DIREKTIV

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2022/2555

av den 14 december 2022

om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet)

(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 centralbankens yttrande ([1]),

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande ([2]),

efter att ha hört Regionkommittén,

i enlighet med det ordinarie lagstiftningsförfarandet ([3]), och

av följande skäl:

(1) Syftet med Europaparlamentets och rådets direktiv (EU) 2016/1148 ([4]) var att bygga upp cybersäkerhetskapaciteten i hela unionen, begränsa 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 incidenter, och därigenom bidra till unionens säkerhet och till att dess ekonomi och samhälle kan fungera effektivt.

(2) Sedan direktiv (EU) 2016/1148 trädde i kraft har betydande framsteg gjorts med att öka unionens nivå av cyberresiliens. 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 för säkerhet i nätverks- och informationssystem genom att fastställa nationella strategier för säkerhet i nätverks- och informationssystem och inrätta nationell kapacitet och genom att genomföra lagstiftningsåtgärder som omfattar väsentliga infrastrukturer och entiteter som identifierats av varje medlemsstat. Direktiv (EU) 2016/1148 har också bidragit till samarbete på unionsnivå genom inrättandet av samarbetsgruppen samt nätverket av nationella it-incidentcentrum. Trots dessa framsteg har översynen av direktiv (EU) 2016/1148 avslöjat inneboende brister som hindrar det från att effektivt hantera befintliga och framväxande utmaningar på cybersäkerhetsområdet.

(3) Nätverks- och informationssystem har utvecklats till 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 utvidgad cyberhotbild, som medfört nya utmaningar som kräver anpassade, samordnade och innovativa svarsåtgärder i alla medlemsstater. Incidenter, som blir allt fler och mer omfattande, sofistikerade och vanliga och får allt större inverkan, utgör ett allvarligt hot mot nätverks- och informationssystemens funktion. Därför kan sådana incidenter hindra utövandet av ekonomisk verksamhet på den inre marknaden, generera

([1]) EUT C 233, 16.6.2022, s. 22.
([2]) EUT C 286, 16.7.2021, s. 170.
([3]) Europaparlamentets ståndpunkt av den 10 november 2022 (ännu inte offentliggjord i EUT) och rådets beslut av den 28 november 2022.
([4]) 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).

ekonomisk förlust, 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 fungera väl. Cybersäkerhet är dessutom en viktig förutsättning för att många kritiska sektorer ska kunna tillgodogöra sig den digitala omställningen och fullt ut utnyttja digitaliseringens ekonomiska, sociala och hållbarhetsmässiga fördelar.

(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 utför verksamhet som är ekonomiskt betydelsefull varierar avsevärt mellan medlemsstaterna vad gäller typen av krav, kravens utförlighet och tillsynsmetoden. Dessa skillnader medför extra kostnader och gör det svårt för entiteterna att erbjuda varor och tjänster över gränserna. Krav som ställs av en medlemsstat och som skiljer sig från, eller till och med står i strid med, krav som ställs av en annan medlemsstat kan väsentligt påverka sådan gränsöverskridande verksamhet. Det är dessutom sannolikt att otillräckligt utformade eller genomförda cybersäkerhetskrav 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 medlemsstaternas genomförande, 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 säkerhets- och incidentrapporteringsskyldigheter som fastställs i det. Dessa skyldigheter genomfördes därför på väsentligt skilda sätt på nationell nivå. Det finns liknande skillnader i genomförandet av bestämmelserna om tillsyn och efterlevnadskontroll i direktiv (EU) 2016/1148.

(5) Alla dessa skillnader medför en fragmentering av den inre marknaden och kan ha en skadlig inverkan på dess funktion, vilket påverkar i synnerhet tillhandahållandet av tjänster över gränserna och nivån av cyberresiliens till följd av tillämpningen av ett spektrum av åtgärder. Dessa skillnader kan till sist leda till att vissa medlemsstater har större sårbarhet för cyberhot, med potentiella spridningseffekter i hela unionen. Direktivets mål är att undanröja dessa stora skillnader mellan medlemsstaterna, särskilt genom att föreskriva minimiregler för ett fungerande samordnat regelverk genom att fastställa mekanismer för effektivt samarbete mellan de ansvariga myndigheterna i varje medlemsstat, genom att uppdatera förteckningen över sektorer och verksamheter som omfattas av skyldigheter vad gäller cybersäkerhet och genom att föreskriva effektiva rättsmedel och efterlevnadskontrollåtgärder, vilket är centralt 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) I och med upphävandet av direktiv (EU) 2016/1148 bör tillämpningsområdet med avseende på olika sektorer utvidgas till en större del av ekonomin 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. I synnerhet syftar det här direktivet till att åtgärda bristerna i fråga om differentieringen mellan leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster, vilken har visat sig vara inaktuell eftersom den inte speglar den betydelse som dessa sektorer och tjänster har för samhälleliga och ekonomiska verksamheter på den inre marknaden.

(7) Enligt direktiv (EU) 2016/1148 hade medlemsstaterna ansvaret för att identifiera de entiteter som uppfyllde kriterierna för att klassificeras som leverantörer av samhällsviktiga tjänster. För att undanröja de stora skillnaderna mellan medlemsstaterna i detta avseende och säkerställa rättslig säkerhet vad gäller riskhanteringsåtgärderna för cybersäkerhet 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 som innebär att alla entiteter som betraktas som medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG ([5]), eller överstiger de trösklar för medelstora företag som fastställs i punkt 1 i den artikeln, och som är verksamma i de sektorer och tillhandahåller de typer av tjänster eller

([5]) 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).

bedriver de verksamheter som omfattas av det här direktivet också omfattas av tillämpningsområdet för det här direktivet. Medlemsstaterna bör även föreskriva att vissa små företag och mikroföretag, enligt definitionen i artikel 2.2 och 2.3 i den bilagan, som uppfyller specifika kriterier som visar deras nyckelroll för samhället, ekonomin eller för särskilda sektorer eller typer av tjänster ska omfattas av tillämpningsområdet för det här direktivet.

(8) Undantaget för offentliga förvaltningsentiteter från detta direktivs tillämpningsområde bör omfatta entiteter vars verksamhet till övervägande del bedrivs på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet verksamhet som rör utredning, förebyggande, upptäckt och lagföring av brott. Offentliga förvaltningsentiteter vars verksamhet endast marginellt hänför sig till dessa områden bör dock inte vara undantagna från direktivets tillämpningsområde. Vid tillämpningen av detta direktiv anses entiteter med tillsynsbefogenheter inte bedriva verksamhet på brottsbekämpningsområdet, och de är därför inte undantagna från tillämpningsområdet för detta direktiv. Offentliga förvaltningsentiteter som inrättats gemensamt med ett tredjeland i enlighet med ett internationellt avtal är undantagna från detta direktivs tillämpningsområde. Detta direktiv är inte tillämpligt på medlemsstaters diplomatiska och konsulära beskickningar i tredjeländer eller på deras nätverks- och informationssystem, såvida dessa system är belägna inom beskickningen eller drivs för användare i ett tredjeland.

(9) Medlemsstaterna bör kunna vidta de åtgärder som är nödvändiga för att skydda väsentliga nationella säkerhetsintressen, upprätthålla allmän ordning och säkerhet och möjliggöra förebyggande, utredning, upptäckt och lagföring av brott. I detta syfte bör medlemsstaterna kunna undanta särskilda entiteter som bedriver verksamhet på områdena, nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott, från vissa skyldigheter i detta direktiv med avseende på sådan verksamhet. Om en entitet tillhandahåller tjänster uteslutande för en offentlig förvaltningsentitet som är undantagen från detta direktivs tillämpningsområde bör medlemsstaterna kunna undanta den entiteten från vissa skyldigheter enligt detta direktiv med avseende på dessa tjänster. Vidare bör ingen medlemsstat vara skyldig att lämna information vars avslöjande skulle strida mot dess väsentliga intressen i fråga om nationell säkerhet, allmän säkerhet eller försvar. Unionsregler eller nationella regler till skydd för säkerhetsskyddsklassificerade uppgifter, sekretessavtal samt informella sekretessavtal såsom Traffic Light Protocol bör beaktas i detta sammanhang. Traffic Light Protocol bör ses som ett medel för att informera om eventuella begränsningar i vidarespridningen av information. Det används inom nästan alla enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter) och av vissa informations- och analyscentraler.

(10) Även om detta direktiv tillämpas på entiteter som bedriver verksamhet inom produktion av el från kärnkraftverk kan viss verksamhet vara kopplad till den nationella säkerheten. När så är fallet bör en medlemsstat kunna utöva sitt ansvar för att skydda den nationella säkerheten i samband med sådan verksamhet, inklusive verksamhet inom kärnenergins värdekedja, i enlighet med fördragen.

(11) Vissa entiteter bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott, samtidigt som de även tillhandahåller betrodda tjänster. Tillhandahållare av betrodda tjänster som omfattas av Europaparlamentets och rådets förordning (EU) nr 910/2014 ([6]) bör omfattas av detta direktiv för att säkerställa samma nivå på säkerhetskraven och tillsynen som den som tidigare fastställdes i den förordningen vad gäller tillhandahållare av betrodda tjänster. I överensstämmelse med undantaget för vissa specifika tjänster från förordning (EU) nr 910/2014 bör detta direktiv inte vara tillämpligt på tillhandahållande av betrodda tjänster som på grund av nationell rätt eller avtal mellan en avgränsad grupp deltagare endast används inom slutna system.

([6]) 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).

(12) Tillhandahållare av posttjänster enligt definitionen i Europaparlamentets och rådets direktiv 97/67/EG ([7]), inklusive tillhandahållare av budtjänster, bör omfattas av detta direktiv om de tillhandahåller minst ett led i postleveranskedjan, särskilt insamling, sortering, transport eller distribution av postförsändelser, inklusive upphämtning, samtidig som hänsyn tas till den grad i vilken de är beroende av nätverks- och informationssystem. Transporttjänster som inte utförs i samband med något av dessa led bör vara undantagna från tillämpningsområdet för posttjänster.

(13) Med tanke på att cyberhoten intensifieras och blir alltmer sofistikerade bör medlemsstaterna sträva efter att säkerställa att entiteter som är undantagna från detta direktivs tillämpningsområde uppnår en hög cybersäkerhetsnivå och stödja tillämpningen av likvärdiga riskhanteringsåtgärder för cybersäkerhet som speglar dessa entiteters känsliga natur.

(14) Unionens dataskyddslagstiftning och integritetslagstiftning är tillämplig på all behandling av personuppgifter inom ramen för detta direktiv. I synnerhet påverkar detta direktiv inte tillämpningen av Europaparlamentets och rådets förordning (EU) 2016/679 ([8]) och Europaparlamentets och rådets direktiv 2002/58/EG ([9]). Därför bör detta direktiv inte påverka exempelvis uppgifterna och befogenheterna för de myndigheter som är behöriga att övervaka efterlevnaden av unionens tillämpliga dataskyddslagstiftning och integritetslagstiftning.

(15) De entiteter som omfattas av tillämpningsområdet för detta direktiv med avseende på efterlevnad av riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter bör indelas i två kategorier, väsentliga entiteter och viktiga entiteter, vilket speglar i vilken mån de är av kritisk betydelse med avseende på sektor eller de typer av tjänster de tillhandahåller samt deras storlek. I detta avseende bör vederbörlig hänsyn i förekommande fall tas till eventuella relevanta sektorsspecifika riskbedömningar eller vägledning från de behöriga myndigheterna. Tillsyns- och efterlevnadskontrollsystemen för dessa båda kategorier av entiteter bör differentieras för att säkerställa en rättvis balans mellan riskbaserade krav och skyldigheter å ena sidan och den administrativa börda som följer av tillsynen av efterlevnaden å den andra.

