sårbarheter i den mening som avses i artikel 6**.1**.

d) En politik för att upprätthålla den allmänna tillgängligheten**,** [...] integriteten **och konfidentialiteten** hos den offentliga kärnan i det öppna internet.

e) En politik för att främja och utveckla **cybersäkerhetsutbildning,** cybersäkerhetskompetens, medvetandehöjande åtgärder samt forsknings- och utvecklingsinitiativ.

---

38 *[ange fullständig titel och EUT-hänvisning om detta är känt]*

f) En politik för stöd till akademiska institutioner och forskningsinstitut för att utveckla cybersäkerhetsverktyg och säker nätinfrastruktur.

g) En politik, relevanta förfaranden och lämpliga verktyg för informationsutbyte för att stödja ett frivilligt informationsutbyte om cybersäkerhet mellan företag i enlighet med unionsrätten.

h) En politik som tillgodoser särskilda behov hos små och medelstora företag, särskilt de som inte omfattas av detta direktiv, när det gäller vägledning och stöd för att förbättra deras motståndskraft mot cyberhot.

3. Medlemsstaterna ska meddela sina nationella strategier för cybersäkerhet till kommissionen inom tre månader från det att de antagits. **Härvid** får medlemsstaterna undanta **delar av strategin som rör** [...] den nationella säkerheten.

4. Medlemsstaterna ska regelbundet och minst vart [...] **femte** år bedöma sina nationella strategier för cybersäkerhet på grundval av centrala resultatindikatorer och vid behov ändra dem. Europeiska unionens cybersäkerhetsbyrå (Enisa) ska på **medlemsstaternas** begäran bistå medlemsstaterna vid utarbetandet av en nationell strategi och centrala resultatindikatorer för bedömningen av strategin.

Artikel 6

Samordnad information om sårbarheter och ett europeiskt sårbarhetsregister

1. Varje medlemsstat ska utse en av sina CSIRT-enheter enligt artikel 9 till samordnare för den samordnade informationen om sårbarheter. Den utsedda CSIRT-enheten ska fungera som betrodd mellanhand och vid behov underlätta interaktionen mellan en rapporterande entitet**, ägaren av den potentiella sårbarheten** och tillverkare eller leverantörer av IKT-produkter eller IKT-tjänster. **Varje fysisk eller juridisk person får, eventuellt anonymt, rapportera en sådan sårbarhet som avses i artikel 4.8 till den utsedda CSIRT-enheten. Den utsedda CSIRT-enheten ska säkerställa en noggrann uppföljning av rapporten samt en konfidentiell identitet för den person som rapporterar sårbarheten.** Om en rapporterad sårbarhet [...] **skulle kunna ha en betydande påverkan på entiteter i fler än en medlemsstat**, ska den utsedda CSIRT-enheten i varje berörd medlemsstat **i tillämpliga fall** samarbeta med **andra utsedda CSIRT-enheter inom** CSIRT-nätverket.

2. Enisa ska utveckla och underhålla ett europeiskt sårbarhetsregister **i samråd med samarbetsgruppen**. I detta syfte ska Enisa inrätta och underhålla lämpliga informationssystem, riktlinjer och förfaranden, särskilt för att göra det möjligt för viktiga och väsentliga entiteter och deras leverantörer av nätverks- och informationssystem att **på frivillig basis** lämna information om och registrera **allmänt kända** sårbarheter hos IKT-produkter eller IKT-tjänster, samt för att ge alla berörda parter tillgång till den information om sårbarheter som finns i registret. Registret ska särskilt innehålla information som beskriver sårbarheten, den berörda IKT-produkten eller IKT-tjänsten och hur allvarlig sårbarheten är med tanke på de omständigheter under vilka den kan utnyttjas, tillgången till relaterade programfixar och, i avsaknad av tillgängliga programfixar, vägledning **utfärdad av nationella behöriga myndigheter eller CSIRT-enheter som är** riktad till användare av sårbara produkter och tjänster om hur riskerna med meddelade sårbarheter kan minskas. **Enisa ska säkerställa att det europeiska sårbarhetsregistret använder säker och motståndskraftig kommunikations- och informationsinfrastruktur.**

Artikel 7

Nationella ramar för hantering av cybersäkerhetskriser

1. Varje medlemsstat ska utse en eller flera behöriga myndigheter med ansvar för hanteringen av storskaliga **cyber**incidenter och **cyber**kriser. Medlemsstaterna ska se till att de behöriga myndigheterna har tillräckliga resurser för att kunna utföra sina uppgifter på ett ändamålsenligt och effektivt sätt. **Medlemsstaterna ska säkerställa samstämmighet med befintliga ramar för allmän krishantering.**

2. För tillämpning av detta direktiv ska varje medlemsstat identifiera vilka kapaciteter, tillgångar och förfaranden som kan användas i händelse av en kris.

3. Varje medlemsstat ska anta en nationell incident- och krishanteringsplan för cybersäkerhet där mål och villkor för hanteringen av storskaliga cyberincidenter och cyberkriser fastställs. Planen ska särskilt innehålla följande:

   a) Målen för nationella beredskapsåtgärder och beredskapsverksamheter.

   b) De nationella behöriga myndigheternas uppgifter och ansvarsområden.

   c) Krishanteringsförfaranden för cybersäkerhet**, inbegripet deras integrering i den allmänna nationella ramen för krishantering,** och kanaler för informationsutbyte.

   d) Beredskapsåtgärder, inbegripet regelbundna övningar och utbildningsverksamhet.

   e) Berörda offentliga och privata parter och berörd infrastruktur.

   f) Nationella förfaranden och arrangemang mellan relevanta nationella myndigheter och organ för att säkerställa att medlemsstaten på ett ändamålsenligt sätt kan delta i och stödja en samordnad hantering av storskaliga cyberincidenter och cyberkriser på unionsnivå.

4. Medlemsstaterna ska [...] **meddela** kommissionen när en behörig myndighet utsetts enligt punkt 1 och lämna in **relevant information avseende kraven i punkt 3 i denna artikel för** deras nationella incident- och krishanteringsplaner för cybersäkerhet [...] inom tre månader från det att myndigheterna utsetts och dessa planer antagits. Medlemsstaterna får undanta specifik information [...] om och i den utsträckning det är [...] nödvändigt för den nationella säkerheten**, den allmänna säkerheten eller försvaret**.

Artikel 8

Nationella behöriga myndigheter och gemensamma kontaktpunkter

1. Varje medlemsstat ska utse en eller flera behöriga myndigheter med ansvar för cybersäkerhet och för de tillsynsuppgifter som avses i kapitel VI i detta direktiv. Medlemsstaterna får för detta ändamål utse en eller flera befintliga myndigheter.

2. De behöriga myndigheter som avses i punkt 1 ska övervaka tillämpningen av detta direktiv på nationell nivå.

3. Varje medlemsstat ska utse en nationell gemensam kontaktpunkt för cybersäkerhet (nedan kallad gemensam kontaktpunkt). Om en medlemsstat bara utser en behörig myndighet, ska denna behöriga myndighet också vara den gemensamma kontaktpunkten i den medlemsstaten.

4. Varje gemensam kontaktpunkt ska utöva en sambandsfunktion som säkerställer ett gränsöverskridande samarbete mellan medlemsstatens myndigheter och relevanta myndigheter i andra medlemsstater och ett sektorsövergripande samarbete med andra nationella behöriga myndigheter i medlemsstaten.

5. Medlemsstaterna ska säkerställa att de behöriga myndigheter som avses i punkt 1 och de gemensamma kontaktpunkterna har tillräckliga resurser för att på ett ändamålsenligt och effektivt sätt kunna utföra de uppgifter de tilldelas och därigenom uppnå målen med detta direktiv. Medlemsstaterna ska säkerställa att de utsedda företrädarna i den samarbetsgrupp som avses i artikel 12 samarbetar på ett ändamålsenligt, effektivt och säkert sätt.

6. Varje medlemsstat ska utan onödigt dröjsmål underrätta kommissionen om utnämningen av den behöriga myndighet som avses i punkt 1 och den gemensamma kontaktpunkt som avses i punkt 3 och deras uppgifter samt alla senare ändringar. Varje medlemsstat ska offentliggöra utnämningen. Kommissionen ska offentliggöra en förteckning över utsedda gemensamma kontaktpunkter.

Artikel 9

Enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter)

1. Varje medlemsstat ska utse en eller flera CSIRT-enheter som ska uppfylla kraven i artikel 10.1, omfattande minst de sektorer, delsektorer och entiteter som avses i bilagorna I och II, och som ansvarar för hanteringen av incidenter i enlighet med ett tydligt fastställt förfarande. En CSIRT-enhet får inrättas inom en behörig myndighet som avses i artikel 8.

2. Medlemsstaterna ska säkerställa att varje CSIRT-enhet har tillräckliga resurser för att på ett ändamålsenligt sätt kunna utföra sina uppgifter enligt artikel 10.2. **Vid utförandet av dessa uppgifter får CSIRT-enheterna prioritera tillhandahållandet av särskilda tjänster till entiteter på grundval av en riskbaserad metod.**

3. Medlemsstaterna ska säkerställa att varje CSIRT-enhet har tillgång till en lämplig, säker och motståndskraftig kommunikations- och informationsinfrastruktur för utbyte av information med väsentliga och viktiga entiteter och andra relevanta berörda parter. För detta ändamål ska medlemsstaterna se till att CSIRT-enheterna bidrar till införandet av säkra verktyg för informationsutbyte.

4. CSIRT-enheterna ska samarbeta och vid behov utbyta relevant information i enlighet med artikel 26 med betrodda sektoriella eller sektorsövergripande grupper av väsentliga och viktiga entiteter.

5. CSIRT-enheter ska delta i peer [...] **learning** som organiseras i enlighet med artikel 16.

6. Medlemsstaterna ska säkerställa ett ändamålsenligt, effektivt och säkert samarbete mellan sina CSIRT-enheter i det CSIRT-nätverk som avses i artikel 13.

7. Medlemsstaterna ska utan onödigt dröjsmål meddela kommissionen de CSIRT-enheter som utsetts i enlighet med punkt 1, den CSIRT-samordnare som utsetts i enlighet med artikel 6.1 och deras respektive uppgifter i förhållande till de entiteter som avses i bilagorna I och II.

8. Medlemsstaterna får begära Enisas bistånd vid inrättandet av nationella CSIRT-enheter.

Artikel 10

Krav på CSIRT-enheter och deras uppgifter

1. CSIRT-enheter ska uppfylla följande krav:

   a) De ska säkerställa en hög nivå av tillgänglighet för sina kommunikations[...]**kanaler** genom att undvika felkritiska systemdelar och ska kunna kontaktas och kontakta andra när som helst och på flera olika sätt. De ska tydligt ange kommunikationskanalerna och underrätta användargrupper och samarbetspartner om dessa.

   b) Deras lokaler och de informationssystem som de använder sig av ska vara belägna på säkra platser.

c) De ska ha ett ändamålsenligt system för handläggning och dirigering av förfrågningar, särskilt för att underlätta ändamålsenliga och effektiva överlämnanden.

d) De ska ha tillräckligt med personal för att ständigt kunna vara tillgängliga.

e) De ska utrustas med system med inbyggd redundans och reservlokaler för att säkerställa kontinuiteten i deras tjänster.

f) De ska kunna delta i internationella samarbetsnätverk.

2. CSIRT-enheter ska ha följande uppgifter:

a) Övervakning av cyberhot, sårbarheter och incidenter på nationell nivå.

b) Tillhandahållande av tidiga varningar, larm, meddelanden och spridning av information till väsentliga och viktiga entiteter samt till **behöriga myndigheter och** andra relevanta berörda parter om cyberhot, sårbarheter och incidenter.

c) Vidtagande av åtgärder till följd av incidenter.

d) Insamling och analys av forensiska uppgifter och tillhandahållande av dynamisk risk- och incidentanalys och situationsmedvetenhet när det gäller cybersäkerhet.

e) Tillhandahållande **[...]** av en proaktiv skanning av nätverks- och informationssystem**en** [...] **i syfte att upptäcka sårbarheter med potentiellt betydande påverkan, förutsatt att det – om entiteten inte har gett sitt samtycke – inte görs något intrång i nätverks- och informationssystemen och att deras funktion inte påverkas negativt.**

f) Deltagande i CSIRT-nätverket och tillhandahållande av ömsesidigt bistånd **i enlighet med deras kapacitet och befogenheter** till andra medlemmar i nätverket på deras begäran.

fa) I tillämpliga fall, att fungera som processamordnare för den samordnade informationen om sårbarheter i enlighet med artikel 6.1, vilket särskilt ska omfatta att underlätta interaktionen mellan rapporterande entiteter, ägaren av den potentiella sårbarheten och tillverkaren eller leverantören av IKT-produkter eller IKT-tjänster i fall där detta är nödvändigt, att identifiera och kontakta berörda entiteter, stödja rapporterande entiteter, förhandla om tidsramar för meddelande av information och hantera sårbarheter som påverkar flera organisationer (samordnad information om sårbarheter omfattande flera parter).

3. CSIRT-enheter ska upprätta samarbetsförbindelser med relevanta aktörer inom den privata sektorn i syfte att bättre uppnå direktivets mål.