(16) För att undvika att entiteter som har partnerföretag eller som är anknutna företag betraktas som väsentliga eller viktiga entiteter när detta vore oproportionellt kan medlemsstaterna ta hänsyn till vilken grad av oberoende som entiteten åtnjuter i förhållande till sin partner eller de anknutna företagen vid tillämpningen av artikel 6.2 i bilagan till rekommendation 2003/361/EG. I synnerhet kan medlemsstaterna ta hänsyn till att en entitet är oberoende av sin partner eller de anknutna företagen med avseende på de nätverks- och informationssystem som entiteten använder vid tillhandahållandet av sina tjänster och med avseende på de tjänster som entiteten tillhandahåller. På grundval av detta kan medlemsstaterna när det är lämpligt anse att en sådan entitet inte betraktas som ett medelstort företag enligt artikel 2 i bilagan till rekommendation 2003/361/EG, eller inte överstiger de trösklar för ett medelstort företag som fastställs i punkt 1 i den artikeln, om entiteten, med hänsyn tagen till dess grad av oberoende, inte skulle ha ansetts betraktas som ett medelstort företag eller överstiga dessa trösklar om bara dess egna data hade tagits i beaktande. Detta påverkar inte skyldigheterna enligt detta direktiv för partnerföretag och anknutna företag som omfattas av direktivets tillämpningsområde.

(17) Medlemsstaterna bör kunna besluta 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.

([7]) 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).

([8]) 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).

([9]) 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).

(18) För att skapa en tydlig överblick över entiteter som omfattas av detta direktivs tillämpningsområde bör medlemsstaterna upprätta en förteckning över väsentliga och viktiga entiteter samt entiteter som tillhandahåller domännamnsregistreringstjänster. I detta syfte bör medlemsstaterna ålägga entiteter att till de behöriga myndigheterna lämna åtminstone följande information: namn, adress och aktuella kontaktuppgifter, inklusive entitetens e-postadresser, IP-adressintervall och telefonnummer, och i tillämpliga fall den relevanta sektor och delsektor som avses i de bilagorna samt i tillämpliga fall en förteckning över de medlemsstater där de tillhandahåller tjänster som omfattas av detta direktivs tillämpningsområde. I detta syfte bör kommissionen, med bistånd från Europeiska unionens cybersäkerhetsbyrå (Enisa), utan onödigt dröjsmål tillhandahålla riktlinjer och mallar avseende skyldigheten att lämna information. I syfte att underlätta upprättandet och uppdateringen av förteckningen över väsentliga och viktiga entiteter samt entiteter som tillhandahåller domännamnsregistreringstjänster bör medlemsstaterna kunna fastställa nationella mekanismer för att entiteter ska kunna registrera sig själva. Om det finns register på nationell nivå kan medlemsstaterna besluta om lämpliga mekanismer som gör det möjligt att identifiera entiteter som omfattas av detta direktiv.

(19) Medlemsstaterna bör ansvara för att förse kommissionen åtminstone med uppgifter om antalet väsentliga och viktiga entiteter för varje sektor och delsektor enligt bilagorna samt relevant information om antalet identifierade entiteter och den bestämmelse i detta direktiv på vars grundval dessa identifierats, och den typ av tjänster de tillhandahåller. Medlemsstaterna uppmuntras att utbyta information med kommissionen om väsentliga och viktiga entiteter och, i händelse av en storskalig cybersäkerhetsincident, relevant information såsom den berörda entitetens namn.

(20) Kommissionen bör, i samarbete med samarbetsgruppen och efter samråd med relevanta intressenter, tillhandahålla riktlinjer om genomförandet av de kriterier som ska tillämpas på mikroföretag och små företag för att bedöma om de omfattas av detta direktiv. Kommissionen bör även säkerställa att mikroföretag och små företag som omfattas av detta direktiv får lämplig vägledning. Kommissionen bör, med bistånd från medlemsstaterna, göra information tillgänglig för mikroföretag och små företag i detta avseende.

(21) Kommissionen kan tillhandahålla vägledning för att bistå medlemsstaterna med att genomföra bestämmelserna i detta direktiv om tillämpningsområde och med att utvärdera proportionaliteten i de åtgärder som ska vidtas i enlighet med direktivet, särskilt vad gäller entiteter med komplexa affärsmodeller eller driftsmiljöer, varvid en entitet samtidigt kan uppfylla kriterierna för både väsentliga och viktiga entiteter eller samtidigt kan bedriva viss verksamhet som omfattas av, och viss verksamhet som är undantagen från, detta direktiv.

(22) I detta direktiv fastställs referensscenariot för riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter i alla sektorer som omfattas av dess tillämpningsområde. För att undvika fragmentering av cybersäkerhetsbestämmelserna i unionsrättsakter bör kommissionen, när ytterligare sektorsspecifika unionsrättsakter om riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter anses nödvändiga för att säkerställa en hög cybersäkerhetsnivå i hela unionen, bedöma om sådana ytterligare bestämmelser kan fastställas i en genomförandeakt inom ramen för detta direktiv. Om en sådan genomförandeakt inte är lämplig för detta ändamål skulle sektorsspecifika unionsrättsakter kunna bidra till att säkerställa en hög cybersäkerhetsnivå i hela unionen, samtidigt som de berörda sektorernas särdrag och komplexitet beaktas fullt ut. Därför hindrar detta direktiv inte antagandet av ytterligare sektorsspecifika unionsrättsakter innehållande riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter som tar vederbörlig hänsyn till behovet av en övergripande och konsekvent cybersäkerhetsram. Detta direktiv påverkar inte de befintliga genomförandebefogenheter som har tilldelats kommissionen med avseende på ett antal sektorer, däribland transport och energi.

(23) Om en sektorsspecifik unionsrättsakt innehåller bestämmelser som föreskriver att väsentliga eller viktiga entiteter ska anta riskhanteringsåtgärder för cybersäkerhet eller anmäla betydande incidenter, och om dessa krav har minst samma verkan som de skyldigheter som fastställs i detta direktiv, bör de bestämmelserna, inbegripet om tillsyn och

efterlevnadskontroll, tillämpas på sådana entiteter. Om en sektorsspecifik 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 den rättsakten.

(24) Om bestämmelserna i en sektorsspecifik unionsrättsakt föreskriver att väsentliga eller viktiga entiteter ska uppfylla rapporteringskrav som har minst samma verkan som rapporteringsskyldigheterna enligt detta direktiv bör samstämdhet och ändamålsenlighet säkerställas vid hanteringen av incidentanmälningar. I detta syfte bör den sektorsspecifika unionsrättsaktens bestämmelser om incidentanmälan föreskriva att CSIRT-enheterna, de behöriga myndigheterna eller de gemensamma kontaktpunkterna för cybersäkerhet (de gemensamma kontaktpunkterna) enligt detta direktiv ska ha omedelbar tillgång till de incidentanmälningar som lämnats in i enlighet med den sektorsspecifika unionsrättsakten. I synnerhet kan sådan omedelbar tillgång säkerställas om incidentanmälningar vidarebefordras utan onödigt dröjsmål till CSIRT-enheten, den behöriga myndigheten eller den gemensamma kontaktpunkten enligt detta direktiv. När det är lämpligt bör medlemsstaterna införa en automatisk och direkt rapporteringsmekanism som säkerställer systematisk och omedelbar informationsdelning med CSIRT-enheterna, de behöriga myndigheterna eller de gemensamma kontaktpunkterna angående hanteringen av sådana incidentanmälningar. I syfte att förenkla rapporteringen och genomföra den automatiska och direkta rapporteringsmekanismen kan medlemsstaterna, i enlighet med den sektorsspecifika unionsrättsakten, använda en gemensam kontaktpunkt.

(25) Sektorsspecifika unionsrättsakter som föreskriver riskhanteringsåtgärder för cybersäkerhet eller rapporteringsskyldigheter som minst har samma verkan som de som fastställs i detta direktiv kan föreskriva att behöriga myndigheter inom ramen för de rättsakterna utövar sina tillsyns- och efterlevnadskontrollbefogenheter avseende sådana åtgärder eller skyldigheter med bistånd av de behöriga myndigheterna enligt 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 för inspektioner på plats i enlighet med nationell rätt och en mekanism för utbyte av relevant information om tillsyn och efterlevnadskontroll mellan de behöriga myndigheterna, inklusive tillgång till cyberrelaterad information som begärts av de behöriga myndigheterna enligt detta direktiv.

(26) Om sektorsspecifika unionsrättsakter innehåller skyldigheter eller incitament för entiteter att anmäla betydande cyberhot bör medlemsstaterna även uppmuntra till informationsdelning om betydande cyberhot med CSIRT-enheterna, de behöriga myndigheterna eller de gemensamma kontaktpunkterna enligt detta direktiv för att öka dessa organs medvetenhet om cyberhotbilden och göra det möjligt för dem att reagera ändamålsenligt och i lämplig tid om de betydande cyberhoten skulle bli verklighet.

(27) Framtida sektorsspecifika unionsrättsakter bör ta vederbörlig hänsyn till de definitioner och den ram för tillsyn och efterlevnadskontroll som fastställs i detta direktiv.

(28) Europaparlamentets och rådets förordning (EU) 2022/2554 ([10]) bör betraktas som en sektorsspecifik unionsrättsakt vid tillämpning av detta direktiv med avseende på finansiella entiteter. Bestämmelserna i förordning (EU) 2022/2554 avseende riskhanteringsåtgärder för informations- och kommunikationsteknik (IKT), hantering av IKT-relaterade incidenter, särskilt rapportering om större IKT-relaterade incidenter, samt avseende 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 på finansiella entiteter som omfattas av förordning (EU) 2022/2554. Det är samtidigt viktigt att upprätthålla starka förbindelser och informationsutbyte med finanssektorn inom ramen för detta direktiv. Därför gör förordning (EU) 2022/2554 det möjligt för de europeiska tillsynsmyndigheterna och de behöriga myndigheterna enligt den förordningen att delta i samarbetsgruppens verksamhet och att utbyta information och samarbeta med de gemensamma kontaktpunkterna och med CSIRT-enheterna och de behöriga myndigheterna enligt detta direktiv. De behöriga myndigheterna enligt förordning (EU) 2022/2554[++] bör även översända uppgifter om större IKT-relaterade incidenter och, i förekommande fall, betydande cyberhot till CSIRT-enheterna, de behöriga myndigheterna eller de gemensamma kontaktpunkterna enligt detta direktiv. Detta kan ske genom att ge omedelbar tillgång till incidentan-

([10]) Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (se sidan 1 i detta nummer av EUT).

mälningar, och antingen vidarebefordra dem direkt eller genom en gemensam kontaktpunkt. Vidare bör medlemsstaterna fortsätta att inkludera finanssektorn i sina strategier för cybersäkerhet, och CSIRT-enheterna kan inbegripa finanssektorn i sin verksamhet.