3a. CSIRT-enheter får upprätta samarbetsförbindelser med nationella CSIRT-enheter i tredjeländer. Som en del av detta samarbete får de utbyta relevant information, inbegripet personuppgifter i enlighet med unionsrätten om dataskydd.

4. För att underlätta samarbetet ska CSIRT-enheterna främja antagande och användning av gemensamma eller standardiserade metoder, klassificeringssystem och taxonomier när det gäller följande:

a) Förfaranden för incidenthantering.

b) Hantering av cybersäkerhetskriser.

c) Samordnad information om sårbarheter.

Artikel 11

Samarbete på nationell nivå

1. Om de är separata ska de behöriga myndigheter som avses i artikel 8, den gemensamma kontaktpunkten och CSIRT-enheten eller CSIRT-enheterna i en och samma medlemsstat samarbeta sinsemellan när det gäller fullgörandet av skyldigheter enligt detta direktiv.

2. Medlemsstaterna ska se till att antingen deras behöriga myndigheter eller deras CSIRT-enheter mottar anmälningar om incidenter, betydande cyberhot och tillbud som lämnas in i enlighet med detta direktiv. Om en medlemsstat beslutar att dess CSIRT-enheter inte ska motta sådana anmälningar ska CSIRT-enheterna, i den mån det är nödvändigt för att de ska kunna utföra sina uppgifter, beviljas tillgång till uppgifter om incidenter som anmälts av väsentliga eller viktiga entiteter i enlighet med artikel 20.

3. Varje medlemsstat ska se till att dess behöriga myndigheter eller CSIRT-enheter informerar sin gemensamma kontaktpunkt om de anmälningar om incidenter, betydande cyberhot och tillbud som lämnas in i enlighet med detta direktiv.

4. I den utsträckning det är nödvändigt för ett ändamålsenligt fullgörande av de uppgifter och skyldigheter som fastställs i detta direktiv ska medlemsstaterna säkerställa ett lämpligt samarbete mellan behöriga myndigheter, **CSIRT-enheter,** gemensamma kontaktpunkter samt brottsbekämpande myndigheter, dataskyddsmyndigheter och de **behöriga** myndigheter **som utsetts** [...] enligt direktiv (EU) XXXX/XXXX [direktivet om kritiska entiteters motståndskraft][...]], **de behöriga myndigheterna enligt kommissionens genomförandeförordning 2019/1583, de nationella regleringsmyndigheter som utsetts i enlighet med direktiv (EU) 2018/1972, de nationella myndigheter som utsetts i enlighet med artikel 17 i förordning (EU) nr 910/2014,** [...] de nationella finansmyndigheter som utsetts i enlighet med Europaparlamentets och rådets förordning (EU) XXXX/XXXX [DORA-förordningen]**, samt de behöriga myndigheter som utsetts genom andra sektorsspecifika unionsrättsakter,** i den medlemsstaten.

5. Medlemsstaterna ska säkerställa att deras behöriga myndigheter **enligt detta direktiv och de behöriga myndigheter som utsetts i enlighet med direktiv (EU) XXXX/XXXX [direktivet om kritiska entiteters motståndskraft]** regelbundet **utbyter** [...] information [...] om **identifiering av kritiska entiteter,** cybersäkerhetsrisker, cyber**hot och cyberincidenter samt om icke-cyberrelaterade risker, hot och incidenter** som berör väsentliga entiteter som identifierats som kritiska **[**eller som likvärdiga med kritiska entiteter,**]** i enlighet med direktiv (EU) XXXX/XXXX [direktivet om kritiska entiteters motståndskraft], samt om de åtgärder som [...] vidtagits till följd av dessa risker och incidenter. **Medlemsstaterna ska också säkerställa att de behöriga myndigheterna enligt detta direktiv** [...] **och de behöriga myndigheter som utsetts enligt förordning XXXX/XXXX [DORA-förordningen], direktiv 2018/1972 och förordning (EU) nr 910/2014 regelbundet utbyter relevant information.**

När det gäller tillhandahållare av betrodda tjänster och [...]i synnerhet[...] i fall där denna tillsynsroll enligt detta direktiv tilldelas ett annat organ än de tillsynsorgan som utsetts i enlighet med förordning (EU) nr 910/2014, ska de nationella behöriga myndigheterna enligt detta direktiv samarbeta nära och i god tid genom att utbyta relevant information i syfte att säkerställa att tillsynen är effektiv och att tillhandahållare av betrodda tjänster uppfyller kraven i detta direktiv och denna förordning [XXXX/XXXX], **och i förekommande fall ska den nationella behöriga myndigheten enligt detta direktiv utan onödigt dröjsmål informera eIDA:s tillsynsorgan om ett anmält betydande cyberhot eller en anmäld betydande cyberincident som påverkar betrodda tjänster**.

5a. I syfte att [...] förenkla rapporteringen av incidenter får medlemsstaterna inrätta en gemensam kontaktpunkt för alla anmälningar som krävs enligt detta direktiv och även enligt förordning (EU) 2016/679 och direktiv 2002/58/EG, när så är lämpligt. Medlemsstaterna får använda den gemensamma kontaktpunkten för anmälningar som krävs enligt andra sektorsspecifika unionsrättsakter. Denna gemensamma kontaktpunkt ska inte påverka tillämpningen av bestämmelserna i förordning (EU) 2016/679 och direktiv 2002/58/EG, särskilt inte de som rör oberoende tillsynsmyndigheter.

KAPITEL III

EU-samarbete

Artikel 12

Samarbetsgrupp

1. För att stödja och underlätta strategiskt samarbete och informationsutbyte mellan medlemsstaterna **samt** [...] **stärka förtroende och tillit** [...] inrättas härmed en samarbetsgrupp.

2. Samarbetsgruppen ska utföra sina uppgifter på grundval av de tvååriga arbetsprogram som avses i punkt 6.

3. Samarbetsgruppen ska bestå av företrädare för medlemsstater, kommissionen och Enisa. Europeiska utrikestjänsten ska delta som observatör i samarbetsgruppens verksamhet. De europeiska tillsynsmyndigheterna **och de behöriga myndigheter som utsetts enligt förordning (EU) XXXX/XXXX [DORA-förordningen]** [...] får delta i samarbetsgruppens verksamhet **i enlighet med artikel 42.1 i förordning (EU) XXXX/XXXX [DORA-förordningen].**

   När så är lämpligt får samarbetsgruppen bjuda in företrädare för relevanta intressenter att delta i arbetet.

   Kommissionen ska tillhandahålla sekretariatet.

4. Samarbetsgruppen ska ha följande uppgifter:

   a) Tillhandahållande av vägledning till behöriga myndigheter angående införlivande och genomförande av detta direktiv**.**

   aa) Tillhandahållande av vägledning angående utarbetande och genomförande av strategier för den samordnade information om sårbarheter som avses i artiklarna 5.2 c och 6.1.

b) Utbyte av bästa praxis och information i fråga om genomförandet av detta direktiv, bland annat när det gäller cyberhot, incidenter, sårbarheter, tillbud, initiativ för att öka medvetenheten, utbildning, övningar och kompetens, kapacitetsuppbyggnad, standarder och tekniska specifikationer.

c) Utbyte av råd och samarbete med kommissionen om framväxande politiska initiativ för cybersäkerhet.

d) Utbyte av råd och samarbete med kommissionen om utkast till kommissionens genomförandeakter […] som antas i enlighet med detta direktiv.

e) Utbyte av bästa praxis och information med relevanta institutioner, organ och byråer på unionsnivå.

ea) Diskussioner om genomförandet av sektorsspecifik lagstiftning med cybersäkerhetsaspekter.

f) Diskussioner om de rapporter om […] **peer learning** som avses i artikel 16.7.

g) Diskussioner om **erfarenheterna från** […] sådan gemensam tillsynsverksamhet i gränsöverskridande fall som avses i artikel 34.

h) Tillhandahållande av strategisk vägledning till CSIRT-nätverket **och EU-CyCLONe** om specifika framväxande frågor.

ha) Diskussioner om den politiska uppföljningen av storskaliga cyberincidenter på grundval av lärdomarna från CSIRT-nätverket och EU-CyCLONe.

i) Bidrag till cybersäkerhetskapaciteten i hela unionen genom att underlätta utbytet av nationella tjänstemän i form av ett kapacitetsuppbyggnadsprogram som inbegriper personal från medlemsstaternas behöriga myndigheter eller CSIRT-enheter.

j) Anordnande av regelbundna gemensamma möten med relevanta privata intressenter från hela unionen för att diskutera gruppens verksamhet och inhämta synpunkter på framväxande politiska frågor.

k) Diskussioner om det arbete som utförts i samband med cybersäkerhetsövningar, inbegripet det arbete som utförs av Enisa.

ka) Inrättande av en peer learning-mekanism i enlighet med artikel 16 i detta direktiv.

5. Samarbetsgruppen får begära en teknisk rapport från CSIRT-nätverket om utvalda frågor.

6. Samarbetsgruppen ska senast den... [24 månader efter dagen för detta direktivs ikraftträdande] och därefter vartannat år upprätta ett arbetsprogram för de åtgärder som ska vidtas för att genomföra dess mål och uppgifter. Tidsramen för det första program som antas enligt detta direktiv ska anpassas till tidsramen för det sista program som antas enligt direktiv (EU) 2016/1148.

7. Kommissionen får anta genomförandeakter i vilka fastställs de förfaranden som krävs för samarbetsgruppens verksamhet. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 37.2.

8. Samarbetsgruppen ska regelbundet och minst en gång om året sammanträda med den grupp för kritiska entiteters motståndskraft som inrättats enligt direktiv (EU) XXXX/XXXX [direktivet om kritiska entiteters motståndskraft], för att främja strategiskt samarbete och **underlätta** informationsutbyte.

Artikel 13

CSIRT-nätverk

1. För att bidra till utvecklingen av förtroende och tillit och för att främja ett snabbt och ändamålsenligt operativt samarbete mellan medlemsstaterna inrättas härmed ett nätverk för nationella CSIRT-enheter.

2. CSIRT-nätverket ska bestå av företrädare för medlemsstaternas CSIRT-enheter **som utsetts i enlighet med artikel 9** och Cert-EU. Kommissionen ska delta i CSIRT-nätverket som observatör. Enisa ska tillhandahålla sekretariatet och aktivt stödja samarbetet mellan CSIRT-enheterna.

3. CSIRT-nätverket ska ha följande uppgifter:

   a) Att utbyta information om CSIRT-enheternas kapacitet.

   b) Att utbyta relevant information om incidenter, tillbud, cyberhot, risker och sårbarheter.

ba) Att utbyta information med avseende på publikationer och rekommendationer om cybersäkerhet.

bb) Att utbyta tekniska lösningar som underlättar den tekniska hanteringen av incidenter.

bc) Att utbyta bästa praxis, verktyg och processer när det gäller CSIRT-enheternas uppgifter.

c) Att, på begäran av en […] **medlem i** CSIRT-nätverket som potentiellt berörs av en incident, utbyta och diskutera information om den incidenten och relaterade cyberhot, risker och sårbarheter.

d) Att, på begäran av en […] **medlem i** CSIRT-nätverket, diskutera och om möjligt genomföra en samordnad åtgärd till följd av en incident som har identifierats inom den medlemsstatens jurisdiktion.

e) Att ge medlemsstaterna stöd när det gäller att hantera gränsöverskridande incidenter i enlighet med detta direktiv.

f) Att samarbeta **och utbyta bästa praxis** med samt ge stöd till de utsedda CSIRT-enheter som avses i artikel 6 när det gäller hanteringen av samordnad information […] om sårbarheter som berör flera tillverkare eller leverantörer av IKT-produkter, IKT-tjänster och IKT-processer som är etablerade i olika medlemsstater.

g) Att diskutera och identifiera ytterligare former av operativt samarbete, inbegripet när det gäller

i) kategorier av cyberhot och incidenter,

ii) tidiga varningar,

iii) ömsesidigt bistånd,

iv) principer och metoder för samordning i samband med åtgärder mot gränsöverskridande risker och incidenter,

v) bidrag till den nationella incident- och krishanteringsplan för cybersäkerhet som avses i artikel 7.3 **på begäran av en medlemsstat**.

h) Att informera samarbetsgruppen om sin verksamhet och om ytterligare former av operativt samarbete som diskuteras enligt led g **och** vid behov begära vägledning i detta avseende.

i) Att utvärdera cybersäkerhetsövningar, bland annat sådana som anordnas av Enisa.

j) Att på begäran av en enskild CSIRT-enhet diskutera den enhetens kapacitet och beredskap.

k) Att samarbeta och utbyta information med säkerhetscentrum (SOC) på regional nivå och unionsnivå, för att förbättra den gemensamma situationsmedvetenheten om incidenter och hot i hela unionen.

l) Att diskutera de […] **peer learning-**rapporter som avses i artikel 16.7.

m) Att utfärda riktlinjer för att underlätta en mer enhetlig operativ praxis när det gäller tillämpningen av bestämmelserna i denna artikel om operativt samarbete.