(29) För att undvika luckor eller överlappning mellan de cybersäkerhetsskyldigheter som åläggs entiteter inom luftfartssektorn bör de nationella myndigheterna enligt Europaparlamentets och rådets förordningar (EG) nr 300/2008 ([11]) och (EU) 2018/1139 ([12]) och de behöriga myndigheterna enligt detta direktiv samarbeta när det gäller genomförandet av riskhanteringsåtgärder för cybersäkerhet och tillsynen av efterlevnaden av de åtgärderna på nationell nivå. En entitets efterlevnad av de säkerhetskrav som fastställs i förordningarna (EG) nr 300/2008 och (EU) 2018/1139 och i relevanta delegerade akter och genomförandeakter som antagits i enlighet med de förordningarna kan av de behöriga myndigheterna enligt detta direktiv anses utgöra efterlevnad av motsvarande krav som fastställs i detta direktiv.

(30) Med tanke på kopplingarna mellan cybersäkerhet och entiteters fysiska säkerhet bör man säkerställa samstämmighet mellan Europaparlamentets och rådets direktiv (EU) 2022/2557 ([13]) och det här direktivet. För att uppnå detta bör entiteter som identifieras som kritiska entiteter enligt direktiv (EU) 2022/2557 anses vara väsentliga entiteter enligt det här direktivet. Vidare bör varje medlemsstat säkerställa att dess nationella strategi för cybersäkerhet tillhandahåller en politisk ram för ökad samordning inom den medlemsstaten mellan dess behöriga myndigheter enligt detta direktiv och de behöriga myndigheterna enligt direktiv (EU) 2022/2557 när det gäller informationsutbyte om risker, cyberhot och incidenter, liksom om icke-cyberrelaterade risker, hot och incidenter, samt utövande av tillsynsuppgifter. De behöriga myndigheterna enligt det här direktivet och direktiv (EU) 2022/2557 bör samarbeta och utbyta information utan onödigt dröjsmål, särskilt när det gäller identifiering av kritiska entiteter, risker, cyberhot och incidenter samt när det gäller icke-cyberrelaterade risker, hot och incidenter som påverkar kritiska entiteter, inbegripet cybersäkerhetsåtgärder och fysiska åtgärder som vidtas av kritiska entiteter samt resultaten av den tillsynsverksamhet som bedrivs med avseende på sådana entiteter.

För att effektivisera tillsynsverksamheten mellan de behöriga myndigheterna enligt det här direktivet och direktiv (EU) 2022/2557 och för att minimera den administrativa bördan för de berörda entiteterna bör de behöriga myndigheterna dessutom sträva efter att harmonisera mallarna för incidentanmälningar och tillsynsförfaranden. När så är lämpligt bör behöriga myndigheter enligt direktiv (EU) 2022/2557 kunna begära att behöriga myndigheter enligt det här direktivet utövar sina befogenheter med avseende på tillsyn och efterlevnadskontroll gentemot en entitet som identifieras som en kritisk entitet enligt direktiv (EU) 2022/2557. Det här direktivet och direktiv (EU) 2022/2557 bör, om möjligt i realtid, samarbeta och utbyta information i detta syfte.

(31) 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 riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter. Eftersom dessa frågor omfattas av det här direktivet är de skyldigheter som fastställs i kapitlen III, IV och VI i direktiv (EU) 2022/2557 inte tillämpliga på sådana entiteter.

([11]) 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).

([12]) 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).

([13]) Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (se sidan 164 i detta nummer av EUT).

(32) Att upprätthålla och bevara ett tillförlitligt, resilient och säkert domännamnssystem (DNS) är viktiga faktorer 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 vara tillämpligt på registreringsenheter för toppdomäner och leverantörer av DNS-tjänster, som bör förstås som entiteter som tillhandahåller allmänt tillgängliga rekursiva tjänster för att lösa domännamnsfrågor för internetslutanvändare eller auktoritativa tjänster för att lösa domännamnsfrågor för tredjepartsanvändning. Detta direktiv bör inte vara tillämpligt på rotnamnsservrar.

(33) Molntjänster bör omfatta digitala tjänster som möjliggör administration av beställtjänster och bred fjärråtkomst till en skalbar och elastisk pool av delbara och distribuerade dataresurser, även när sådana resurser är distribuerade på flera platser. Beräkningsresurser 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 en tjänst och nätverk som en tjänst. Distribueringsmodellerna för molntjänster bör omfatta privat moln, gemensamt moln, offentligt moln och hybridmoln. Molntjänste- 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 beräkningsresurser 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 beräkningsresurser som tillhandahålls 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 beräkningsresurser 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 beräkningsresurser som finns på olika nätverksanslutna datorer eller enheter och som kommunicerar och samordnar sig sinsemellan genom meddelandepassning.

(34) Med tanke på framväxten av innovativ teknik och nya affärsmodeller förväntas nya molntjänste- och distribueringsmodeller uppstå på den inre 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*).

(35) 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 därför omfatta leverantörer av datacentraltjänster som inte är molntjänster. Vid tillämpningen av detta direktiv bör termen *datacentraltjänst* omfatta 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* bör inte vara tillämplig på interna datacentraler som ägs och drivs av den berörda entiteten för egen räkning.

(36) Forskningsverksamhet spelar en nyckelroll i utvecklingen av nya produkter och processer. Mycket av den verksamheten genomförs av entiteter som delar, sprider eller utnyttjar resultaten av sin forskning i kommersiella syften. Dessa entiteter kan därför vara viktiga aktörer i värdekedjor, vilket gör säkerheten i deras nätverks- och informationssystem till en integrerad del av den övergripande cybersäkerheten på den inre marknaden. Forskningsorganisationer bör anses inbegripa entiteter som riktar in större delen av sin verksamhet på tillämpad forskning eller experimentell utveckling i den mening som avses i ”Frascatimanualen 2015: Riktlinjer för insamling och

rapportering av uppgifter om forskning och experimentell utveckling” från Organisationen för ekonomiskt samarbete och utveckling, i syfte att utnyttja sina resultat i kommersiella syften, såsom tillverkning eller utveckling av en produkt eller process, tillhandahållande av en tjänst, eller marknadsföring därav.

(37) De växande ömsesidiga beroendeförhållandena är resultatet av ett allt mer gränsöverskridande nätverk av tillhandahållande av tjänster, med ett inbördes beroende, som använder central infrastruktur över hela unionen inom sektorer såsom 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. De intensifierade cyberattackerna under covid-19-pandemin har visat sårbarheten hos alltmer av varandra beroende samhällena är för risker med låg sannolikhet.

(38) Mot bakgrund av skillnaderna i nationella förvaltningsstrukturer, och för att skydda befintliga sektorsspecifika arrangemang eller unionens tillsyns- och regleringsorgan, bör medlemsstaterna kunna utse eller inrätta en eller flera behöriga myndigheter med ansvar för cybersäkerhet och för tillsynsuppgifterna enligt detta direktiv.

(39) 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 gemensam kontaktpunkt med ansvar för samordningen av frågor angående säkerhet i nätverks- och informationssystem och gränsöverskridande samarbete på unionsnivå.

(40) De gemensamma kontaktpunkterna bör säkerställa effektivt gränsöverskridande samarbete med relevanta myndigheter i en annan medlemsstat och, när det är lämpligt, med kommissionen och Enisa. De gemensamma kontaktpunkterna bör därför ges i uppgift att vidarebefordra underrättelser om betydande incidenter med gränsöverskridande verkningar till de gemensamma kontaktpunkterna i andra berörda medlemsstater på begäran av CSIRT-enheten eller den behöriga myndigheten. På nationell nivå bör de gemensamma kontaktpunkterna möjliggöra smidigt sektorsövergripande samarbete med andra behöriga myndigheter. De gemensamma kontaktpunkterna kan också vara mottagare av relevant information om incidenter rörande finansiella entiteter från de behöriga myndigheterna enligt förordning (EU) 2022/2554, som de bör kunna vidarebefordra till CSIRT-enheterna eller de behöriga myndigheterna enligt detta direktiv, beroende på vad som är lämpligt.

(41) Medlemsstaterna bör ha både den tekniska och organisatoriska kapacitet som krävs för att förebygga, upptäcka, vidta åtgärder mot och begränsa incidenter och risker. Medlemsstaterna bör därför inrätta eller utse en eller flera CSIRT-enheter enligt detta direktiv och säkerställa att de har tillräckligt med resurser och teknisk kapacitet. CSIRT-enheterna bör uppfylla kraven enligt detta direktiv i syfte att garantera effektiv och kompatibel kapacitet att hantera incidenter och risker och säkerställa ett effektivt samarbete på unionsnivå. Medlemsstaterna bör kunna utse befintliga incidenthanteringsorganisationer (Cert) till CSIRT-enheter. För att stärka förtroendeförhållandet mellan entiteterna och CSIRT-enheterna bör medlemsstaterna, när en CSIRT-enhet är en del av de behörig myndighet, kunna överväga funktionell åtskillnad mellan de operativa uppgifter som utförs av CSIRT-enheterna, särskilt när det gäller informationsutbyte och bistånd till entiteterna, och de behöriga myndigheternas tillsynsverksamhet.

(42) CSIRT-enheterna ansvarar för incidenthantering. Detta omfattar behandling av stora mängder ibland känsliga uppgifter. Medlemsstaterna bör säkerställa att CSIRT-enheterna har en infrastruktur för utbyte och behandling av information, samt väl rustad personal, som säkerställer verksamhetens konfidentialitet och trovärdighet. CSIRT-enheterna kan även anta uppförandekoder i detta avseende.

(43) Vad gäller personuppgifter bör CSIRT-enheterna, i enlighet med förordning (EU) 2016/679, på begäran av en väsentlig eller viktig entitet tillhandahålla en proaktiv skanning av de nätverks- och informationssystem som används för att tillhandahålla entitetens tjänster. När det är tillämpligt bör medlemsstaterna sträva efter att säkerställa en lika hög nivå av teknisk kapacitet hos alla sektorsspecifika CSIRT-enheter. Medlemsstaterna bör kunna begära Enisas bistånd vid inrättandet av sina CSIRT-enheter.

(44) CSIRT-enheter bör ha förmåga att, på en väsentlig eller viktig entitets begäran, övervaka entitetens internettillvända tillgångar, både inom och utanför lokalerna, för att identifiera, förstå och hantera entitetens övergripande organisatoriska risker med avseende på nyligen identifierade kompromisser i leveranskedjan eller kritiska sårbarheter. Entiteten bör uppmuntras att meddela CSIRT-enheten om den har ett privilegierat hanteringsgränssnitt, då detta kan påverka hur snabbt begränsningsåtgärder kan vidtas.

(45) 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. För att utföra sina uppgifter bör CSIRT-enheterna och de behöriga myndigheterna därför kunna utbyta information, inklusive personuppgifter, med de nationella enheterna för hantering av it-säkerhetsincidenter eller behöriga myndigheter i tredjeländer, förutsatt att villkoren i unionens dataskyddslagstiftning för överföring av personuppgifter till tredjeländer är uppfyllda, bland annat villkoren i artikel 49 i förordning (EU) 2016/679.

(46) Det är angeläget att säkerställa tillräckliga resurser för att uppnå målen för detta direktiv och göra det möjligt för de behöriga myndigheterna och CSIRT-enheterna att utföra de uppgifter som fastställs i detta direktiv. Medlemsstaterna kan på nationell nivå införa en finansieringsmekanism för att täcka de nödvändiga utgifterna i samband med att offentliga entiteter med ansvar för cybersäkerheten i medlemsstaterna utför sina uppgifter i enlighet med detta direktiv. En sådan mekanism bör vara förenlig med unionsrätten samt proportionell och icke-diskriminerande och bör beakta olika tillvägagångssätt för att tillhandahålla säkra tjänster.