4. I samband med den översyn som avses i artikel 35 ska CSIRT-nätverket, inom [24 månader efter dagen för detta direktivs ikraftträdande] och därefter vartannat år, bedöma de framsteg som gjorts med det operativa samarbetet och utarbeta en rapport. Rapporten ska särskilt innehålla slutsatser om resultaten av den **peer learning** [...] som avses i artikel 16 och som utförts med avseende på nationella CSIRT-enheter, inbegripet slutsatser och rekommendationer i enlighet med den artikeln. Rapporten ska även lämnas till samarbetsgruppen.

5. CSIRT-nätverket ska anta sin arbetsordning.

6. CSIRT-nätverket ska samarbeta med EU-CyCLONe på grundval av överenskomna förfaranden.

Artikel 14

Det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe)

1. För att stödja en samordnad hantering av storskaliga cyberincidenter och cyberkriser på operativ nivå och säkerställa ett regelbundet informationsutbyte mellan medlemsstaterna och unionens institutioner, organ och byråer inrättas härmed Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe).

2. EU-CyCLONe ska bestå av de företrädare för medlemsstaternas **cyber**krishanteringsmyndigheter som utsetts i enlighet med artikel 7 […]. **Kommissionen ska delta i nätverkets verksamhet som observatör.** Enisa ska tillhandahålla nätverkets sekretariat och stödja ett säkert informationsutbyte **samt tillhandahålla nödvändiga verktyg för att stödja samarbete mellan medlemsstaterna så att ett säkert informationsutbyte säkerställs**.

När så är lämpligt får EU-CyCLONe bjuda in företrädare för relevanta intressenter att delta i arbetet.

3. EU-CyCLONe ska ha följande uppgifter:

a) Att öka beredskapen för hantering av storskaliga cyberincidenter och cyberkriser.

b) Att utveckla en gemensam situationsmedvetenhet om […] storskaliga cyberincidenter och cyberkriser.

ba) Att bedöma konsekvenserna och effekterna av relevanta storskaliga cyberincidenter och föreslå möjliga begränsningsåtgärder.

c) Att samordna hanteringen av storskaliga cyberincidenter och cyberkriser och ge stöd till beslutsfattande på politisk nivå i samband med sådana incidenter och kriser.

d) Att**, på begäran av en medlemsstat,** diskutera **dess** nationella incident- och **kris**hanteringsplaner för cybersäkerhet enligt artikel 7**.3** […].[...]

4. EU-CyCLONe ska anta sin arbetsordning.

5. EU-CyCLONe ska regelbundet rapportera till samarbetsgruppen **om hanteringen av storskaliga cyberincidenter och cyberkriser** […], med särskild inriktning på deras inverkan på väsentliga och viktiga entiteter.

6. EU-CyCLONe ska samarbeta med CSIRT-nätverket på grundval av överenskomna förfaranden.

7. EU-CyCLONe ska senast den [24 månader efter den dag då detta direktiv träder i kraft] lämna en rapport till Europaparlamentet och rådet med en bedömning av dess arbete.

Artikel 14a

Internationellt samarbete

Unionen får, i förekommande fall, ingå internationella avtal, i enlighet med artikel 218 i EUF-fördraget, med tredjeländer eller internationella organisationer, och därvid tillåta och organisera deras deltagande i vissa av samarbetsgruppens, CSIRT-nätverkets och EU-CyCLONes verksamheter i enlighet med unionsrätten om dataskydd.

Artikel 15

Rapport om cybersäkerhetssituationen i unionen

1. Enisa ska, i samarbete med kommissionen **och samarbetsgruppen**, vartannat år utfärda en rapport om cybersäkerhetssituationen i unionen. Rapporten ska **framför allt** innehålla följande:

   aa) En riskbedömning av cybersäkerheten på unionsnivå, med beaktande av hotbilden.

   a) […] **En bedömning av** utvecklingen av cybersäkerhetskapaciteten i den offentliga och privata sektorn i hela unionen.

   b) [...]

   c) **En aggregerad bedömning, på grundval av** […] **kvantitativa och kvalitativa** cybersäkerhets**indikatorer,** som ger en […] **översikt** över mognadsnivån på cybersäkerhetskapaciteten**, inbegripet den sektorsspecifika kapaciteten**.

2. Rapporten ska innehålla särskilda politiska rekommendationer för att höja cybersäkerhetsnivån i hela unionen och en sammanfattning av resultaten för den aktuella perioden från de tekniska lägesrapporter om cybersäkerhet i EU som Enisa utfärdat i enlighet med artikel 7.6 i förordning (EU) 2019/881.

Artikel 16

Peer learning

1. **För att stärka det ömsesidiga förtroendet, uppnå en hög gemensam cybersäkerhetsnivå och stärka medlemsstaternas cybersäkerhetskapacitet och cybersäkerhetsstrategier som är nödvändiga för ett effektivt genomförande av detta direktiv** ska […] **samarbetsgruppen – med stöd av kommissionen och** efter samråd med […] Enisa **samt, när så är relevant, CSIRT-nätverket –** senast **24 […]** månader efter detta direktivs ikraftträdande fastställa en metod **[…] för ett objektivt, icke-diskriminerande och rättvist […] peer learning-**system **[…] rörande** medlemsstaternas **[…] genomförande av detta direktiv. Det är frivilligt att delta i peer learning. Systemet ska bestå av bedömningsomgångar** […] som ska utföras av […] cybersäkerhetsexperter […] från medlemsstaterna […] och ska omfatta […] **en eller flera av** följande **aspekter**:

   i) […] Genomförandet av de riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter som avses i artiklarna 18 och 20.

   ii) Kapaciteten […], inbegripet tillgängliga […] resurser, och […] det arbete som utförs av de behöriga myndigheterna **enligt artikel 8 och CSIRT-nätverket enligt artikel 9**.

[...]

i**ii)**[...] […] **Genomförandet av** det ömsesidiga bistånd som avses i artikel 34.

iv) […] **Genomförandet av** den ram för informationsutbyte som avses i artikel 26 […].

2. **De kriterier på grundval av vilka medlemsstaterna ska utse experter som är berättigade att delta i peer learning-omgångarna ska vara** […] objektiva, icke-diskriminerande, rättvisa och transparenta […] **och ska ingå i den metod som avses i punkt 1**. Enisa och kommissionen […] **får** utse experter som ska delta som observatörer i […] **peer learning-omgångarna**. [...]

3. [...].

3a. Innan peer learning-omgångarna inleds får medlemsstaterna göra en självbedömning av de aspekter som ingår i den särskilda peer learning-omgången och överlämna denna självbedömning till de utsedda experter som avses i punkt 2.

4. […] **Peer learning** […] **får** inbegripa […] **fysiska** eller virtuella besök på plats och distansbaserade utbyten. Med hänsyn till principen om gott samarbete ska de medlemsstater som […] **deltar i peer learning** förse de utsedda experterna med den […] information som krävs för bedömningen […]**, utan att det påverkar den nationella lagstiftningen eller unionslagstiftningen om skydd av sekretessbelagda eller säkerhetsskyddsklassificerade uppgifter eller skyddet av väsentliga statliga funktioner, såsom nationell säkerhet.** All information som erhålls genom […] **peer learning-processen** får endast användas för dess ändamål. De experter som deltar i […] **peer learning** får inte lämna ut känslig eller konfidentiell information som erhållits i […] **detta sammanhang** till någon tredje part. **Den medlemsstat som deltar i peer learning får invända mot utnämningen av särskilda experter av vederbörligen motiverade skäl som meddelas samarbetsgruppen.**

5. När aspekter **har omfattats av en peer learning-omgång** […] ska de inte bli föremål för ytterligare […] **peer learning-omgångar** […] **för de deltagande** medlemsstaterna under de […] **fyra** år som följer på slutförandet av **den** […] **peer learning-omgången, om inte den berörda medlemsstaten begär det eller samtycker till det på förslag** […] av **samarbetsgruppen […].**

6. [...]

7. Experter som deltar i **peer learning-omgångar** […] ska utarbeta rapporter om resultatet och slutsatserna av […] **bedömningarna**. **Medlemsstaterna ska ges möjlighet att lämna synpunkter på respektive utkast till rapporter, vilka ska bifogas rapporten. Slut**rapporterna ska lämnas till […] samarbetsgruppen[…]. **Medlemsstaterna får besluta att offentliggöra sina respektive rapporter.**

KAPITEL IV

Riskhanterings- och rapporteringskrav för cybersäkerhet

AVSNITT I

Riskhantering och rapportering i fråga om cybersäkerhet

Artikel 17

Styrning

1. Medlemsstaterna ska säkerställa att väsentliga och viktiga entiteters ledningsorgan godkänner de riskhanteringsåtgärder för cybersäkerhet som dessa entiteter vidtar för att följa artikel 18, övervakar genomförandet av dem och […] **kan ställas** till svars om entiteterna inte fullgör sina skyldigheter enligt den artikeln.

   Tillämpningen av denna punkt ska inte påverka tillämpningen av medlemsstaternas nationella lagar när det gäller bestämmelserna om ansvar i offentliga institutioner samt ansvaret för statligt anställda och valda och utnämnda tjänstepersoner.

2. Medlemsstaterna ska säkerställa att **ledningsorganets medlemmar […] är skyldiga att** regelbundet genomgå […] utbildning för att skaffa sig tillräckliga kunskaper och kompetenser så att de förstår och kan bedöma cybersäkerhetsrisker och praxis för hantering av cybersäkerhet och deras inverkan på entitetens verksamhet.

Artikel 18

Riskhanteringsåtgärder för cybersäkerhet

1a. **I detta direktiv tillämpas en ”allriskstrategi” som omfattar skydd av nätverks- och informationssystem och deras fysiska miljö mot varje händelse som kan undergräva tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystemen.**

1. Medlemsstaterna ska säkerställa att väsentliga och viktiga entiteter […] vidtar lämpliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i de nätverks- […] och informationssystem som de använder för att tillhandahålla sina tjänster. Med beaktande av den senaste tekniska utvecklingen **och genomförandekostnaderna** ska dessa åtgärder säkerställa en säkerhetsnivå i nätverks- och informationssystemen som är lämplig i förhållande till den föreliggande risken. **Vid bedömningen av dessa åtgärders proportionalitet ska vederbörlig hänsyn tas till graden av entitetens exponering för risker, dess storlek, sannolikheten för att en incident inträffar och incidentens allvarlighetsgrad. Med beaktande av nivån på och typen av risk för samhället vid incidenter som påverkar väsentliga eller viktiga entiteter kan de riskhanteringsåtgärder för cybersäkerhet som åläggs viktiga entiteter vara mindre strikta än de åtgärder som åläggs väsentliga entiteter.**

2. De åtgärder som avses i punkt 1 ska åtminstone inbegripa

a) strategier för riskanalys och informationssystemens säkerhet,

b) incidenthantering (förebyggande, upptäckt, […] åtgärder **och återhämtning från [**...] incidenter),

c) driftskontinuitet och krishantering,

d) säkerhet i leveranskedjan, inbegripet säkerhetsaspekter som rör förbindelserna mellan varje entitet och dess **direkt**leverantörer eller tjänsteleverantörer, såsom leverantörer av datalagrings- och databehandlingstjänster eller hanterade säkerhetstjänster,

e) säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem, inbegripet hantering av och information om sårbarheter,

f) strategier och förfaranden […] för att bedöma effektiviteten i riskhanteringsåtgärderna för cybersäkerhet,

g) **en politik för** användningen av kryptografi och kryptering,

ga) personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning.

3. Medlemsstaterna ska säkerställa att entiteter, när de överväger de lämpliga åtgärder som avses i punkt 2 d, […] **är skyldiga att** beakta de sårbarheter som är specifika för varje **direkt**leverantör och tjänsteleverantör och den övergripande kvaliteten på deras leverantörers och tjänsteleverantörers produkter och cybersäkerhetspraxis, inbegripet deras förfaranden för säker utveckling. **Medlemsstaterna ska också säkerställa att entiteterna är skyldiga att beakta resultatet av de samordnade riskbedömningar som utförs i enlighet med artikel 19.1 när de överväger lämpliga åtgärder enligt punkt 2 d.**

4. Medlemsstaterna ska säkerställa att om en entitet finner att dess tjänster eller uppgifter inte uppfyller kraven i punkt 2, ska den utan onödigt dröjsmål vidta alla nödvändiga korrigerande åtgärder för att den berörda tjänsten ska uppfylla kraven.

5. Kommissionen får anta genomförandeakter för att fastställa de tekniska och metodologiska specifikationerna **samt vid behov de sektorsspecifika särdragen** för de aspekter som anges i punkt 2 **i denna artikel**. **Kommissionen ska senast den [18 månader efter detta direktivs ikraftträdande] anta genomförandeakter för att fastställa de tekniska och metodologiska specifikationerna för de entiteter som avses i artikel 24.1 och de tillhandahållare av betrodda tjänster som avses i punkt 8 i bilaga I. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 37.2.** När kommissionen […] utarbetar […] **dessa genomförande**akter ska den […] i största möjliga utsträckning **följa** internationella och europeiska standarder samt relevanta tekniska specifikationer **och utbyta råd med samarbetsgruppen och Enisa om utkastet till genomförandeakt i enlighet med artikel 12.4 d.**

6. [...]