(47) CSIRT-nätverket bör fortsätta att bidra till att stärka förtroendet och tilliten 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.

(48) För att uppnå och behålla en hög cybersäkerhetsnivå bör de nationella strategier för cybersäkerhet som krävs enligt detta direktiv bestå av enhetliga ramar med strategiska mål och prioriteringar på cybersäkerhetsområdet samt en styrningsram för att uppnå dem. Dessa strategier kan bestå av ett eller flera instrument av lagstiftningskaraktär eller annan karaktär.

(49) Riktlinjer för cyberhygien utgör grunden för att skydda nätverks- och informationssystemens infrastruktur, maskinvara, programvara och säkerhet för onlinetillämpningar samt affärs- eller slutanvändardata som entiteter förlitar sig på. Riktlinjer för cyberhygien som omfattar en gemensam grundläggande uppsättning rutiner, bland annat uppdateringar av programvara och maskinvara, byte av lösenord, hantering av nya installationer, begränsning av användarkonton på administratörsnivå och säkerhetskopiering av data, möjliggör en proaktiv ram för beredskap samt övergripande säkerhet och trygghet i händelse av incidenter eller cyberhot. Enisa bör övervaka och analysera medlemsstaternas riktlinjer för cyberhygien.

(50) Medvetenhet om cybersäkerhet och cyberhygien är av väsentlig betydelse för att stärka cybersäkerheten inom unionen, särskilt mot bakgrund av det ökande antalet uppkopplade enheter som i tilltagande grad används vid cyberattacker. Ansträngningar bör göras för att öka den allmänna medvetenheten om risker kopplade till sådana enheter, samtidigt som bedömningar på unionsnivå kan bidra till att säkerställa samsyn i fråga om sådana risker på den inre marknaden.

(51) Medlemsstaterna bör uppmuntra användningen av all innovativ teknik, däribland artificiell intelligens, som kan förbättra upptäckten och förebyggandet av cyberattacker och göra det möjligt att styra över resurser till cyberattacker på ett effektivare sätt. Medlemsstaterna bör därför i sin nationella strategi för cybersäkerhet uppmuntra forsknings- och utvecklingsverksamhet för att underlätta användningen av sådan teknik, särskilt sådan som avser automatiserade eller halvautomatiserade cybersäkerhetsverktyg, och i förekommande fall utbyte av data som behövs för att utbilda användarna av sådan teknik och förbättra den. Användningen av innovativ teknik, däribland artificiell intelligens, bör vara förenlig med unionens dataskyddslagstiftning, däribland dataskyddsprinciperna om uppgifternas korrekthet, uppgiftsminimering, rättvisa och transparens samt datasäkerhet, såsom avancerad krypteringsteknik. Kraven på inbyggt dataskydd och dataskydd som standard enligt förordning (EU) 2016/679 bör utnyttjas till fullo.

(52) Cybersäkerhetsverktyg och applikationer med öppen källkod kan bidra till en högre grad av öppenhet och inverka positivt på effektiviteten i industriell innovation. Öppna standarder främjar interoperabilitet mellan säkerhetsverktyg, vilket gynnar säkerheten för berörda parter inom industrin. Cybersäkerhetsverktyg och applikationer med öppen källkod kan dra nytta av utvecklargemenskapen i stort och möjliggöra diversifiering av leverantörer. Öppen källkod kan leda till en mer transparent verifieringsprocess för cybersäkerhetsrelaterade verktyg och till en gemenskapsdriven process för att upptäcka sårbarheter. Medlemsstaterna bör därför kunna främja användningen av programvara med öppen källkod och öppna standarder genom att tillämpa riktlinjer för användning av öppna data och öppen källkod som ett led i säkerhet genom transparens. Riktlinjer som främjar införande och hållbar användning av cybersäkerhetsverktyg med öppen källkod är särskilt viktig för små och medelstora företag som har stora genomförandekostnader som kan minimeras om behovet av specifika applikationer eller verktyg minskades.

(53) Allmännyttiga tjänster är alltmer uppkopplade mot digitala nätverk i städer i syfte att förbättra städernas transportnät, uppgradera anläggningar för vattenförsörjning och avfallshantering och effektivisera belysning och uppvärmning i byggnader. Dessa digitaliserade allmännyttiga tjänster är sårbara för cyberattacker och riskerar i händelse av en lyckad cyberattack att vålla medborgarna omfattande skada på grund av att de är sammankopplade. Medlemsstaterna bör, som ett led i sin nationella strategi för cybersäkerhet, ta fram riktlinjer som hanterar utvecklingen av sådana sammankopplade eller smarta städer, och deras potentiella inverkan på samhället.

(54) På senare år har unionen upplevt en exponentiell ökning av attacker genom utpressningsprogram där sabotageprogram krypterar data och system och kräver en lösensumma för att låsa upp dem. Att attacker genom utpressningsprogram blir vanligare och allvarligare kan bero på flera faktorer, såsom olika attackmönster, kriminella affärsmodeller som kretsar kring ”utpressningsprogram som service” och kryptovalutor, krav på lösensumma och ökat antal attacker i leveranskedjan. Medlemsstaterna bör ta fram riktlinjer för att hantera det ökande antalet utpressningsattacker som ett led i sin nationella strategi för cybersäkerhet.

(55) Offentlig-privata partnerskap inom cybersäkerhet kan utgöra en lämplig ram för kunskapsutbyte, utbyte av bästa praxis och utveckling av samsyn bland berörda parter. Medlemsstaterna bör främja riktlinjer som stöder inrättande av cybersäkerhetsspecifika offentlig-privata partnerskap. Sådana riktlinjer bör bland annat klargöra tillämpningsområdet och de berörda aktörerna, styrningsmodellen, de tillgängliga finansieringsalternativen och samspelet mellan deltagande aktörer i samband med offentlig-privata partnerskap. Offentlig-privata partnerskap kan dra nytta av expertisen hos privata entiteter för att bistå behöriga myndigheter vid utvecklingen av avancerade tjänster och processer med informationsutbyte, tidiga varningar, cyberhots- och incidentövningar, krishantering och resiliensplanering.

(56) Medlemsstaterna bör i sina nationella strategier för cybersäkerhet ta itu med små och medelstora företags särskilda cybersäkerhetsbehov. Små och medelstora företag står, i hela unionen, för en stor andel av industri- och affärsmarknaden och har ofta svårt att anpassa sig till nya affärsmetoder i en mer uppkopplad värld, och till den digitala miljön, med anställda som arbetar hemifrån och en verksamhet som i allt högre grad bedrivs online. Vissa små och medelstora företag upplever särskilda cybersäkerhetsutmaningar, såsom låg cybermedvetenhet, bristande it-säkerhet på distans, höga kostnader för cybersäkerhetslösningar och en förhöjd hotnivå, t.ex. genom utpressningsprogram, och bör för detta få vägledning och bistånd. Små och medelstora företag blir i allt högre grad måltavlor för attacker i leveranskedjan på grund av att de har mindre strikta åtgärder för hantering av cybersäkerhetsrisker och attacker och på grund av det faktum att de har begränsade säkerhetsresurser. Sådana attacker i leveranskedjan påverkar inte bara små och medelstora företag och deras verksamhet isolerat utan kan också få en dominoeffekt i fråga om större attacker mot entiteter som de levererat till. Medlemsstaterna bör genom sina nationella strategier för cybersäkerhet hjälpa små och medelstora företag att ta itu med utmaningarna i sina

leveranskedjor. Medlemsstaterna bör ha en kontaktpunkt för små och medelstora företag på nationell eller regional nivå som antingen ger vägledning och bistånd till små och medelstora företag eller hänvisar dem till lämpliga organ för vägledning och bistånd i cybersäkerhetsrelaterade frågor. Medlemsstaterna uppmanas även att erbjuda tjänster såsom konfiguration av webbplatser och möjliggörande av loggning för mikroföretag och små företag som saknar sådan kapacitet.

(57) Inom ramen för sina nationella strategier för cybersäkerhet bör medlemsstaterna anta riktlinjer för främjande av ett aktivt cyberskydd som ett led i en vidare försvarsstrategi. I stället för reaktiva insatser innebär ett aktivt cyberskydd förebyggande, upptäckt, övervakning, analys och begränsning av överträdelser av nätverkssäkerheten, i kombination med användning av kapacitet som satts in inom och utanför det angripna nätverket. Detta kan bland annat innebära att medlemsstaterna erbjuder vissa entiteter kostnadsfria tjänster eller verktyg, t.ex. självbetjäningskontroller, upptäcktsverktyg och borttagningstjänster. Förmågan att snabbt och automatiskt utbyta och förstå information om och analyser av hot, varningar om cyberverksamhet samt motåtgärder är avgörande för att med förenade ansträngningar lyckas förebygga, upptäcka, hantera och blockera attacker mot nätverks- och informationssystem. Ett aktivt cyberskydd bygger på en defensiv strategi som utesluter offensiva åtgärder.

(58) Eftersom utnyttjandet av sårbarheter i nätverks- och informationssystem kan orsaka betydande störningar och skada, är snabb identifiering och snabbt åtgärdande av sådana sårbarheter en viktig faktor för att minska risken. Entiteter som utvecklar eller administrerar nätverks- och informationssystem bör därför inrätta lämpliga förfaranden för att hantera sårbarheter när de upptäcks. Eftersom sårbarheter ofta upptäcks och meddelas av tredjeparter, bör tillverkaren eller leverantören av IKT-produkter eller IKT-tjänster även införa nödvändiga förfaranden för att motta sårbarhetsinformation från tredjeparter. I detta avseende ger de internationella standarderna ISO/IEC 30111 och ISO/IEC 29147 vägledning om sårbarhetshantering och om delgivning av information om sårbarheter. En stärkt samordning mellan rapporterande fysiska och juridiska personer och tillverkare eller leverantörer av IKT-produkter eller IKT-tjänster är särskilt viktig för att underlätta den frivilliga ramen för delgivning av information om sårbarheter. Samordnad delgivning av information om sårbarheter specificerar en strukturerad process genom vilken sårbarheter rapporteras till tillverkaren eller leverantören av de potentiellt sårbara IKT-produkterna eller IKT-tjänsterna på ett sätt som gör det möjligt för denne att diagnostisera och åtgärda sårbarheten innan detaljerad information om sårbarheten meddelas tredjeparter eller allmänheten. Samordnad delgivning av information om sårbarheter bör även inbegripa samordning mellan den rapporterande fysiska eller juridiska personen och tillverkaren eller leverantören av de potentiellt sårbara IKT-produkterna eller IKT-tjänsterna vad gäller tidpunkten för åtgärdandet och offentliggörandet av sårbarheter.

(59) Kommissionen, Enisa och medlemsstaterna bör fortsätta att främja anpassningar till internationella standarder och befintlig bästa branschpraxis inom hantering av cybersäkerhetrisker, exempelvis inom säkerhetsbedömningar i leveranskedjan, informationsutbyte och delgivning av information om sårbarheter.