Artikel 19

EU-samordnade riskbedömningar av kritiska leveranskedjor

1. Samarbetsgruppen får, i samarbete med kommissionen och Enisa, utföra samordnade säkerhetsriskbedömningar av specifika kritiska leveranskedjor för IKT-tjänster, IKT-system eller IKT-produkter, med beaktande av tekniska och, i relevanta fall, icke-tekniska riskfaktorer.

2. Kommissionen ska, efter samråd med samarbetsgruppen och Enisa, identifiera de specifika kritiska IKT-tjänster, IKT-system eller IKT-produkter som kan bli föremål för den samordnade riskbedömning som avses i punkt 1.

Artikel 20

Rapporteringsskyldigheter

1. Medlemsstaterna ska säkerställa att väsentliga och viktiga entiteter utan onödigt dröjsmål anmäler alla incidenter som har en betydande inverkan på tillhandahållandet av deras tjänster till de behöriga myndigheterna eller CSIRT-enheten i enlighet med punkterna 3 och 4. När så är lämpligt ska dessa entiteter utan onödigt dröjsmål till mottagarna av deras tjänster anmäla **dessa** incidenter som sannolikt inverkar negativt på tillhandahållandet av de berörda tjänsterna. Medlemsstaterna ska säkerställa att dessa entiteter bland annat rapporterar information som gör det möjligt för de behöriga myndigheterna eller CSIRT-enheten att fastställa incidentens eventuella gränsöverskridande verkningar. **Anmälan av incidenten ska i sig inte medföra ökat ansvar för den anmälande entiteten.**

2. [...]

I tillämpliga fall ska […] **de väsentliga och viktiga** entiteterna utan onödigt dröjsmål underrätta de mottagare av deras tjänster som kan påverkas av ett betydande cyberhot om eventuella åtgärder eller avhjälpande arrangemang som dessa mottagare kan vidta som svar på hotet. När så är lämpligt ska entiteterna också underrätta dessa mottagare om själva hotet. Anmälan av incidenten ska **i sig** inte medföra ökat ansvar för den anmälande entiteten.

3. En incident ska anses vara betydande om

a) den har orsakat eller kan orsaka **allvarliga** […] driftsstörningar **för tjänsten** eller ekonomiska förluster för den berörda entiteten,

b) den har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiella eller immateriella förluster.

4. När det gäller det anmälningsförfarande som avses i punkt 1 ska medlemsstaterna säkerställa att de berörda entiteterna lämnar följande till de behöriga myndigheterna eller CSIRT-enheten:

a) Utan onödigt dröjsmål och under alla omständigheter inom 24 timmar efter att ha fått kännedom om incidenten, en första anmälan **som en tidig varning** där det i tillämpliga fall ska anges om incidenten antas ha orsakats av olagliga eller avsiktligt skadliga handlingar.

b) På begäran av en behörig myndighet eller en CSIRT-enhet, en delrapport om relevanta statusuppdateringar.

c) Senast en månad efter inlämningen av den […] **första anmälan** som avses i led a, en **slut**rapport som minst ska innehålla följande:

i) En detaljerad beskrivning av incidenten, dess allvarlighetsgrad och dess konsekvenser.

ii) Den typ av hot eller grundorsak som sannolikt utlöst incidenten.

iii) Tillämpade och pågående avhjälpande åtgärder.

Medlemsstaterna ska föreskriva att den berörda entiteten i vederbörligen motiverade fall och i samförstånd med de behöriga myndigheterna eller CSIRT-enheten får frångå de tidsfrister som anges i leden a och c. **Framför allt kan en avvikelse från tidsfristen i led c motiveras i fall där incidenten alltjämt pågår.**

5. De behöriga nationella myndigheterna eller CSIRT-enheten ska […] **utan onödigt dröjsmål** efter mottagandet av den första anmälan som avses i punkt 4 a lämna ett svar till den anmälande entiteten, inbegripet initial återkoppling om incidenten och, på entitetens begäran, vägledning om genomförandet av möjliga avhjälpande åtgärder. Om CSIRT-enheten inte har mottagit den anmälan som avses i punkt 1 ska vägledningen tillhandahållas av den behöriga myndigheten i samarbete med CSIRT-enheten. CSIRT-enheten ska tillhandahålla ytterligare tekniskt stöd om den berörda entiteten begär det. Om incidenten misstänks vara av brottslig art ska de behöriga nationella myndigheterna eller CSIRT-enheten också tillhandahålla vägledning om rapportering av incidenten till brottsbekämpande myndigheter.

6. När så är lämpligt, och särskilt om den incident som avses i punkt 1 berör två eller flera medlemsstater, ska den behöriga myndigheten, CSIRT-enheten eller **den gemensamma kontaktpunkten** informera andra berörda medlemsstater och Enisa om incidenten. **Denna information ska åtminstone innehålla de uppgifter som anges i punkt 4 i denna artikel.** Därvid ska de behöriga myndigheterna, CSIRT-enheterna och de gemensamma kontaktpunkterna, i enlighet med unionsrätten eller nationell lagstiftning som är förenlig med unionsrätten, bevara entitetens säkerhets- och affärsintressen samt den tillhandahållna informationens konfidentialitet.

7. Om allmänhetens medvetenhet är nödvändig för att förhindra en incident eller för att hantera en pågående incident, eller om information om incidenten på annat sätt ligger i allmänhetens intresse, får den behöriga myndigheten eller CSIRT-enheten och, om det är lämpligt, myndigheterna eller CSIRT-enheterna i andra berörda medlemsstater, efter samråd med den berörda entiteten, informera allmänheten om incidenten eller kräva att entiteten gör det.

8. På begäran av den behöriga myndigheten eller CSIRT-enheten ska den gemensamma kontaktpunkten vidarebefordra de anmälningar som mottagits i enlighet med punkt […] 1 […] till de gemensamma kontaktpunkterna i andra berörda medlemsstater.

9. Den gemensamma kontaktpunkten ska […] **var sjätte månad** lämna in en sammanfattande rapport till Enisa med anonymiserade och aggregerade uppgifter om incidenter, betydande cyberhot och tillbud som anmälts i enlighet med punkt […] 1 […] och i enlighet med artikel 27. För att bidra till att jämförbar information lämnas får Enisa utfärda teknisk vägledning om parametrarna för den information som tas med i den sammanfattande rapporten. **Enisa ska var sjätte månad informera samarbetsgruppen och CSIRT-nätverket om sina slutsatser om de mottagna anmälningarna.**

10. De behöriga myndigheterna ska förse de behöriga myndigheter som utsetts i enlighet med direktiv (EU) XXXX/XXXX [direktivet om kritiska entiteters motståndskraft] med information om incidenter och cyberhot som anmälts i enlighet med punkterna 1 och 2 av väsentliga entiteter som identifierats som kritiska **[**eller som likvärdiga med kritiska entiteter**]**, i enlighet med direktiv (EU) XXXX/XXXX [direktivet om kritiska entiteters motståndskraft].

11. Kommissionen får anta genomförandeakter som närmare anger typen av information i och formatet och förfarandet för de anmälningar som lämnas i enlighet med punkterna 1 och 2. Kommissionen får också anta genomförandeakter som närmare anger i vilka fall en incident ska anses vara betydande enligt punkt 3. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 37.2.

Artikel 21

Användning av europeiska ordningar för cybersäkerhetscertifiering

1. För kontroll av att vissa krav enligt artikel 18 är uppfyllda **får medlemsstaterna kräva att entiteterna använder vissa IKT-produkter, IKT-tjänster och IKT-processer som är certifierade** enligt särskilda europeiska ordningar för cybersäkerhetscertifiering som antagits i enlighet med artikel 49 i förordning (EU) 2019/881. De **IKT-**produkter, **IKT-**tjänster och **IKT-**processer som är föremål för certifiering kan utvecklas av en väsentlig eller viktig entitet eller upphandlas från tredje part.

2. Kommissionen får […] anta […] **genomförande**akter som anger vilka kategorier av väsentliga **eller viktiga** entiteter som ska vara skyldiga **att använda vissa certifierade IKT-produkter, IKT-tjänster och IKT-processer eller** erhålla ett certifikat […] inom ramen för [...] **de specifika europeiska ordningar för cybersäkerhetscertifiering som antagits i enlighet med artikel 49 i förordning (EU) 2019/881.** [...] **Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 37.2. När kommissionen utarbetar sådana genomförandeakter ska den, i enlighet med artikel 56 i förordning (EU) 2019/881,**

   i) beakta åtgärdernas konsekvenser i kostnadsavseende för tillverkarna och leverantörerna av de berörda IKT-produkterna, IKT-tjänsterna eller IKT-processerna och för användarna samt de samhälleliga och/eller ekonomiska vinsterna med den förväntade höjningen av säkerhetsnivån för de berörda IKT-produkterna, IKT-tjänsterna eller IKT-processerna och tillgången till alternativ på marknaden,

   ii) genomföra en öppen, transparent och inkluderande samrådsprocess med alla berörda intressenter och medlemsstater,

iii) beakta eventuella genomförandefrister och övergångsåtgärder och övergångsperioder, i synnerhet åtgärdernas tänkbara inverkan på tillverkare eller leverantörer av IKT-produkter, IKT-tjänster eller IKT-processer, eller användarna, däribland små och medelstora företag, samt

iv) ta i beaktande existensen och införlivandet av relevant nationell rätt i medlemsstaterna.

3. Kommissionen kan begära att Enisa utarbetar ett förslag till certifieringsordning **eller ser över en befintlig europeisk ordning för cybersäkerhetscertifiering** i enlighet med artikel 48.2 i förordning (EU) 2019/881 i fall där det inte finns någon lämplig europeisk ordning för cybersäkerhetscertifiering för tillämpningen av punkt 2 **i den här artikeln**.

Artikel 22

Standardisering

1. För att främja en enhetlig tillämpning av artikel 18.1 och 18.2 ska medlemsstaterna, utan att föreskriva eller gynna användning av en viss typ av teknik, uppmuntra användningen av europeiska eller internationellt accepterade standarder och specifikationer av relevans för säkerheten i nätverks- och informationssystem.

2. Enisa ska i samarbete med medlemsstaterna utarbeta råd och riktlinjer för de tekniska områden som ska beaktas när det gäller punkt 1 samt för redan befintliga standarder, inklusive medlemsstaternas nationella standarder, som skulle kunna täcka dessa områden.

Artikel 23

Databaser över domännamn och registreringsuppgifter

1. För att bidra till säkerheten, stabiliteten och motståndskraften hos domännamnssystemet ska medlemsstaterna säkerställa att registreringsenheterna för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster för toppdomäner samlar in och upprätthåller korrekta **[…]** och fullständiga registreringsuppgifter för domännamn i en särskild databas med tillbörlig aktsamhet i enlighet med unionens dataskyddslagstiftning när det gäller personuppgifter.

2. Medlemsstaterna ska säkerställa att de databaser med registreringsuppgifter för domännamn som avses i punkt 1 innehåller relevant information för att identifiera och kontakta innehavarna av domännamnen och de kontaktpunkter som administrerar domännamnen under toppdomänerna**, vilket inbegriper minst följande uppgifter:**

   a) Domännamn.

   b) Registreringsdatum.

   c) Uppgifter om registranten, inbegripet

      i) för privatpersoner – förnamn, efternamn och e-postadress,

      ii) för juridiska personer – namn och e-postadress.

3. Medlemsstaterna ska säkerställa att registreringsenheterna för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster för toppdomäner har strategier och förfaranden för att säkerställa att databaserna innehåller korrekt och fullständig information. Medlemsstaterna ska säkerställa att sådana strategier och förfaranden offentliggörs.

4. Medlemsstaterna ska säkerställa att registreringsenheterna för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster för toppdomäner utan onödigt dröjsmål efter registreringen av ett domännamn offentliggör domänregistreringsuppgifter som inte är personuppgifter.

5. Medlemsstaterna ska säkerställa att registreringsenheterna för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster för toppdomäner ger åtkomst till specifika registreringsuppgifter för domännamn på lagliga och vederbörligen motiverade begäranden från legitima åtkomstsökande, i enlighet med unionens dataskyddslagstiftning. Medlemsstaterna ska säkerställa att registreringsenheterna för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster för toppdomäner utan onödigt dröjsmål **och under alla omständigheter inom 72 timmar** besvarar alla begäranden om åtkomst. Medlemsstaterna ska säkerställa att strategierna och förfarandena för utlämning av sådana uppgifter offentliggörs.

Avsnitt II

Jurisdiktion och registrering

Artikel 24

Jurisdiktion och territorialitet

1a. Entiteter enligt detta direktiv ska anses omfattas av jurisdiktionen i den medlemsstat där de tillhandahåller sina tjänster. De entiteter som avses i punkterna 1–7 och 10 i bilaga I samt de tillhandahållare av betrodda tjänster och de leverantörer av internetknutpunkter som avses i punkt 8 i bilaga I och punkterna 1–5 i bilaga II ska anses omfattas av jurisdiktionen i den medlemsstat på vars territorium de är etablerade.

1. Leverantörer av DNS-tjänster, registreringsenheter för toppdomäner […] **och entiteter som tillhandahåller domännamnsregistreringstjänster för toppdomäner,** leverantörer av molntjänster, leverantörer av datacentraltjänster, […] leverantörer av nätverk för innehållsleverans, **leverantörer av hanterade tjänster och leverantörer av hanterade säkerhetstjänster** enligt punkt**erna** 8 **och 8a** i bilaga I samt digitala leverantörer enligt punkt 6 i bilaga II ska anses omfattas av jurisdiktionen i den medlemsstat där de har sitt huvudsakliga etableringsställe i unionen.

2. Vid tillämpning av detta direktiv ska entiteter som avses i punkt 1 anses ha sitt huvudsakliga etableringsställe i unionen i den medlemsstat där besluten om riskhanteringsåtgärder för cybersäkerhet **i huvudsak** fattas. Om **platsen där sådana beslut i huvudsak fattas inte kan fastställas eller om** sådana beslut inte fattas vid något etableringsställe i unionen ska det huvudsakliga etableringsstället anses vara beläget i den medlemsstat där entiteterna har det etableringsställe som har flest anställda i unionen. **Om tjänsterna tillhandahålls av en koncern ska det huvudsakliga etableringsstället anses vara koncernens huvudsakliga etableringsställe.**

3. Om en entitet som avses i punkt 1 inte är etablerad i unionen, men erbjuder tjänster inom unionen, ska den utse en företrädare i unionen. Företrädaren ska vara etablerad i en av de medlemsstater där tjänsterna erbjuds. Entiteten ska anses omfattas av jurisdiktionen i den medlemsstat där företrädaren är etablerad. Om det inte finns någon utsedd företrädare i unionen enligt denna artikel får varje medlemsstat där entiteten tillhandahåller tjänster vidta rättsliga åtgärder mot entiteten för bristande fullgörande av skyldigheterna enligt detta direktiv.

4. Det faktum att en entitet som avses i punkt 1 utsett en företrädare ska inte påverka eventuella rättsliga åtgärder mot entiteten själv.

4a. De medlemsstater som har mottagit en begäran om ömsesidigt bistånd med avseende på de entiteter som avses i punkt 1 får, inom ramen för begäran, vidta lämpliga tillsyns- och efterlevnadskontrollåtgärder med avseende på den berörda entitet som tillhandahåller tjänster eller som har ett nätverks- och informationssystem inom deras territorium.

Artikel 25

Register för vissa entiteter för digital infrastruktur och digitala leverantörer

1. […] **Medlemsstaterna ska säkerställa att** […] de entiteter **som avses i artikel 24.1 och som har sitt huvudsakliga etableringsställe på deras territorium eller, om de inte är etablerade i unionen, vars utsedda företrädare i unionen är etablerad på deras territorium är skyldiga att** […] lämna följande uppgifter **till de behöriga myndigheterna** […] senast [12 månader efter direktivets ikraftträdande]:

a) Entitetens namn.

aa) Typen av entitet enligt bilagorna I och II till detta direktiv.

b) Adressen till entitetens huvudsakliga etableringsställe och andra rättsligt giltiga etableringsställen i unionen eller, om entiteten inte är etablerad i unionen, till dess företrädare som utsetts i enlighet med artikel 24.3.

c) Aktuella kontaktuppgifter, inklusive e-postadresser och telefonnummer till entiteten **och dess företrädare**.

d) De medlemsstater där entiteten tillhandahåller tjänsten.

I tillämpliga fall ska denna information lämnas via den nationella mekanism […] för självanmälan som avses i artikel 2a.

2. **Medlemsstaterna ska säkerställa att** […] de entiteter som avses i punkt 1 **[…] även anmäler** alla ändringar av de uppgifter som de lämnat enligt punkt 1 utan dröjsmål och under alla omständigheter inom tre månader från den dag då ändringen fått verkan.

3. […] **Medlemsstaternas gemensamma kontaktpunkter** ska vidarebefordra **den information som avses i punkterna 1 och 2** […] till […] **Enisa**. [...]

3a. På grundval av den information som mottagits i enlighet med punkt 3 i denna artikel ska Enisa skapa och upprätthålla ett register över de entiteter som avses i punkt 1. På begäran av medlemsstaterna ska Enisa ge de berörda behöriga myndigheterna tillgång till registret, samtidigt som skydd av informationens konfidentialitet säkerställs i tillämpliga fall.

4. [...]

KAPITEL V

Informationsutbyte

Artikel 26

Arrangemang för informationsutbyte om cybersäkerhet

1. […] Medlemsstaterna ska säkerställa att väsentliga och viktiga entiteter **på frivillig basis** får utbyta relevant information om cybersäkerhet sinsemellan, inbegripet information om cyberhot, sårbarheter, **tillbud,** angreppsindikatorer, taktik, tekniker och förfaranden, cybersäkerhetsvarningar och konfigurationsverktyg, om sådant informationsutbyte

   a) syftar till att förebygga, upptäcka, reagera på eller begränsa incidenter,

b) höjer cybersäkerhetsnivån, särskilt genom att öka medvetenheten om cyberhot, begränsa eller hindra sådana hots spridningsförmåga eller stödja en rad defensiva förmågor, avhjälpande av och information om sårbarheter, metoder för att upptäcka hot, strategier för begränsning av hot eller reaktions- och återhämtningsfaser.

2. Medlemsstaterna ska säkerställa att informationsutbytet sker inom […] grupper av väsentliga och viktiga entiteter. Sådant utbyte ska genomföras med hjälp av arrangemang för informationsutbyte med hänsyn till den potentiellt känsliga karaktären hos den information som utbyts […].

3. Medlemsstaterna […] **får** fastställa regler som anger förfarandet för, de operativa aspekterna av (inbegripet användning av särskilda IKT-plattformar), innehållet i och villkoren för de arrangemang för informationsutbyte som avses i punkt 2. Sådana regler […] **får** också fastställa närmare bestämmelser om offentliga myndigheters deltagande i sådana arrangemang, liksom operativa aspekter, inbegripet användning av särskilda it-plattformar. Medlemsstaterna ska erbjuda stöd för tillämpningen av sådana arrangemang i enlighet med den politik som avses i artikel 5.2 g.

4. Väsentliga och viktiga entiteter ska underrätta de behöriga myndigheterna om sitt deltagande i de arrangemang för informationsutbyte som avses i punkt 2, när de ingår sådana arrangemang eller, om de utträder ur sådana arrangemang, när utträdet får verkan.

5. […] Enisa ska stödja inrättandet av de arrangemang för informationsutbyte om cybersäkerhet som avses i punkt 2 genom att tillhandahålla bästa praxis och vägledning.

Artikel 27

Frivillig anmälan av relevant information

1. Utan att det påverkar tillämpningen av artikel 20 ska medlemsstaterna säkerställa att väsentliga och viktiga entiteter på frivillig basis kan anmäla relevanta incidenter, cyberhot eller tillbud till de behöriga myndigheterna eller CSIRT-enheterna.

2. Utan att det påverkar tillämpningen av artikel 3 ska medlemsstaterna säkerställa att entiteter som inte ingår i detta direktivs tillämpningsområde på frivillig basis kan lämna in anmälningar om betydande incidenter, cyberhot eller tillbud. Vid behandlingen av anmälningarna ska medlemsstaterna agera i enlighet med det förfarande som anges i artikel 20. Medlemsstaterna får ge behandling av obligatoriska anmälningar företräde framför behandling av frivilliga anmälningar. **Utan att det påverkar utredningen, avslöjandet och lagföringen av brott** får […] frivillig rapportering inte leda till att den rapporterande entiteten åläggs ytterligare skyldigheter som den inte skulle ha blivit föremål för om den inte hade lämnat in anmälan.

3. Frivilliga anmälningar ska endast behandlas om behandlingen inte utgör en oproportionell eller orimlig börda för den berörda medlemsstaten.

KAPITEL VI

Tillsyn och efterlevnadskontroll

Artikel 28

Allmänna aspekter på tillsyn och efterlevnadskontroll

1. Medlemsstaterna ska säkerställa att de behöriga myndigheterna på ett ändamålsenligt sätt övervakar och vidtar de åtgärder som krävs för att säkerställa att detta direktiv efterlevs[...], särskilt de skyldigheter som anges i artiklarna 18**,** [...] 20 **och 23**. **Medlemsstaterna får tillåta att de behöriga myndigheterna prioriterar tillsyn, som ska grundas på en riskbaserad metod.**

2. Vid hanteringen av cybersäkerhetsincidenter ska de behöriga myndigheterna ha ett nära samarbete med dataskyddsmyndigheterna**, de behöriga myndigheter som utsetts i enlighet med direktiv (EU) XXXX/XXXX [direktivet om kritiska entiteters motståndskraft], de tillsynsorgan som utsetts i enlighet med förordning (EU) 910/2014 och andra behöriga myndigheter som utsetts genom sektorsspecifika unionsrättsakter**. [...]

3. Utan att det påverkar de nationella rättsliga och institutionella ramarna ska medlemsstaterna säkerställa att de behöriga myndigheterna, vid tillsynen av de offentliga förvaltningsentiteternas efterlevnad av detta direktiv och verkställigheten av potentiella sanktioner vid bristande efterlevnad, har lämpliga befogenheter att utföra sådana uppgifter och är operativt oberoende i förhållande till de enheter som står under tillsyn. Medlemsstaterna får besluta att införa lämpliga, proportionella och effektiva tillsyns- och efterlevnadskontrollåtgärder med avseende på dessa entiteter i enlighet med de nationella ramarna och den nationella rättsordningen.

Artikel 29

Tillsyn och efterlevnadskontroll i fråga om väsentliga entiteter

1. Medlemsstaterna ska säkerställa att de tillsyns- eller efterlevnadskontrollåtgärder som åläggs väsentliga entiteter angående de skyldigheter som anges i detta direktiv är effektiva, proportionella och avskräckande, med beaktande av omständigheterna i varje enskilt fall.

2. Medlemsstaterna ska säkerställa att de behöriga myndigheterna, när de utövar sina tillsynsuppgifter avseende väsentliga entiteter, **tillämpar en riskbaserad metod och** har befogenhet att underställa dessa entiteter **åtminstone**

   a) inspektioner på plats och distansbaserad tillsyn, inklusive slumpvisa kontroller,

   b) regelbundna **säkerhets**revisioner,

   c) riktade säkerhetsrevisioner baserade på riskbedömningar eller tillgänglig riskrelaterad information,

   d) säkerhetsskanningar på grundval av objektiva, icke-diskriminerande, rättvisa och transparenta riskbedömningskriterier**, vid behov av tekniska skäl, i samarbete med den berörda entiteten**,

   e) begäranden om information som behövs för att bedöma de cybersäkerhetsåtgärder som antagits av entiteten, inbegripet dokumenterade cybersäkerhetsstrategier[...],

   f) begäranden om tillgång till uppgifter, handlingar eller annan information som behövs för att de ska kunna utföra sina tillsynsuppgifter,

   g) begäranden om bevis på genomförandet av cybersäkerhetsstrategier, t.ex. resultaten av säkerhetsrevisioner som utförts av en kvalificerad revisor och respektive underliggande bevis.

2a. När de behöriga myndigheterna utövar sina tillsynsuppgifter enligt punkt 2 i denna artikel får de fastställa tillsynsmetoder som gör det möjligt att prioritera sådana uppgifter enligt en riskbaserad metod.

3. När de behöriga myndigheterna utövar sina befogenheter enligt punkt 2 e–g ska de ange syftet med begäran och specificera den begärda informationen.

4. Medlemsstaterna ska säkerställa att behöriga myndigheter, när de utövar sina efterlevnadskontrollbefogenheter avseende väsentliga entiteter, **åtminstone** har befogenhet att

a) utfärda varningar om entiteters bristande fullgörande av de skyldigheter som fastställs i detta direktiv,

b) utfärda bindande instruktioner eller ett föreläggande om att dessa entiteter ska avhjälpa konstaterade brister eller överträdelser av de skyldigheter som fastställs i detta direktiv,

c) ålägga dessa entiteter att upphöra med beteenden som inte överensstämmer med de skyldigheter som fastställs i detta direktiv och att avstå från att upprepa sådana beteenden,

d) ålägga dessa entiteter att se till att deras riskhanteringsåtgärder och/eller rapporteringsskyldigheter överensstämmer med de skyldigheter som fastställs i artiklarna 18 och 20, på ett specifikt sätt och inom en specifik period,

e) ålägga dessa entiteter att informera den eller de fysiska eller juridiska personer till vilka de tillhandahåller tjänster eller verksamheter som potentiellt kan beröras av ett betydande cyberhot om **hotets karaktär och** om eventuella skyddsåtgärder eller avhjälpande åtgärder som dessa fysiska eller juridiska personer kan vidta som svar på hotet,

f) ålägga dessa entiteter att inom en rimlig tidsfrist genomföra de rekommendationer som lämnats till följd av en säkerhetsrevision,

g) [...]

h) ålägga dessa entiteter att offentliggöra aspekter av bristande fullgörande av de skyldigheter som fastställs i detta direktiv på ett specifikt sätt**, om ett sådant offentliggörande inte leder till en skadlig exponering för entiteten i fråga**,

i) [...]

j) påföra eller begära att relevanta organ eller domstolar i enlighet med nationell lagstiftning påför en administrativ sanktionsavgift enligt artikel 31 utöver eller i stället för de åtgärder som avses i leden a–i i denna punkt, beroende på omständigheterna i varje enskilt fall.