(60) Medlemsstaterna bör, i samarbete med Enisa, vidta åtgärder för att underlätta samordnad delgivning av information om sårbarheter genom att fastställa en relevant nationell policy. Som ett led i den nationella policyn 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 nationell rätt. Med tanke på att fysiska och juridiska personer som forskar om sårbarheter kan riskera straff- och civilrättsligt ansvar i vissa medlemsstater uppmuntras medlemsstaterna att anta riktlinjer för icke-lagföring av forskare i informationssäkerhet och befrielse från civilrättsligt ansvar för deras verksamhet.

(61) Medlemsstaterna bör utse en av sina CSIRT-enheter till samordnare, som bör fungera som betrodd mellanhand mellan rapporterande fysiska eller juridiska personer och tillverkare eller leverantörer av IKT-produkter eller IKT-tjänster som sannolikt kommer att påverkas av sårbarheten, när detta är nödvändigt. Den CSIRT-enhet som utsetts till samordnare bör bland annat ha i uppgift att identifiera och kontakta de berörda entiteterna, bistå de fysiska eller juridiska personer som rapporterar en sårbarhet, förhandla om tidsfrister för delgivning av information och hantera

sårbarheter som påverkar flera entiteter (samordnad delgivning av information om sårbarheter omfattande flera parter). Om den rapporterade sårbarheten kan ha en betydande påverkan på entiteter i fler än en medlemsstat bör de CSIRT-enheter som utsetts till samordnare samarbeta inom CSIRT-nätverket när så är lämpligt.

(62) Tillträde till korrekt information i lämplig tid om sårbarheter som påverkar IKT-produkter och IKT-tjänster bidrar till en förbättrad riskhantering på cybersäkerhetsområdet. Källor till offentligt tillgänglig information om sårbarheter är ett viktigt verktyg för entiteterna och användarna av deras tjänster, men även för behöriga myndigheter och CSIRT-enheter. Av denna anledning bör Enisa upprätta en europeisk sårbarhetsdatabas där entiteter, oberoende av om de omfattas av tillämpningsområdet för detta direktiv, och deras leverantörer av nätverks- och informationssystem, samt de behöriga myndigheterna och CSIRT-enheterna på frivillig basis kan meddela information om och registrera allmänt kända sårbarheter för att möjliggöra för användarna att vidta lämpliga riskreducerande åtgärder. Syftet med databasen är att hantera de unika utmaningar som risker innebär för entiteter i unionen. Vidare bör Enisa inrätta ett lämpligt förfarande för offentliggörandet för att ge entiteterna tid att vidta riskreducerande åtgärder när det gäller deras sårbarheter och använda avancerade riskhanteringsåtgärder på cybersäkerhetsområdet samt maskinläsbara dataset och motsvarande gränssnitt. För att uppmuntra en kultur där information lämnas om sårbarheter bör informationslämnande inte få negativa effekter för den rapporterande fysiska eller juridiska personen.

(63) Även om liknande sårbarhetsregister eller -databaser finns, förvaltas och underhålls de av entiteter som inte är etablerade i unionen. En europeisk sårbarhetsdatabas som underhålls av Enisa skulle ge förbättrad insyn i processen för offentliggörande innan sårbarheten meddelas offentligt samt motståndskraft i händelse av en störning eller ett avbrott i tillhandahållandet av liknande tjänster. För att i möjligaste mån undvika dubbelarbete och eftersträva komplementaritet bör Enisa undersöka möjligheten att ingå avtal om strukturerat samarbete med liknande register eller databaser som omfattas av ett tredjelands jurisdiktion. Enisa bör särskilt undersöka möjligheten till ett nära samarbete med operatörerna av systemet för gemensamma sårbarheter och exponeringar (*Common Vulnerabilities and Exposures* – CVE).

(64) Samarbetsgruppen bör stödja och underlätta strategiskt samarbete och informationsutbyte samt stärka förtroendet och tilliten mellan medlemsstaterna. Samarbetsgruppen bör upprätta ett arbetsprogram vartannat år. Arbetsprogrammet bör omfatta de åtgärder som samarbetsgruppen ska vidta för att genomföra sina mål och uppgifter. Tidsramen för att inrätta det första arbetsprogrammet enligt detta direktiv bör anpassas till tidsramen för det senaste arbetsprogram som inrättats enligt direktiv (EU) 2016/1148 i syfte att undvika potentiella avbrott i samarbetsgruppens arbete.

(65) 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, särskilt om hur ett samordnat införlivande av direktivet kan underlättas bland medlemsstaterna, som bör beaktas genom ett bättre genomförande av befintliga bestämmelser. Samarbetsgruppen skulle även kunna kartlägga de nationella lösningarna för att främja kompatibiliteten mellan de cybersäkerhetslösningar som tillämpas inom varje specifik sektor i unionen. Detta är särskilt relevant för sektorer av internationell eller gränsöverskridande karaktär.

(66) Samarbetsgruppen bör förbli ett flexibelt forum och kunna reagera på föränderliga och nya politiska prioriteringar och utmaningar samtidigt som tillgången till resurser beaktas. Den kan anordna regelbundna gemensamma möten med relevanta privata intressenter från hela unionen för att diskutera samarbetsgruppens verksamhet och inhämta uppgifter och synpunkter avseende framväxande politiska frågor. Dessutom bör samarbetsgruppen göra en regelbunden bedömning av läget när det gäller cyberhot eller incidenter, såsom utpressningsprogram. För att stärka

samarbetet på unionsnivå bör samarbetsgruppen överväga att bjuda in relevanta unionsinstitutioner, -organ, -kontor och -byråer som arbetar med frågor som rör cybersäkerhetspolitiken, såsom Europaparlamentet, Europol, Europeiska dataskyddsstyrelsen, Europeiska unionens byrå för luftfartssäkerhet, som inrättats genom förordning (EU) 2018/1139, och Europeiska unionens rymdprogrambyrå, som inrättats genom Europaparlamentets och rådets förordning (EU) 2021/696 ([14]), att delta i dess arbete.

(67) De behöriga myndigheterna och CSIRT-enheterna bör kunna delta i utbytesprogram för tjänstemän från andra medlemsstater inom en särskild ram och, i tillämpliga fall, efter det erforderliga säkerhetsgodkännandet för tjänstemän som deltar i sådana utbytesprogram, i syfte att förbättra samarbetet och stärka tilliten mellan medlemsstaterna. 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 eller CSIRT-värdenheten.

(68) Medlemsstaterna bör bidra till inrättandet av en EU-ram för hantering av cyberkriser enligt kommissionens rekommendation (EU) 2017/1584 ([15]) 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 specificerar detaljerna för detta samarbete och undvika dubbelarbete. Arbetsordningen för EU-CyCLONe bör ytterligare specificera de arrangemang enligt vilka det nätverket ska fungera, däribland nätverkets roller, samarbetsformer, samverkan med andra relevanta aktörer och mallar för informationsutbyte, samt kommunikationsmedel. För krishantering på unionsnivå bör berörda parter stödja sig på EU-arrangemangen för integrerad politisk krishantering enligt rådets genomförandebeslut (EU) 2018/1993 ([16]) (IPCR-arrangemang). 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.

(69) I enlighet med bilagan till rekommendation (EU) 2017/1584 bör en storskalig incident anses vara en cybersäkerhetsincident som orsakar störningar som är så omfattande att en medlemsstat inte kan hantera dem eller som har en betydande påverkan på minst två medlemsstater. Beroende på orsak och verkan kan storskaliga cybersäkerhetsincidenter eskalera och förvandlas till fullt utvecklade kriser som hindrar den inre marknaden från att fungera korrekt eller som allvarligt hotar den allmänna tryggheten och säkerheten för entiteter eller medborgare i flera medlemsstater eller i unionen som helhet. Med beaktande av sådana incidenters stora omfattning och, i de flesta fall, gränsöverskridande karaktär, bör medlemsstater och relevanta unionsinstitutioner, -organ, -kontor och -byråer samarbeta på teknisk, operativ och politisk nivå i syfte att på lämpligt sätt samordna insatserna i hela unionen.

(70) Storskaliga cybersäkerhetsincidenter och kriser på unionsnivå kräver samordnade åtgärder för att säkerställa snabba och effektiva insatser på grund av den höga graden av ömsesidigt beroende mellan sektorer och medlemsstater. Tillgången till cyberresilienta nätverks- och informationssystem och uppgifternas tillgänglighet, konfidentialitet och riktighet är av vital betydelse för unionens säkerhet och skyddet av dess medborgare, företag och institutioner mot incidenter och cyberhot och för att stärka människors och organisationers tilltro till unionens förmåga att främja och skydda en global, öppen, fri, stabil och säker cyberrymd som bygger på mänskliga rättigheter, grundläggande friheter, demokrati och rättsstatliga principer.

([14]) Europaparlamentets och rådets förordning (EU) 2021/696 av den 28 april 2021 om inrättande av unionens rymdprogram och Europeiska unionens rymdprogrambyrå och om upphävande av förordningarna (EU) nr 912/2010, (EU) nr 1285/2013 och (EU) nr 377/2014 och beslut nr 541/2014/EU (EUT L 170, 12.5.2021, s. 69).

([15]) 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).

([16]) Rådets genomförandebeslut (EU) 2018/1993 av den 11 december 2018 om EU-arrangemangen för integrerad politisk krishantering (EUT L 320, 17.12.2018, s. 28).

(71) EU-CyCLONe bör fungera som mellanhand mellan den tekniska och politiska nivån under storskaliga cybersäkerhetsincidenter och kriser och bör stärka samarbetet på operativ nivå och stödja beslutsfattandet på politisk nivå. I samarbete med kommissionen, och med beaktande av kommissionens behörighet inom krishantering, bör EU-CyCLONe ta fasta på CSIRT-nätverkets slutsatser och använda sin egen kapacitet för att göra en konsekvensanalys av storskaliga cybersäkerhetsincidenter och kriser.

(72) Cyberattacker är av en gränsöverskridande natur, och en betydande incident kan störa och skada kritisk informationsinfrastruktur som en välfungerande inre marknad är beroende av. Rekommendation (EU) 2017/1584 tar upp alla relevanta aktörers roller. Vidare är kommissionen inom ramen för unionens civilskyddsmekanism, som inrättats genom Europaparlamentets och rådets beslut nr 1313/2013/EU ([17]), ansvarig för allmänna beredskapsåtgärder, bland annat för att förvalta centrumet för samordning av katastrofberedskap och det gemensamma kommunikations- och informationssystemet för olyckor, upprätthålla och vidareutveckla situationsmedvetenhet och analyskapacitet samt upprätta och förvalta kapacitet att mobilisera och sända ut expertgrupper vid förfrågan om bistånd från en medlemsstat eller ett tredjeland. Kommissionen är även ansvarig för tillhandahållande av analytiska rapporter inför IPCR-arrangemang enligt genomförandebeslut (EU) 2018/1993, bland annat med avseende på situationsmedvetenhet och beredskap på cybersäkerhetsområdet, samt för situationsmedvetenhet och krishantering på områdena jordbruk, ogynnsamma väderförhållanden, kartläggning av och prognoser för konflikter, system för tidig varning vid naturkatastrofer, hälsokriser, övervakning av infektionssjukdomar, växtskydd, kemiska incidenter, livsmedels- och fodersäkerhet, djurhälsa, migration, tull, nukleära och radiologiska nödsituationer och energi.