5. Om efterlevnadskontrollåtgärder som antas enligt punkt 4 a–d och f visar sig vara ineffektiva ska medlemsstaterna säkerställa att de behöriga myndigheterna har befogenhet att fastställa en tidsfrist inom vilken en väsentlig entitet är skyldig att vidta nödvändiga åtgärder för att avhjälpa bristerna eller fullgöra dessa myndigheters krav. Om de begärda åtgärderna inte vidtas inom den fastställda tidsfristen ska medlemsstaterna säkerställa att de behöriga myndigheterna har befogenhet att

a) tillfälligt upphäva eller begära att ett certifierings- eller auktorisationsorgan **eller domstolar i enlighet med nationell lagstiftning** tillfälligt upphäver en certifiering eller auktorisation för en del av eller alla tjänster eller verksamheter som tillhandahålls av en väsentlig entitet,

b) införa eller begära att relevanta organ eller domstolar i enlighet med nationell lagstiftning inför ett tillfälligt förbud för personer som på nivån för verkställande direktör eller juridiskt ombud har ledningsansvar i den väsentliga entiteten och alla andra fysiska personer som hålls ansvariga för överträdelsen att utöva ledningsfunktioner i den entiteten.

Dessa sanktioner ska endast tillämpas till dess att entiteten vidtar nödvändiga åtgärder för att avhjälpa bristerna eller uppfylla kraven från den behöriga myndighet som tillämpade sanktionerna.

De sanktioner som föreskrivs i denna punkt är inte tillämpliga på offentliga förvaltningsentiteter som omfattas av detta direktiv.

6. Medlemsstaterna ska säkerställa att varje fysisk person som ansvarar för eller agerar som företrädare för en väsentlig entitet på grundval av en behörighet att företräda entiteten, att fatta beslut på dess vägnar eller att utöva kontroll över entiteten har befogenhet att säkerställa att entiteten fullgör de skyldigheter som fastställs i detta direktiv. Medlemsstaterna ska säkerställa att dessa fysiska personer kan hållas ansvariga för överträdelser av sitt uppdrag att säkerställa att de skyldigheter som fastställs i detta direktiv fullgörs. **När det gäller offentliga förvaltningsentiteter ska denna bestämmelse inte påverka tillämpningen av medlemsstaternas lagstiftning om det ansvar som åligger statligt anställda och valda och utnämnda tjänstepersoner.**

7. När de behöriga myndigheterna tillämpar efterlevnadskontrollåtgärder eller sanktioner i enlighet med punkterna 4 och 5 ska de iaktta rätten till försvar och ta hänsyn till omständigheterna i varje enskilt fall och som ett minimum ta vederbörlig hänsyn till följande:

   a) Hur allvarlig överträdelsen är och de överträdda bestämmelsernas betydelse. Överträdelser som bör betraktas som allvarliga är exempelvis upprepade överträdelser, underlåtenhet att anmäla eller avhjälpa incidenter som innebär en betydande störning, underlåtenhet att avhjälpa brister enligt bindande instruktioner från behöriga myndigheter, hindrande av revisioner eller övervakningsverksamhet som den behöriga myndigheten beordrat efter det att en överträdelse konstaterats och tillhandahållande av falsk eller grovt felaktig information i fråga om riskhanteringskrav eller rapporteringsskyldigheter enligt artiklarna 18 och 20.

b) Överträdelsens varaktighet, inbegripet upprepade överträdelser.

c) De faktiska skador eller förluster som uppstått eller potentiella skador eller förluster som skulle ha kunnat orsakas, i den mån de kan fastställas. Vid bedömningen av denna aspekt ska hänsyn bland annat tas till faktiska eller potentiella finansiella eller ekonomiska förluster, effekter på andra tjänster och det antal användare som påverkas eller potentiellt kan påverkas.

d) Huruvida överträdelsen skett med uppsåt eller genom oaktsamhet.

e) De åtgärder som entiteten vidtagit för att förhindra eller minska skadan och/eller förlusterna.

f) Efterlevnad av godkända uppförandekoder eller godkända certifieringsmekanismer.

g) Huruvida den eller de fysiska eller juridiska personer som hålls ansvariga samarbetar med de behöriga myndigheterna.

8. De behöriga myndigheterna ska utförligt motivera sina beslut angående efterlevnadskontroll. Innan sådana beslut fattas ska de behöriga myndigheterna underrätta de berörda entiteterna om sina preliminära slutsatser och ge dessa entiteter en rimlig tidsfrist för att lämna synpunkter**, såvida det inte föreligger en omedelbar fara**.

9. Medlemsstaterna ska säkerställa att deras behöriga myndigheter **i enlighet med detta direktiv** informerar de berörda behöriga myndigheter **i samma** [...] medlemsstat [...] som utsetts i enlighet med direktiv (EU) XXXX/XXXX [direktivet om kritiska entiteters motståndskraft] när de utövar sina tillsyns- och efterlevnadskontrollbefogenheter som syftar till att säkerställa att en väsentlig entitet som identifierats som kritisk **[**eller som likvärdig med en kritisk entitet**]** i enlighet med direktiv (EU) XXXX/XXXX [direktivet om kritiska entiteters motståndskraft] om skyldigheterna enligt detta direktiv. **När så är lämpligt** [...] **får** de behöriga myndigheterna i enlighet med direktiv (EU) XXXX/XXXX [direktivet om kritiska entiteters motståndskraft][...] **begära** att de behöriga myndigheterna **i enlighet med det här direktivet** [...] utövar sina tillsyns- och efterlevnadskontroll**befogenheter avseende** en väsentlig entitet som omfattas av det här direktivet och som också identifierats som kritisk **[**eller likvärdig**] i enlighet med direktiv (EU) XXXX/XXXX [direktivet om kritiska entiteters motståndskraft].**

10. Medlemsstaterna ska säkerställa att deras behöriga myndigheter i enlighet med detta direktiv informerar forumet för övervakning i enlighet med artikel 29.1 i förordning (EU) XXXX/XXXX [DORA-förordningen] när de utövar sina tillsyns- och efterlevnadskontrollbefogenheter som syftar till att säkerställa att en väsentlig entitet som identifierats som kritisk tredjepartsleverantör av IKT-tjänster i enlighet med artikel 28 i förordning (EU) XXXX/XXXX [DORA-förordningen] fullgör skyldigheterna enligt detta direktiv.

10a. Medlemsstaterna ska säkerställa att deras behöriga myndigheter i enlighet med detta direktiv informerar de berörda behöriga myndigheter som utsetts i enlighet med förordning (EU) 910/2014 när de utövar sina tillsyns- och efterlevnadskontrollbefogenheter som syftar till att säkerställa att en väsentlig entitet som utsetts som tillhandahållare av betrodda tjänster i enlighet med förordning (EU) 910/2014 fullgör sina skyldigheter enligt detta direktiv.

Artikel 30

Tillsyn och efterlevnadskontroll i fråga om viktiga entiteter

1. När medlemsstaterna får bevis eller indikationer på **eller information om** att en viktig entitet **påstås** inte fullgöra de skyldigheter som fastställs i detta direktiv, särskilt artiklarna 18 och 20, ska de säkerställa att de behöriga myndigheterna vid behov vidtar åtgärder i form av tillsynsåtgärder i efterhand.

2. Medlemsstaterna ska säkerställa att de behöriga myndigheterna, när de utövar sina tillsynsuppgifter avseende viktiga entiteter, **tillämpar en riskbaserad metod och** har befogenhet att underställa dessa entiteter **åtminstone**

   a) inspektioner på plats och distansbaserad tillsyn i efterhand,

   b) riktade säkerhetsrevisioner baserade på riskbedömningar eller tillgänglig riskrelaterad information,

   c) säkerhetsskanningar på grundval av objektiva, **icke-diskriminerande,** rättvisa och transparenta riskbedömningskriterier**, vid behov av tekniska skäl, i samarbete med den berörda entiteten**,

   d) begäranden om all information som behövs för att i efterhand bedöma cybersäkerhetsåtgärderna[...],

   e) begäranden om tillgång till uppgifter, handlingar och/eller annan information som behövs för att de ska kunna utföra tillsynsuppgifterna,

   ea) begäranden om bevis på genomförandet av cybersäkerhetsstrategier, t.ex. resultaten av säkerhetsrevisioner som utförts av en kvalificerad revisor och respektive underliggande bevis.

2a. När de behöriga myndigheterna utövar sina tillsynsuppgifter enligt punkt 2 i denna artikel får de fastställa tillsynsmetoder som gör det möjligt att prioritera sådana uppgifter enligt en riskbaserad metod.

3. När de behöriga myndigheterna utövar sina befogenheter enligt punkt 2 d–**ea** ska de ange syftet med begäran och specificera den begärda informationen.

4. Medlemsstaterna ska säkerställa att de behöriga myndigheterna, när de utövar sina efterlevnadskontrollbefogenheter avseende viktiga entiteter **åtminstone** har befogenhet att

a) utfärda varningar om entiteters bristande fullgörande av de skyldigheter som fastställs i detta direktiv,

b) utfärda bindande instruktioner eller ett föreläggande om att dessa entiteter ska avhjälpa konstaterade brister eller överträdelser av de skyldigheter som fastställs i detta direktiv,

c) ålägga dessa entiteter att upphöra med beteenden som inte överensstämmer med de skyldigheter som fastställs i detta direktiv och att avstå från att upprepa sådana beteenden,

d) ålägga dessa entiteter att säkerställa att deras riskhanteringsåtgärder eller rapporteringsskyldigheter överensstämmer med de skyldigheter som fastställs i artiklarna 18 och 20, på ett specifikt sätt och inom en specifik period,

e) ålägga dessa entiteter att informera den eller de fysiska eller juridiska personer till vilka de tillhandahåller tjänster eller verksamheter som potentiellt kan beröras av ett betydande cyberhot om **hotets karaktär och** om eventuella skyddsåtgärder eller avhjälpande åtgärder som dessa fysiska eller juridiska personer kan vidta som svar på hotet,

f) ålägga dessa entiteter att inom en rimlig tidsfrist genomföra de rekommendationer som lämnats till följd av en säkerhetsrevision,

g) ålägga dessa entiteter att offentliggöra aspekter av bristande fullgörande av deras skyldigheter som fastställs i detta direktiv på ett specifikt sätt**, om ett sådant offentliggörande inte leder till en skadlig exponering för entiteten i fråga**,

h) [...]

i) påföra eller begära att relevanta organ eller domstolar i enlighet med nationell lagstiftning påför en administrativ sanktionsavgift enligt artikel 31 utöver eller i stället för de åtgärder som avses i leden a–h i denna punkt, beroende på omständigheterna i varje enskilt fall.

5. Artikel 29.6–29.8 ska också tillämpas på de tillsyns- och efterlevnadskontrollåtgärder som föreskrivs i denna artikel för [...] viktiga entiteter [...].

Artikel 31

Allmänna villkor för påförande av administrativa sanktionsavgifter för väsentliga och viktiga entiteter

1. Medlemsstaterna ska säkerställa att de administrativa sanktionsavgifter som påförs väsentliga och viktiga entiteter i enlighet med denna artikel för överträdelser av de skyldigheter som fastställs i detta direktiv i varje enskilt fall är effektiva, proportionella och avskräckande.

2. Administrativa sanktionsavgifter ska, beroende på omständigheterna i varje enskilt fall, påföras utöver eller i stället för de åtgärder som avses i artikel 29.4 a–i, artikel 29.5 och artikel 30.4 a–h.

3. När beslut fattas om huruvida administrativa sanktionsavgifter ska påföras och om avgiftsbeloppet ska i varje enskilt fall vederbörlig hänsyn tas till åtminstone de faktorer som anges i artikel 29.7.

4. Medlemsstaterna ska säkerställa att **väsentliga entiteters** överträdelser av skyldigheterna enligt artikel 18 eller artikel 20, i enlighet med punkterna 2 och 3 i den här artikeln, medför administrativa sanktionsavgifter på minst **4** [...] 000 000 EUR eller**, om det rör sig om en juridisk person,** [...] 2 % av den totala globala årsomsättningen under det föregående räkenskapsåret för det företag som den väsentliga [...] entiteten tillhör, beroende på vilken siffra som är högst.

4a. Medlemsstaterna ska säkerställa att viktiga entiteters överträdelser av skyldigheterna enligt artikel 18 eller artikel 20, i enlighet med punkterna 2 och 3 i den här artikeln, medför administrativa sanktionsavgifter på minst 2 000 000 EUR eller, om det rör sig om en juridisk person, 1 % av den totala globala årsomsättningen under det föregående räkenskapsåret för det företag som den viktiga entiteten tillhör, beroende på vilken siffra som är högst.

5. Medlemsstaterna får föreskriva befogenhet att förelägga viten för att tvinga en väsentlig eller viktig entitet att upphöra med en överträdelse i enlighet med ett föregående beslut av den behöriga myndigheten.

6. Utan att det påverkar behöriga myndigheters befogenheter enligt artiklarna 29 och 30 får varje medlemsstat fastställa regler för huruvida och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga förvaltningsentiteter som avses i artikel 4.23 och som omfattas av de skyldigheter som föreskrivs i detta direktiv.

6a. Om administrativa sanktionsavgifter inte föreskrivs i medlemsstatens rättssystem ska medlemsstaterna säkerställa att den här artikeln får tillämpas på ett sådant sätt att förfarandet inleds av den behöriga myndigheten och sanktionsavgifterna sedan utdöms av de behöriga nationella domstolarna, varvid det säkerställs att rättsmedlen är effektiva och har samma verkan som de administrativa sanktionsavgifter som påförs av de behöriga myndigheterna. De sanktionsavgifter som påförs ska i alla händelser vara effektiva, proportionella och avskräckande. Dessa medlemsstater ska till kommissionen anmäla de bestämmelser i deras lagstiftning som de antar i enlighet med denna punkt senast den […], samt utan dröjsmål anmäla eventuell senare ändringslagstiftning eller ändringar som berör dem.

Artikel 32

Överträdelser som innebär personuppgiftsincidenter

1. Om de behöriga myndigheterna **under tillsynen eller efterlevnadskontrollen** [...] **får kännedom om** att en väsentlig eller viktig entitets överträdelse av de skyldigheter som fastställs i artiklarna 18 och 20 **i detta direktiv kan** innebära [...] en personuppgiftsincident, enligt definitionen i artikel 4.12 i förordning (EU) 2016/679 och som ska anmälas i enlighet med artikel 33 i den förordningen, ska de **utan onödigt dröjsmål** informera de tillsynsmyndigheter som är behöriga i enlighet med artiklarna 55 och 56 i den förordningen [...].

2. Om de tillsynsmyndigheter som är behöriga i enlighet med artiklarna 55 och 56 i förordning (EU) 2016/679 beslutar att utöva sina befogenheter enligt artikel 58**.2** i i den förordningen och påföra administrativa sanktionsavgifter, ska de behöriga myndigheter **som avses i artikel 8 i detta direktiv** inte påföra någon administrativ sanktionsavgift för [...] **en** överträdelse **avseende samma agerande som i** [...] artikel 31 i detta direktiv. De behöriga myndigheterna får dock tillämpa de efterlevnadskontrollåtgärder eller utöva de sanktionsbefogenheter som föreskrivs i artikel 29.4 a–i, artikel 29.5 och artikel 30.4 a–h i detta direktiv.

3. Om den tillsynsmyndighet som är behörig enligt förordning (EU) 2016/679 är etablerad i en annan medlemsstat än den behöriga myndigheten, får den behöriga myndigheten informera den tillsynsmyndighet som är etablerad i samma medlemsstat.

Artikel 33

Sanktioner

1. Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av nationella bestämmelser som antagits enligt detta direktiv och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande.

2. Medlemsstaterna ska till kommissionen anmäla dessa regler och åtgärder senast [två] år efter ikraftträdandet av detta direktiv samt utan onödigt dröjsmål eventuella ändringar som berör dem.

Artikel 34

Ömsesidigt bistånd

1. Om en väsentlig eller viktig entitet tillhandahåller tjänster i mer än en medlemsstat eller [...] **tillhandahåller tjänster** i **en eller flera** medlemsstat**er** men dess nätverks- och informationssystem är belägna i en eller flera andra medlemsstater ska de behöriga myndighete[...]**rna** i de **berörda** medlemsstaterna [...] vid behov samarbeta med och bistå varandra. Detta samarbete ska åtminstone omfatta följande:

a) Att de behöriga myndigheter som tillämpar tillsyns- eller efterlevnadskontrollåtgärder i en medlemsstat via den gemensamma kontaktpunkten informerar och samråder med de behöriga myndigheterna i övriga berörda medlemsstater om de tillsyns- och efterlevnadskontrollåtgärder som vidtagits [...].

b) Att en behörig myndighet får begära att en annan behörig myndighet vidtar tillsyns- eller efterlevnadskontrollåtgärder [...].

c) Att en behörig myndighet, efter att ha mottagit en motiverad begäran från en annan behörig myndighet, ska bistå den andra behöriga myndigheten **i proportion till dess tillgängliga resurser** så att tillsyns- eller efterlevnadskontrollåtgärderna [...] kan genomföras på ett ändamålsenligt, effektivt och konsekvent sätt. Sådant ömsesidigt bistånd får omfatta begäranden om information och tillsynsåtgärder, inbegripet begäranden om att utföra inspektioner på plats, distansbaserad tillsyn eller riktade säkerhetsrevisioner. En behörig myndighet till vilken en begäran om bistånd riktas får bara avslå begäran om det efter ett utbyte med övriga berörda myndigheter [...] fastställs att [...] myndigheten inte är behörig att tillhandahålla det begärda biståndet**, att den inte har de resurser som krävs,** att det begärda biståndet inte står i proportion till den behöriga myndighetens tillsynsuppgifter [...] **eller att begäran avser information eller verksamhet som står i strid med den medlemsstatens nationella säkerhet, allmänna säkerhet eller försvar**.

2. När så är lämpligt får behöriga myndigheter från olika medlemsstater i samförstånd genomföra de gemensamma tillsynsåtgärderna [...].

KAPITEL VII

Övergångsbestämmelser och slutbestämmelser

Artikel 35

Översyn

Kommissionen ska regelbundet se över hur detta direktiv fungerar och rapportera resultaten till Europaparlamentet och rådet. Rapporten ska särskilt bedöma relevansen av de sektorer, delsektorer och, i fråga om storlek och typ, entiteter som avses i bilagorna I och II för ekonomins och samhällets funktion när det gäller cybersäkerhet. […] **Med** tanke **på översynen** […] ska kommissionen beakta rapporterna från […] CSIRT-nätverket om de erfarenheter som förvärvats på […] operativ nivå. Den första rapporten ska lämnas senast den ... [54 månader efter dagen för detta direktivs ikraftträdande].

Artikel 36

[...]

[...]

[...]

Artikel 37

Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.

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

3. Om kommitténs yttrande ska inhämtas genom skriftligt förfarande, ska det förfarandet avslutas utan resultat om kommitténs ordförande, inom tidsfristen för att avge yttrandet, så beslutar eller en kommittéledamot så begär.

Artikel 38

Införlivande

1. **Senast den** … [[...] **24** månader efter dagen för detta direktivs ikraftträdande**]** ska medlemsstaterna anta och offentliggöra […] de lagar och andra författningar som är nödvändiga för att följa detta direktiv. De ska genast underrätta kommissionen om detta. De ska tillämpa dessa bestämmelser från och med den ... [en dag efter den dag som avses i första stycket].

2. 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.

Artikel 39

Ändring av förordning (EU) nr 910/2014

Artikel 19 […] **i förordning (EU) nr 910/2014** ska utgå **med verkan från och med ... [datumet för tidsfristen för införlivande av detta direktiv].**

Artikel 40

Ändring av direktiv (EU) 2018/1972

Artiklarna 40 och 41 […] **i direktiv (EU) 2018/1972** ska utgå **med verkan från och med ... [datumet för tidsfristen för införlivande av detta direktiv].**

Artikel 41

Upphävande

Direktiv (EU) 2016/1148 upphör att gälla med verkan från och med [datumet för tidsfristen för införlivande av direktivet].

Hänvisningar till direktiv (EU) 2016/1148 ska anses som hänvisningar till det här direktivet och läsas i enlighet med jämförelsetabellen i bilaga II[…].

Artikel 42

Ikraftträdande

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

Artikel 43

Adressater

Detta direktiv riktar sig till medlemsstaterna.

Utfärdat i Bryssel

På Europaparlamentets vägnar	*På rådets vägnar*
Ordförande	*Ordförande*

BILAGA I

SEKTORER, DELSEKTORER OCH TYPER AV ENTITETER

Sektor	Delsektor	Typ av entitet
1. Energi	a) Elektricitet	– Elföretag som avses i artikel 2.57 i direktiv (EU) 2019/944 och som bedriver ”leverans” enligt artikel 2.12 i det direktivet ([39])
		– Systemansvariga för distributionssystem som avses i artikel 2.29 i direktiv (EU) 2019/944
		– Systemansvariga för överföringssystem som avses i artikel 2.35 i direktiv (EU) 2019/944
		– Producenter som avses i artikel 2.38 i direktiv (EU) 2019/944
		— Nominerade elmarknadsoperatörer som avses i artikel 2.8 i förordning (EU) 2019/943 ([40])
		– Marknadsaktörer på elmarknaden som avses i artikel 2.25 i förordning (EU) 2019/943 och som tillhandahåller aggregering, efterfrågeflexibilitet eller energilagringstjänster som avses i artikel 2.18, 2.20 och 2.59 i direktiv (EU) 2019/944

[39] Europaparlamentets och rådets direktiv (EU) 2019/944 av den 5 juni 2019 om gemensamma regler för den inre marknaden för el och om ändring av direktiv 2012/27/EU (EUT L 158, 14.6.2019, s. 125).

[40] Europaparlamentets och rådets förordning (EU) 2019/943 om den inre marknaden för el (EUT L 158, 14.6.2019, s. 54).

	b) Fjärrvärme eller fjärrkyla	– Fjärrvärme eller fjärrkyla som avses i artikel 2.19 i direktiv (EU) 2018/2001 om främjande av användningen av energi från förnybara energikällor ([41])
	c) Olja	– Operatörer av oljeledningar
		– Operatörer av anläggningar för oljeproduktion, raffinaderier, bearbetningsanläggningar och anläggningar för lagring och överföring av olja
		— Centrala lagringsenheter för olja som avses i artikel 2 f i rådets direktiv 2009/119/EG ([42])
	d) Gas	– Gashandelsföretag eller gashandlare som avses i artikel 2.8 i direktiv 2009/73/EG ([43])
		– Systemansvariga för distributionssystemet som avses i artikel 2.6 i direktiv 2009/73/EG
		– Systemansvariga för överföringssystemet som avses i artikel 2.4 i direktiv 2009/73/EG
		– Systemansvariga för lagringssystemet som avses i artikel 2.10 i direktiv 2009/73/EG

41 Europaparlamentets och rådets direktiv (EU) 2018/2001 av den 11 december 2018 om främjande av användningen av energi från förnybara energikällor (EUT L 328, 21.12.2018, s. 82).

42 Rådets direktiv 2009/119/EG av den 14 september 2009 om skyldighet för medlemsstaterna att inneha minimilager av råolja och/eller petroleumprodukter (EUT L 265, 9.10.2009, s. 9).

43 Europaparlamentets och rådets direktiv 2009/73/EG av den 13 juli 2009 om gemensamma regler för den inre marknaden för naturgas och om upphävande av direktiv 2003/55/EG (EUT L 211, 14.8.2009, s. 94).

		– Systemansvariga för en LNG-anläggning som avses i artikel 2.12 i direktiv 2009/73/EG
		– Naturgasföretag enligt definitionen i artikel 2.1 i direktiv 2009/73/EG
		– Operatörer av raffinaderier och bearbetningsanläggningar för naturgas
	e) Vätgas	Operatörer av anläggningar för produktion, lagring och överföring av vätgas
2. Transport	a) Lufttransport	– Lufttrafikföretag som avses i artikel 3.4 i förordning (EG) nr 300/2008 ([44]) **och som används för kommersiella syften**
		– Flygplatsens ledningsenheter som avses i artikel 2.2 i direktiv 2009/12/EG ([45]), flygplatser som avses i artikel 2.1 i det direktivet, inbegripet de huvudflygplatser som förtecknas i avsnitt 2 i bilaga II till förordning (EU) nr 1315/2013 ([46]) och enheter som driver närliggande anläggningar inom flygplatser
		– Operatörer inom trafikstyrning och trafikledning som tillhandahåller flygkontrolltjänst som avses i

[44] Europaparlamentets och rådets förordning (EG) nr 300/2008 av den 11 mars 2008 om gemensamma skyddsregler för den civila luftfarten och om upphävande av förordning (EG) nr 2320/2002 (EUT L 97, 9.4.2008, s. 72).

[45] Europaparlamentets och rådets direktiv 2009/12/EG av den 11 mars 2009 om flygplatsavgifter (EUT L 70, 14.3.2009, s. 11).

[46] Europaparlamentets och rådets förordning (EU) nr 1315/2013 av den 11 december 2013 om unionens riktlinjer för utbyggnad av det transeuropeiska transportnätet och om upphävande av beslut nr 661/2010/EU (EUT L 348, 20.12.2013, s. 1).

		artikel 2.1 i förordning (EG) nr 549/2004 ([47])
	b) Järnvägstransport	– Infrastrukturförvaltare som avses i artikel 3.2 i direktiv 2012/34/EU ([48])
		– Järnvägsföretag som avses i artikel 3.1 i direktiv 2012/34/EU, inbegripet tjänsteleverantörer som avses i artikel 3.12 i direktiv 2012/34/EU
	c) Sjöfart	– Transportföretag som bedriver persontrafik och godstrafik på inre vattenvägar, till havs och längs kuster och som i fråga om sjötransport avses i bilaga I till förordning (EG) nr 725/2004 ([49]), exklusive de enskilda fartyg som drivs av dessa företag
		– Ledningsenheter för hamnar som avses i artikel 3.1 i direktiv 2005/65/EG ([50]), inbegripet deras hamnanläggningar som avses i artikel 2.11 i förordning (EG) nr 725/2004, och enheter som sköter anläggningar och utrustning i hamnar
		– Operatörer av sjötrafikinformationstjänst som

[47] Europaparlamentets och rådets förordning (EG) nr 549/2004 av den 10 mars 2004 om ramen för inrättande av det gemensamma europeiska luftrummet (”ramförordning”) (EUT L 96, 31.3.2004, s. 1).