(73) Unionen kan när det är lämpligt ingå internationella avtal, i enlighet med artikel 218 i EUF-fördraget, med tredjeländer eller internationella organisationer och därvid tillåta och organisera deras deltagande i särskild verksamhet inom samarbetsgruppen, CSIRT-nätverket och EU-CyCLONe. Sådana avtal bör säkerställa unionens intressen och ändamålsenligt skydd av uppgifter. Detta bör inte utesluta medlemsstaternas rätt att samarbeta med tredjeländer om hantering av sårbarheter och riskhantering på cybersäkerhetsområdet och därvid underlätta rapportering och allmänt informationsutbyte i enlighet med unionsrätten.

(74) För att underlätta ett effektivt genomförande av detta direktiv i fråga om bland annat hantering av sårbarheter, riskhanteringsåtgärder för cybersäkerhet, rapporteringsskyldigheter och arrangemang för informationsutbyte om cybersäkerhet kan medlemsstaterna samarbeta med tredjeländer och bedriva verksamhet som anses lämplig för detta ändamål, bland annat informationsutbyte om cyberhot, incidenter, sårbarheter, verktyg, metoder, taktik, tekniker och förfaranden, beredskap och övningar för cybersäkerhetskrishantering, utbildning, förtroendeskapande åtgärder och arrangemang för ett strukturerat informationsutbyte.

(75) Sakkunnigbedömningar bör införas i syfte att dra lärdom av delade erfarenheter, stärka det ömsesidiga förtroendet och uppnå en hög gemensam cybersäkerhetsnivå. Sakkunnigbedömningarna kan leda till värdefulla insikter och rekommendationer som kan stärka den övergripande cybersäkerhetskapaciteten, skapa ytterligare en funktionell väg för utbyte av bästa praxis mellan medlemsstater och bidra till att förbättra medlemsstaternas mognadsnivå inom cybersäkerhet. Vidare bör sakkunnigbedömningarna beakta resultaten av liknande mekanismer, såsom systemet för sakkunnigbedömning inom ramen för CSIRT-nätverket, samt tillföra mervärde och undvika dubbelarbete. Genomförandet av sakkunnigbedömningarna bör inte påverka tillämpningen av unionsrätt eller nationell rätt om skydd av konfidentiella eller säkerhetsskyddsklassificerade uppgifter.

(76) Samarbetsgruppen bör fastställa en självbedömningsmetod för medlemsstaterna för att täcka in faktorer såsom genomförandenivån för riskhanteringsåtgärderna för cybersäkerhet och rapporteringsskyldigheterna, kapacitetsnivån och effektiviteten i utförandet av de behöriga myndigheternas uppgifter, CSIRT-enheternas operativa kapacitet, genomförandenivån för det ömsesidiga biståndet, genomförandenivån för arrangemangen för informationsutbyte om cybersäkerhet eller särskilda frågor av gränsöverskridande eller sektorsövergripande karaktär. Medlemsstaterna bör uppmuntras att regelbundet genomföra självbedömningar och att presentera och diskutera resultaten av sina självbedömningar i samarbetsgruppen.

([17]) Europaparlamentets och rådets beslut nr 1313/2013/EU av den 17 december 2013 om en civilskyddsmekanism för unionen (EUT L 347, 20.12.2013, s. 924).

(77) Ansvaret för att säkerställa säkerheten i nätverks- och informationssystemen vilar i hög grad på väsentliga och viktiga entiteter. En riskhanteringskultur som inbegriper riskbedömningar och genomförande av riskhanteringsåtgärder för cybersäkerhet som är anpassade till riskerna bör främjas och utvecklas.

(78) Riskhanteringsåtgärder för cybersäkerhet bör ta hänsyn till i vilken grad den väsentliga eller viktiga entiteten är beroende av nätverks- och informationssystem och omfatta åtgärder för att identifiera eventuella incidentrisker, för att förebygga, upptäcka, hantera och återhämta sig från incidenter och för att begränsa deras inverkan. Säkerheten i nätverks- och informationssystem bör omfatta lagrade, överförda och behandlade uppgifters säkerhet. Riskhanteringsåtgärder för cybersäkerhet bör föreskriva systemanalys, med beaktande av den mänskliga faktorn, för att få en fullständig bild av nätverks- och informationssystemets säkerhet.

(79) Eftersom hot mot säkerheten i nätverks- och informationssystem kan ha olika ursprung bör riskhanteringsåtgärder för cybersäkerhet bygga på en allriskansats som syftar till att skydda nätverks- och informationssystem och dessa systems fysiska miljö mot händelser såsom stöld, brand, översvämning, telekommunikations- eller elavbrott eller obehörig fysisk åtkomst till och skada eller störning på en väsentlig eller viktig entitets information och informationsbehandlingsresurser, som kan undergräva tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem. Riskhanteringsåtgärderna för cybersäkerhet bör därför också omfatta den fysiska säkerheten och miljösäkerheten i nätverks- och informationssystem genom att inbegripa åtgärder för att skydda sådana system mot systemfel, mänskliga misstag, avsiktligt skadliga handlingar eller naturfenomen i överensstämmelse med europeiska och internationella standarder, såsom de som ingår i ISO/IEC 27000-serien. I detta avseende bör väsentliga och viktiga entiteter som ett led i sina riskhanteringsåtgärder för cybersäkerhet också ägna sig åt personalsäkerhet och inrätta lämpliga strategier för åtkomstkontroll. Dessa åtgärder bör vara förenliga med direktiv (EU) 2022/2557.

(80) För att påvisa efterlevnaden av riskhanteringsåtgärder för cybersäkerhet, och i frånvaro av lämpliga europeiska ordningar för cybersäkerhetscertifiering som antagits i enlighet med Europaparlamentets och rådets förordning (EU) 2019/881 ([18]), bör medlemsstaterna efter samråd med samarbetsgruppen och den europeiska gruppen för cybersäkerhetscertifiering främja användningen av relevanta europeiska och internationella standarder bland väsentliga och viktiga entiteter, eller så får de ålägga entiteter att använda certifierade IKT-produkter, IKT-tjänster och IKT-processer.

(81) För att undvika oproportionella finansiella och administrativa bördor för väsentliga och viktiga entiteter bör riskhanteringsåtgärderna för cybersäkerhet stå i proportion till riskerna för det berörda nätverks- och informationssystemet, med beaktande av teknikens ståndpunkt i fråga om sådana åtgärder, och i förekommande fall relevanta europeiska och internationella standarder, samt kostnaden för deras genomförande.

(82) Riskhanteringsåtgärder för cybersäkerhet bör stå i proportion till den väsentliga eller viktiga entitetens grad av exponering för risker och samhälleliga och ekonomiska konsekvenser som en incident skulle få. Vid fastställandet av riskhanteringsåtgärder för cybersäkerhet som är anpassade till väsentliga och viktiga entiteter bör vederbörlig hänsyn tas till väsentliga och viktiga entiteters olika riskexponering, t.ex. hur kritisk entiteten är, vilka risker, inklusive samhällsrisker, som den är exponerad för, hur stor entiteten är, hur sannolikt det är med incidenter och hur allvarliga de är, inklusive deras samhälleliga och ekonomiska konsekvenser.

([18]) 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).

(83) 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 de väsentliga och viktiga entiteternas interna it-personal eller vilkas säkerhet har lagts ut på entreprenad. De riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter som fastställs i detta direktiv bör tillämpas på de relevanta väsentliga och viktiga entiteterna oavsett om dessa entiteter underhåller sina nätverks- och informationssystem internt eller lägger ut underhållet på entreprenad.

(84) Med beaktande av deras gränsöverskridande karaktär bör leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster, leverantörer av marknadsplatser online, sökmotorer och plattformar för sociala nätverkstjänster samt tillhandahållare av betrodda tjänster omfattas av en hög nivå av harmonisering på unionsnivå. Genomförandet av riskhanteringsåtgärder för cybersäkerhet vad gäller dessa entiteter bör därför underlättas genom en genomförandeakt.

(85) Det är särskilt viktigt att hantera risker som härrör från en entitets leveranskedja och dess förhållande till sina leverantörer, såsom leverantörer av datalagrings- och databehandlingstjänster eller leverantörer av hanterade säkerhetstjänster och programredigerare, med tanke på förekomsten av incidenter där entiteter har varit föremål för cyberattacker och där inkräktare med avsikt att vålla skada har kunnat äventyra säkerheten i en entitets nätverks- och informationssystem genom att utnyttja sårbarheter som påverkar tredje parts produkter och tjänster. Väsentliga och viktiga entiteter bör därför bedöma och beakta den övergripande kvaliteten och resiliensen hos produkter och tjänster och de riskhanteringsåtgärder för cybersäkerhet som är inbyggda i dem samt cybersäkerhetspraxis hos sina leverantörer och tjänsteleverantörer, inbegripet deras förfaranden för säker utveckling. Väsentliga och viktiga entiteter bör framför allt uppmuntras att införliva riskhanteringsåtgärder för cybersäkerhet i avtal med sina direkta leverantörer och tjänsteleverantörer. Dessa entiteter kan beakta risker som härrör från leverantörer och tjänsteleverantörer på andra nivåer.

(86) Bland tjänsteleverantörerna har leverantörer av hanterade säkerhetstjänster på områden som incidenthantering, penetrationstester, säkerhetsrevisioner och konsulttjänster en särskilt viktig roll när det gäller att bistå entiteter i deras arbete med att förebygga, upptäcka, reagera på eller återhämta sig från incidenter. Leverantörer av hanterade säkerhetstjänster har dock också själva varit mål för cyberattacker, och eftersom de är nära integrerade i entiteternas verksamhet utgör de en särskild risk. Väsentliga och viktiga entiteter bör därför visa större noggrannhet vid valet av en leverantör av hanterade säkerhetstjänster.

(87) De behöriga myndigheterna kan också inom ramen för sina tillsynsuppgifter dra nytta av cybersäkerhetstjänster såsom säkerhetsrevisioner, penetrationstester eller incidenthantering.

(88) Väsentliga och viktiga entiteter bör också hantera risker som härrör från deras samverkan och förbindelser med andra intressenter inom ett vidare ekosystem, bland annat med avseende på att motverka industrispionage och skydda företagshemligheter. I synnerhet bör dessa entiteter 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 bör de väsentliga och viktiga entiteterna, med tanke på hur viktiga och värdefulla data är för deras verksamhet, vidta alla lämpliga riskhanteringsåtgärder för cybersäkerhet när de förlitar sig på dataomvandlings- och dataanalystjänster från tredje parter.

(89) Väsentliga och viktiga entiteter bör anta ett brett spektrum av grundläggande cyberhygienrutiner, såsom nollförtroende-principer, programuppdateringar, enhetskonfiguration, nätverkssegmentering, identitets- och åtkomsthantering eller användarmedvetenhet, anordna utbildning för sin personal och öka medvetenheten om cyberhot, nätfiske eller sociala manipuleringstekniker. Vidare bör dessa entiteter utvärdera sin egen cybersäkerhetskapacitet och när det är lämpligt fortsätta att integrera teknik för ökad cybersäkerhet, såsom artificiell intelligens eller maskininlärningssystem, för att förbättra sin kapacitet och säkerheten i nätverks- och informationssystemen.