[48] Europaparlamentets och rådets direktiv 2012/34/EU av den 21 november 2012 om inrättande av ett gemensamt europeiskt järnvägsområde (EUT L 343, 14.12.2012, s. 32).

[49] Europaparlamentets och rådets förordning (EG) nr 725/2004 av den 31 mars 2004 om förbättrat sjöfartsskydd på fartyg och i hamnanläggningar (EUT L 129, 29.4.2004, s. 6).

[50] Europaparlamentets och rådets direktiv 2005/65/EG av den 26 oktober 2005 om ökat hamnskydd (EUT L 310, 25.11.2005, s. 28).

		avses i artikel 3 o i direktiv 2002/59/EG ([51])
	d) Vägtransport	– Vägmyndigheter enligt artikel 2.12 i kommissionens delegerade förordning (EU) 2015/962 ([52]) med ansvar för trafikstyrning, **med undantag för offentliga entiteter för vilka trafikstyrning eller operatörer av intelligenta transportsystem endast är en icke väsentlig del av deras allmänna verksamhet**
		– Operatörer av intelligenta transportsystem som avses i artikel 4.1 i direktiv 2010/40/EU ([53])
3. Bankverksamhet		— Kreditinstitut som avses i artikel 4.1 i förordning (EU) nr 575/2013 ([54])**, [utom de institut som avses i artikel 2.5.8 i direktiv 2013/36/EU, som är undantagna i enlighet med artikel 2.4 i förordning XX [DORA-förordningen]]**

[51] Europaparlamentets och rådets direktiv 2002/59/EG av den 27 juni 2002 om inrättande av ett övervaknings- och informationssystem för sjötrafik i gemenskapen och om upphävande av rådets direktiv 93/75/EEG (EGT L 208, 5.8.2002, s. 10).

[52] Kommissionens delegerade förordning (EU) 2015/962 av den 18 december 2014 om komplettering av Europaparlamentets och rådets direktiv 2010/40/EU vad gäller tillhandahållande av EU-omfattande realtidstrafikinformationstjänster (EUT L 157, 23.6.2015, s. 21).

[53] Europaparlamentets och rådets direktiv 2010/40/EU av den 7 juli 2010 om ett ramverk för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportslag (EUT L 207, 6.8.2010, s. 1).

[54] Europaparlamentets och rådets förordning (EU) nr 575/2013 av den 26 juni 2013 om tillsynskrav för kreditinstitut och värdepappersföretag och om ändring av förordning (EU) nr 648/2012 (EUT L 176, 27.6.2013, s. 1).

4. Finansmarknadsinfrastruktur		– Operatörer av handelsplatser som avses i artikel 4.24 i direktiv 2014/65/EU ([55])
		– Centrala motparter som avses i artikel 2.1 i förordning (EU) nr 648/2012 ([56])
5. Hälso- och sjukvård		— Vårdgivare som avses i artikel 3 g i direktiv 2011/24/EU ([57])
		— EU-referenslaboratorier som avses i artikel 15 i förordning XXXX/XXXX om allvarliga gränsöverskridande hot mot människors hälsa ([58])
		— Entiteter som bedriver forskning och utveckling avseende läkemedel som avses i artikel 1.2 i direktiv 2001/83/EG ([59]) — Entiteter som tillverkar farmaceutiska basprodukter och läkemedel som avses i avsnitt C huvudgrupp 21 i Nace Rev. 2 — Entiteter som tillverkar medicintekniska produkter som betraktas som kritiska vid ett hot mot folkhälsan (”förteckning över kritiska medicintekniska produkter

[55] Europaparlamentets och rådets direktiv 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU (EUT L 173, 12.6.2014, s. 349).

[56] Europaparlamentets och rådets förordning (EU) nr 648/2012 av den 4 juli 2012 om OTC-derivat, centrala motparter och transaktionsregister (EUT L 201, 27.7.2012, s. 1).

[57] Europaparlamentets och rådets direktiv 2011/24/EU av den 9 mars 2011 om tillämpningen av patienträttigheter vid gränsöverskridande hälso- och sjukvård (EUT L 88, 4.4.2011, s. 45).

[58] [Europaparlamentets och rådets förordning om allvarliga gränsöverskridande hot mot människors hälsa och om upphävande av beslut nr 1082/2013/EU, hänvisning uppdateras när förslag COM(2020) 727 final antas].

[59] Europaparlamentets och rådets direktiv 2001/83/EG av den 6 november 2001 om upprättande av gemenskapsregler för humanläkemedel (EGT L 311, 28.11.2001, s. 67).

		vid ett hot mot folkhälsan”) och som avses i artikel 20 i förordning XXXX ([60])
6. Dricksvatten		Leverantörer och distributörer av dricksvatten som avses i artikel 2.1 a i rådets direktiv 98/83/EG ([61]), dock undantaget distributörer för vilka distribution av dricksvatten endast utgör en **icke väsentlig** del av deras allmänna verksamhet, som består i distribution av andra förnödenheter och varor […]
7. Avloppsvatten		Företag som samlar ihop, släpper ut och renar avloppsvatten från tätbebyggelse, hushållsspillvatten och industrispillvatten som avses i artikel 2.1–2.3 i rådets direktiv 91/271/EEG ([62])**, dock undantaget företag som endast samlar in, släpper ut eller renar avloppsvatten från tätbebyggelse, hushållsspillvatten och industrispillvatten som en icke väsentlig del av sin allmänna verksamhet** [...]
8. Digital infrastruktur		– Leverantörer av internetknutpunkter
		– – Leverantörer av DNS-tjänster**, med undantag för operatörer av rotnamnsservrar**
		— Registreringsenheter för toppdomäner

60 [Europaparlamentets och rådets förordning om en förstärkt roll för Europeiska läkemedelsmyndigheten vid krisberedskap och krishantering avseende läkemedel och medicintekniska produkter, hänvisning uppdateras när förslag COM(2020) 725 final antas].

61 Rådets direktiv 98/83/EG av den 3 november 1998 om kvaliteten på dricksvatten (EGT L 330, 5.12.1998, s. 32).

62 Rådets direktiv 91/271/EEG av den 21 maj 1991 om rening av avloppsvatten från tätbebyggelse (EGT L 135, 30.5.1991, s. 40).

		– Leverantörer av molntjänster
		– Leverantörer av datacentraltjänster
		– Leverantörer av nätverk för innehållsleverans
		– Tillhandahållare av betrodda tjänster som avses i artikel 3.19 i förordning (EU) nr 910/2014 ([63])
		– Tillhandahållare av allmänna elektroniska kommunikationsnät som avses i artikel 2.8 i direktiv (EU) 2018/1972([64]) eller tillhandahållare av elektroniska kommunikationstjänster som avses i artikel 2.4 i direktiv (EU) 2018/1972, om deras tjänster är allmänt tillgängliga
8.a Hantering av IKT-tjänster **Företag till företag (B2B)**		**— Leverantörer av hanterade tjänster** **— Leverantörer av hanterade säkerhetstjänster**

[63] 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 (EUT L 257, 28.8.2014, s. 73).

[64] Europaparlamentets och rådets direktiv (EU) 2018/1972 av den 11 december 2018 om inrättande av en europeisk kodex för elektronisk kommunikation (EUT L 321, 17.12.2018, s. 36).

9. Offentliga förvaltning**sentiteter**		— Offentliga förvaltningsentiteter hos nationella regeringar **såsom de definieras av en medlemsstat i enlighet med den nationella lagstiftningen** — [...][65][...] — [...]
10. Rymdfrågor		— Operatörer av markbaserad infrastruktur som ägs, förvaltas och drivs av medlemsstater eller privata parter och som stöder tillhandahållandet av rymdbaserade tjänster, undantaget tillhandahållare av allmänna elektroniska kommunikationsnät som avses i artikel 2.8 i direktiv (EU) 2018/1972

65 [...]

BILAGA II

SEKTORER, DELSEKTORER OCH TYPER AV ENTITETER

Sektor	Delsektor	Typ av entitet
1. Post- och budtjänster		Tillhandahållare av posttjänster som avses i artikel 2.1 […] i direktiv 97/67/EG ([66]), **inbegripet** […] tillhandahållare av budtjänster
2. Avfallshantering		Verksamhetsutövare som bedriver avfallshantering som avses i artikel 3.9 i direktiv 2008/98/EG ([67]), dock undantaget verksamhetsutövare vars huvudsakliga näringsverksamhet inte utgörs av avfallshantering

[66] Europaparlamentets och rådets direktiv 97/67/EG av den 15 december 1997 om gemensamma regler för utvecklingen av gemenskapens inre marknad för posttjänster och för förbättring av kvaliteten på tjänsterna (EGT L 15, 21.1.1998, s. 14)**, ändrat genom Europaparlamentets och rådets direktiv 2008/6/EG av den 20 februari 2008 om ändring av direktiv 97/67/EG beträffande fullständigt genomförande av gemenskapens inre marknad för posttjänster (EUT L 52, 27.2.2008, s. 3).**

[67] Europaparlamentets och rådets direktiv 2008/98/EG av den 19 november 2008 om avfall och om upphävande av vissa direktiv (EUT L 312, 22.11.2008, s. 3).

3. Tillverkning, produktion och distribution av kemikalier		Företag som tillverkar […] och distribuerar ämnen och […] **blandningar** och som avses i artikel […] 3.9 och 3.14 i förordning (EG) nr 1907/2006 ([68]) **och företag som tillverkar varor enligt artikel 3.3 i den förordningen från ämnen eller blandningar**
4. Produktion, bearbetning och distribution av livsmedel		Livsmedelsföretag som avses i artikel 3.2 i förordning (EG) nr 178/2002 ([69]) **och som är verksamma inom grossisthandel och industriell produktion och bearbetning**
5. Tillverkning	a) Tillverkning av medicintekniska produkter och medicintekniska produkter för in vitro-diagnostik	Entiteter som tillverkar medicintekniska produkter som avses i artikel 2.1 i förordning (EU) 2017/745 ([70]) och entiteter som tillverkar medicintekniska produkter för in vitro-diagnostik som avses i artikel 2.2 i förordning (EU) 2017/746 ([71]), med undantag av entiteter som tillverkar sådana medicintekniska produkter som

[68] Europaparlamentets och rådets förordning (EG) nr 1907/2006 av den 18 december 2006 om registrering, utvärdering, godkännande och begränsning av kemikalier (Reach), inrättande av en europeisk kemikaliemyndighet, ändring av direktiv 1999/45/EG och upphävande av rådets förordning (EEG) nr 793/93 och kommissionens förordning (EG) nr 1488/94 samt rådets direktiv 76/769/EEG och kommissionens direktiv 91/155/EEG, 93/67/EEG, 93/105/EG och 2000/21/EG (EUT L 396 30.12.2006, s. 1).

[69] Europaparlamentets och rådets förordning (EG) nr 178/2002 av den 28 januari 2002 om allmänna principer och krav för livsmedelslagstiftning, om inrättande av Europeiska myndigheten för livsmedelssäkerhet och om förfaranden i frågor som gäller livsmedelssäkerhet (EGT L 31, 1.2.2002, s. 1).

[70] Europaparlamentets och rådets förordning (EU) 2017/745 av den 5 april 2017 om medicintekniska produkter, om ändring av direktiv 2001/83/EG, förordning (EG) nr 178/2002 och förordning (EG) nr 1223/2009 och om upphävande av rådets direktiv 90/385/EEG och 93/42/EEG (EUT L 117, 5.5.2017, s. 1).

[71] Europaparlamentets och rådets förordning (EU) 2017/746 av den 5 april 2017 om medicintekniska produkter för in vitro-diagnostik och om upphävande av direktiv 98/79/EG och kommissionens beslut 2010/227/EU (EUT L 117 5.5.2017, s. 176).

		nämns i punkt 5 i bilaga I.
	b) Tillverkning av datorer, elektronikvaror och optik	Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 26 i Nace Rev. 2
	c) Tillverkning av elapparatur	Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 27 i Nace Rev. 2
	d) Tillverkning av övriga maskiner	Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 28 i Nace Rev. 2
	e) Tillverkning av motorfordon, släpfordon och påhängsvagnar	Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 29 i Nace Rev. 2
	f) Tillverkning av andra transportmedel	Företag som bedriver någon ekonomisk verksamhet som avses i avsnitt C huvudgrupp 30 i Nace Rev. 2
6. Digitala leverantörer		– Leverantörer av internetbaserade marknadsplatser
		– Leverantörer av internetbaserade sökmotorer
		– Leverantörer av plattformar för sociala nätverkstjänster