(90) För att ytterligare hantera centrala risker i leveranskedjan och bistå väsentliga och viktiga entiteter som är verksamma i sektorer som omfattas av detta direktiv att på lämpligt sätt hantera risker i leveranskedjan och leverantörsrelaterade risker bör samarbetsgruppen, i samarbete med kommissionen och Enisa, och när så är lämpligt efter samråd med relevanta intressenter, även från industrin, utföra samordnade säkerhetsriskbedömningar av kritiska leveranskedjor, vilket redan gjorts för 5G-nät efter kommissionens rekommendation (EU) 2019/534 ([19]), i syfte att per sektor identifiera kritiska IKT-tjänster, IKT-system eller IKT-produkter, relevanta hot och sårbarheter. Sådana samordnade säkerhetsriskbedömningar bör fastställa åtgärder, riskreduceringsplaner och bästa praxis för att motverka kritiska beroenden, potentiella felkritiska systemdelar, hot, sårbarheter och andra risker kopplade till leveranskedjan och bör undersöka olika sätt att ytterligare uppmuntra en bredare användning av dessa från väsentliga och viktiga entiteters sida. Potentiella icke-tekniska riskfaktorer, såsom otillbörlig påverkan från ett tredjeland på leverantörer och tjänsteleverantörer, särskilt i samband med alternativa styrningsmodeller, inbegriper dolda sårbarheter eller bakdörrar och potentiella systemiska leveransstörningar, särskilt i samband med teknikinlåsning eller leverantörsberoende.

(91) De samordnade säkerhetsriskbedömningarna av kritiska leveranskedjor 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 EU:s samordnade riskbedömning av cybersäkerheten för 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 säkerhetsriskbedömning 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 under deras livscykel mot störningar, och v) för framväxande IKT-tjänster, IKT-system eller IKT-produkter, deras potentiella framtida betydelse för entiteternas verksamhet. Vidare bör särskild tonvikt läggas vid IKT-tjänster, IKT-system eller IKT-produkter som omfattas av särskilda krav som härrör från tredjeländer.

(92) För att rationalisera de skyldigheter som åläggs tillhandahållare av allmänna elektroniska kommunikationsnät eller av 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 de behöriga myndigheterna enligt Europaparlamentets och rådets direktiv (EU) 2018/1972 ([20]) respektive förordning (EU) nr 910/2014 att dra nytta av den rättsliga ram som inrättas genom detta direktiv, inbegripet utnämning av en CSIRT-enhet med ansvar för risk- och incidenthantering och deltagande av berörda behöriga myndigheter i samarbetsgruppens och CSIRT-nätverkets verksamhet, bör dessa entiteter omfattas av tillämpningsområdet för detta direktiv. De motsvarande bestämmelser som anges i förordning (EU) nr 910/2014 och i direktiv (EU) 2018/1972och som gäller införande av säkerhets- och anmälningskrav för dessa typer av entiteter bör därför utgå. De regler om rapporteringsskyldigheter som fastställs i det här direktivet bör inte påverka tillämpningen av förordning (EU) 2016/679 och direktiv 2002/58/EG.

(93) De cybersäkerhetsskyldigheter som fastställs i detta direktiv bör anses komplettera de krav som åläggs tillhandahållare av betrodda tjänster enligt förordning (EU) nr 910/2014. Tillhandahållare av betrodda tjänster bör vara skyldiga att vidta alla lämpliga och proportionella åtgärder för att hantera riskerna för sina tjänster, även med avseende på kunder och tredje parter som förlitar sig på dessa tjänster, och att rapportera incidenter enligt detta direktiv. Sådana cybersäkerhets- och rapporteringsskyldigheter bör även avse det fysiska skyddet av de tjänster som tillhandahålls. De krav för kvalificerade tillhandahållare av betrodda tjänster som fastställs i artikel 24 i förordning (EU) nr 910/2014 bör fortsätta att vara tillämpliga.

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

([20]) 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).

(94) Medlemsstaterna kan utse tillsynsorganen enligt förordning (EU) nr 910/2014 till behöriga myndigheter för betrodda tjänster för att säkerställa att nuvarande praxis upprätthålls och för att ta fasta på den kunskap och erfarenhet som förvärvats genom tillämpningen av den förordningen. I detta fall bör de behöriga myndigheterna enligt detta direktiv samarbeta nära och i lämplig tid med dessa tillsynsorgan 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 (EU) nr 910/2014. I förekommande fall bör CSIRT-enheten eller den behöriga myndigheten enligt detta direktiv omedelbart informera tillsynsorganet enligt förordning (EU) nr 910/2014 om eventuella betydande cyberhot eller incidenter som anmälts och som påverkar betrodda tjänster samt ifall en tillhandahållare av betrodda tjänster bryter mot detta direktiv. Medlemsstaterna kan för rapporteringsändamål i förekommande fall använda den gemensamma kontaktpunkt som inrättats för att uppnå en gemensam och automatisk rapportering av incidenter till både tillsynsorganet enligt förordning (EU) nr 910/2014 och CSIRT-enheten eller den behöriga myndigheten enligt detta direktiv.

(95) När så är lämpligt och för att undvika onödiga störningar bör befintliga nationella riktlinjer som antagits för att införliva bestämmelserna om säkerhetsåtgärder i artiklarna 40 och 41 i direktiv (EU) 2018/1972 beaktas vid införlivandet av det här direktivet för att ta fasta på den kunskap och kompetens som redan förvärvats inom ramen för direktiv (EU) 2018/1972 avseende säkerhetsåtgärder och incidentunderrättelser. Enisa kan också ta fram vägledning om säkerhetskrav och rapporteringsskyldigheter 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 enligt direktiv (EU) 2018/1972 för att säkerställa att nuvarande praxis upprätthålls och för att ta fasta på den kunskap och erfarenhet som förvärvats som en följd av genomförandet av det direktivet.

(96) Mot bakgrund av den ökande betydelsen av nummeroberoende interpersonella kommunikationstjänster enligt definitionen i direktiv (EU) 2018/1972 är det nödvändigt att säkerställa att sådana tjänster också omfattas av lämpliga säkerhetskrav med tanke på deras särskilda karaktär och ekonomiska betydelse. I takt med att attackytan fortsätter att växa blir nummeroberoende interpersonella kommunikationstjänster, såsom meddelandetjänster, utbredda attackvektorer. Inkräktare med uppsåt att vålla skada använder plattformar för att kommunicera och locka offer att öppna komprometterade webbsidor, vilket ökar sannolikheten för incidenter som involverar utnyttjande av personuppgifter och i förlängningen säkerhet i nätverks- och informationssystemen. Tillhandahållare av nummeroberoende interpersonella kommunikationstjänster bör säkerställa en säkerhetsnivå i nätverks- och informationssystemen som är lämplig i förhållande till de föreliggande riskerna. Eftersom tillhandahållare av nummeroberoende interpersonella kommunikationstjänster i allmänhet inte utövar 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 enligt definitionen i direktiv (EU) 2018/1972 som använder nummer och som inte utövar faktisk kontroll över signalöverföringen.

(97) Den inre marknaden är mer beroende av ett fungerande internet än någonsin. Tjänster från nästan alla väsentliga och viktiga entiteter är beroende av tjänster som tillhandahålls via internet. För att säkerställa ett smidigt tillhandahållande av tjänster som levereras av väsentliga och viktiga entiteter är det viktigt att alla tillhandahållare av allmänna elektroniska kommunikationsnät har infört lämpliga riskhanteringsåtgärder för cybersäkerhet och rapporterar betydande incidenter i samband med dessa. Medlemsstaterna bör säkerställa att säkerheten i de allmänna elektroniska kommunikationsnäten upprätthålls och att deras vitala säkerhetsintressen skyddas mot sabotage och spionage. Eftersom internationell konnektivitet förstärker och påskyndar en konkurrenskraftig digitalisering av unionen och dess ekonomi bör incidenter som påverkar undervattenskablar rapporteras till CSIRT-enheten eller i förekommande fall den behöriga myndigheten. Den nationella strategin för cybersäkerhet bör när så är relevant beakta cybersäkerheten för undervattenskablar och inbegripa kartläggning av potentiella cybersäkerhetsrisker och riskreduceringsåtgärder för att säkerställa högsta skyddsnivå för dem.

(98) För att trygga säkerheten för allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster bör användningen av krypteringsteknik främjas, särskilt totalsträckskryptering samt datacentrerade säkerhetskoncept, såsom kartografi, segmentering, taggning, åtkomstpolicy och åtkomsthantering samt automatiserade beslut om åtkomst. Vid behov bör användningen av kryptering, särskilt totalsträckskryptering, vara obligatorisk för tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster i enlighet med principerna om automatisk och inbyggd säkerhet och automatiskt och inbyggt integritetsskydd vid tillämpningen av detta direktiv. Användningen av totalsträckskryptering bör förenas med medlemsstaternas befogenheter att säkerställa skyddet av sina väsentliga säkerhetsintressen och sin allmänna säkerhet och att möjliggöra förebyggande, utredning, upptäckt och lagföring av brott i enlighet med unionsrätten. Detta bör dock inte försvaga totalsträckskrypteringen, som är en kritisk teknik för ett effektivt dataskydd, integritet och kommunikationssäkerhet.

(99) I syfte att trygga säkerheten för, och förebygga missbruk och manipulering av, allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster bör användningen av säkra dirigeringsstandarder främjas för att säkerställa dirigeringsfunktionernas integritet och robusthet längs hela ekosystemet av internetåtkomstleverantörer.

(100) I syfte att skydda internets funktion och integritet och främja domännamnssystemets säkerhet och resiliens bör relevanta intressenter, däribland privata unionsentiteter, tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster, särskilt internetåtkomstleverantörer, och leverantörer av sökmotorer uppmuntras att anta en strategi för diversifiering av DNS-uppslagning. Vidare bör medlemsstaterna uppmuntra utvecklingen och användningen av en allmän och säker europeisk DNS-resolvertjänst.

(101) I detta direktiv fastställs en flerstegsstrategi för rapportering av betydande incidenter för att hitta rätt balans mellan, å ena sidan, snabb rapportering som bidrar till att begränsa den potentiella spridningen av betydande incidenter och gör det möjligt för väsentliga och viktiga entiteter att söka bistånd och, å andra sidan, ingående rapportering som drar värdefulla lärdomar av enskilda incidenter och med tiden förbättrar cyberresiliensen hos enskilda entiteter och hela sektorer. I detta avseende bör detta direktiv omfatta rapportering av incidenter som, baserat på en första bedömning som utförts av den berörda entiteten, kan orsaka allvarliga störningar i tjänsterna eller ekonomiska förluster för den berörda entiteten eller påverka andra fysiska eller juridiska personer genom att orsaka betydande materiell eller immateriell skada. En sådan inledande bedömning bör bland annat ta hänsyn till de drabbade nätverks- och informationssystemen, särskilt deras betydelse för tillhandahållandet av entitetens tjänster, allvaret i och de tekniska egenskaperna hos cyberhotet och eventuella underliggande sårbarheter som utnyttjas, samt entitetens erfarenhet av liknande incidenter. Indikatorer såsom i vilken utsträckning tjänstens funktion påverkas, hur länge incidenten pågår eller hur många tjänstemottagare som drabbas kan spela en viktig roll när man fastställer om tjänstens driftsstörning är allvarlig.

(102) Om väsentliga eller viktiga entiteter får kännedom om en betydande incident bör de vara skyldiga att lämna in en tidig varning utan onödigt dröjsmål och under alla omständigheter inom 24 timmar. Denna tidiga varning bör åtföljas av en incidentanmälan. De berörda entiteterna bör lämna in en incidentanmälan utan onödigt dröjsmål och under alla omständigheter inom 72 timmar efter att ha fått kännedom om den betydande incidenten, särskilt i syfte att uppdatera den information som lämnats via den tidiga varningen och göra en inledande bedömning av den betydande incidenten, inbegripet dess allvarlighetsgrad och konsekvenser samt, i förekommande fall, angreppsindikatorer. En slutrapport bör lämnas in senast en månad efter incidentunderrättelsen. Den tidiga varningen bör endast innehålla den information som är nödvändig för att göra CSIRT-enheten, eller i förekommande fall den behöriga myndigheten, medveten om den betydande incidenten och ge den berörda entiteten möjlighet att vid behov söka bistånd. Den tidiga varningen bör i tillämpliga fall ange om den betydande incidenten misstänks vara orsakad av olagliga eller avsiktligt skadliga handlingar och om det är troligt att den kommer att få gränsöverskridande verkningar. Medlemsstaterna bör säkerställa att skyldigheten att lämna in den tidiga varningen, eller den efterföljande incidentunderrättelsen, inte avleder den underrättande entitetens resurser från verksamheter i samband med incidenthantering som bör prioriteras, i syfte att förhindra att skyldigheterna att rapportera incidenter antingen avleder resurser från hantering av betydande incidenter eller på annat sätt undergräver entitetens ansträngningar i

detta avseende. I händelse av en pågående incident vid den tidpunkt då slutrapporten lämnas in bör medlemsstaterna säkerställa att berörda entiteter tillhandahåller en lägesrapport vid den tidpunkten och en slutrapport inom en månad efter det att de hanterat den betydande incidenten.

(103) I tillämpliga fall bör väsentliga och viktiga entiteter utan dröjsmål underrätta sina tjänstemottagare om eventuella åtgärder eller avhjälpande arrangemang som dessa kan genomföra för att begränsa de risker som följer av ett betydande cyberhot. När så är lämpligt, och i synnerhet om det är sannolikt att det betydande cyberhotet kommer att förverkligas, bör dessa entiteter även informera sina tjänstemottagare om själva hotet. Kravet på att informera dessa mottagare om betydande cyberhot bör uppfyllas efter bästa förmåga men bör inte befria entiteter från skyldigheten att på egen bekostnad vidta lämpliga och omedelbara åtgärder för att förebygga eller avhjälpa sådana hot och återställa tjänstens normala säkerhetsnivå. Sådan information om betydande cyberhot bör tillhandahållas tjänstemottagarna kostnadsfritt och vara formulerad på ett lättbegripligt sätt.

(104) Tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster bör tillämpa inbyggd säkerhet och säkerhet som standard och informera sina tjänstemottagare om betydande cyberhot och om åtgärder dessa kan vidta för att skydda säkerheten för sina enheter och sin kommunikation, t.ex. genom att använda särskilda typer av programvara eller krypteringsteknik.

(105) En proaktiv strategi mot cyberhot är en viktig del av riskhanteringsåtgärderna för cybersäkerhet som bör göra det möjligt för de behöriga myndigheterna att effektivt förhindra att cyberhot blir incidenter som kan vålla betydande materiell eller immateriell skada. Det är därför av avgörande vikt att cyberhot anmäls. I detta syfte uppmuntras entiteter att rapportera cyberhot på frivillig basis.

(106) För att förenkla rapporteringen av information som krävs enligt detta direktiv och för att minska den administrativa bördan för entiteter bör medlemsstaterna tillhandahålla tekniska hjälpmedel såsom en gemensam kontaktpunkt, automatiserade system, onlineformulär, användarvänliga gränssnitt, mallar och särskilda plattformar för entiteter, oberoende av om de omfattas av tillämpningsområdet för detta direktiv, som de kan använda för att lämna in den relevanta information som ska rapporteras. Unionsfinansiering till stöd för genomförandet av detta direktiv, särskilt inom programmet för ett digitalt Europa, som inrättats genom Europaparlamentets och rådets förordning (EU) 2021/694 ([21]), kan inkludera stöd till gemensamma kontaktpunkter. Vidare befinner sig entiteter ofta i en situation där en viss incident på grund av sina särdrag måste rapporteras till flera olika myndigheter till följd av underrättelseskyldigheter enligt olika rättsliga instrument. Sådana fall skapar ytterligare administrativa bördor och kan också leda till osäkerhet om format och förfaranden för sådana underrättelser. Om en gemensam kontaktpunkt inrättas, uppmuntras medlemsstaterna även att använda denna gemensamma kontaktpunkt för underrättelser om säkerhetsincidenter enligt annan unionsrätt, såsom förordning (EU) 2016/679 och direktiv 2002/58/EG. Användningen av en sådan gemensam kontaktpunkt för att rapportera säkerhetsincidenter enligt förordning (EU) 2016/679 och direktiv 2002/58/EG bör inte påverka tillämpningen av bestämmelserna i förordning (EU) 2016/679 och direktiv 2002/58/EG, särskilt de som rör den oberoende ställningen för de myndigheter som avses i dessa. Enisa bör i samarbete med samarbetsgruppen utarbeta gemensamma mallar för underrättelser med hjälp av riktlinjer för att förenkla och rationalisera den information som ska rapporteras enligt unionsrätten och minska den administrativa bördan för de underrättande entiteterna.

(107) 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 Europeiska it-brottcentrumet (EC3) och Enisa.

([21]) Europaparlamentets och rådets förordning (EU) 2021/694 av den 29 april 2021 om inrättande av programmet för ett digitalt Europa och om upphävande av beslut (EU) 2015/2240 (EUT L 166, 11.5.2021, s. 1).

(108) 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 de myndigheter som avses i förordning (EU) 2016/679 och direktiv 2002/58/EG.

(109) Att upprätthålla korrekta och fullständiga databaser med registreringsuppgifter för domännamn (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 i hela unionen. För detta specifika ändamål bör registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster vara skyldiga att behandla vissa uppgifter som är nödvändiga för detta. Sådan behandling bör vara en rättslig förpliktelse i den mening som avses i artikel 6.1 c i förordning (EU) 2016/679. Denna förpliktelse bör inte påverka möjligheten att samla in registreringsuppgifter för domännamn för andra ändamål, exempelvis på grundval av avtal eller rättsliga skyldigheter som fastställs i annan unionsrätt eller nationell rätt. Denna förpliktelse syftar till att erhålla en fullständig och korrekt uppsättning registreringsuppgifter och bör inte resultera i att samma uppgifter samlas in flera gånger. Registreringsenheterna för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster bör samarbeta med varandra för att undvika dubbelarbete.

(110) Tillgänglighet avseende, och åtkomst i lämplig tid till, domännamnsregistreringsuppgifter för legitima åtkomstsökande är avgörande för att förebygga och bekämpa missbruk av domännamnssystem och för att förebygga, upptäcka och reagera på incidenter. Legitima åtkomstsökande bör tolkas som varje fysisk eller juridisk person som gör en begäran i enlighet med unionsrätten eller nationell rätt. Det kan inbegripa myndigheter som är behöriga enligt detta direktiv och sådana som enligt unionsrätten eller nationell rätt är behöriga i fråga om förebyggande, utredning, upptäckt eller lagföring av brott, samt Cert eller CSIRT-enheter. Registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster bör vara skyldiga att möjliggöra för legitima åtkomstsökande att få laglig åtkomst till specifika domännamnsregistreringsuppgifter som är nödvändiga för åtkomstbegärans syfte, i enlighet med unionsrätten och nationell rätt. Begäran från legitima åtkomstsökande bör åtföljas av en motivering som gör det möjligt att bedöma nödvändigheten av att få åtkomst till uppgifterna.

(111) För att säkerställa tillgången till korrekta och fullständiga registreringsuppgifter för domännamn bör registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster samla in registreringsuppgifter för domännamn och garantera deras integritet och tillgänglighet. I synnerhet bör registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster fastställa policyer och förfaranden för insamling och lagring av korrekta och fullständiga registreringsuppgifter för domännamn samt för att förhindra och korrigera felaktiga registreringsuppgifter i enlighet med unionens dataskyddslagstiftning. Dessa policyer och förfaranden bör så långt det är möjligt beakta de standarder som utvecklats av flerpartsförvaltningsstrukturerna på internationell nivå. Registreringsenheterna för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster bör anta och genomföra proportionella förfaranden för att verifiera registreringsuppgifterna för domännamn. Dessa förfaranden bör spegla bästa branschpraxis och, så långt det är möjligt, de framsteg som gjorts inom elektronisk identifiering. Exempel på verifieringsförfaranden kan vara förhandskontroller som görs i samband med registreringen och efterhandskontroller som görs efter registreringen. Registreringsenheterna för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster bör, i synnerhet, verifiera minst ett av registrantens kontaktsätt.

(112) Registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster bör vara skyldiga att offentliggöra domännamnsregistreringsuppgifter som inte omfattas av unionens dataskyddslagstiftning, till exempel uppgifter som rör juridiska personer, i överensstämmelse med ingressen till förordning (EU) 2016/679. När det gäller juridiska personer bör registreringsenheterna för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster offentliggöra åtminstone registrantens namn och telefonnummer. E-postadressen bör också offentliggöras förutsatt att den inte innehåller några personuppgifter, såsom när det gäller e-postalias eller funktionsbrevlådor. Registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster bör också möjliggöra för legitima åtkomstsökande att få laglig åtkomst till specifika domännamnsregistreringsuppgifter som rör fysiska personer, i enlighet med unionens dataskyddslagstiftning. Medlemsstaterna bör ålägga registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att utan onödigt dröjsmål besvara ansökningar om utlämnande av registreringsuppgifter för domännamn från legitima åtkomstsökande. Registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster bör fastställa policyer och förfaranden för offentliggörande och utlämnande av registreringsuppgifter, inbegripet servicenivåavtal för att hantera ansökningar om åtkomst från legitima åtkomstsökande. Dessa policyer och förfaranden bör så långt det är möjligt beakta eventuell vägledning

och de standarder som utvecklats av flerpartsförvaltningsstrukturerna på internationell nivå. Åtkomstförfarandet kan också omfatta användning av ett gränssnitt, en portal eller annat tekniskt verktyg som ett effektivt system för att begära och få tillgång till registreringsuppgifter. I syfte att främja harmoniserad praxis på hela den inre marknaden kan kommissionen, utan att det påverkar Europeiska dataskyddsstyrelsens befogenheter, tillhandahålla riktlinjer för sådana förfaranden, som i möjligaste mån beaktar de standarder som utvecklats av flerpartsförvaltningsstrukturerna på internationell nivå. Medlemsstaterna bör säkerställa att alla typer av åtkomst till registreringsuppgifter för domännamn, både personuppgifter och icke-personuppgifter, är kostnadsfria.

(113) Entiteter som omfattas av detta direktivs tillämpningsområde bör anses omfattas av jurisdiktionen i den medlemsstat där de är etablerade. Tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster bör dock anses omfattas av jurisdiktionen i den medlemsstat där de tillhandahåller sina tjänster. Leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, entiteter som tillhandahåller domännamnsregistreringstjänster, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster samt leverantörer av marknadsplatser online, sökmotorer och plattformar för sociala nätverkstjänster bör anses omfattas av jurisdiktionen i den medlemsstat där de har sitt huvudsakliga etableringsställe i unionen. Offentliga förvaltningsentiteter bör anses omfattas av jurisdiktionen i den medlemsstat som inrättat dem. 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 när det är lämpligt genomföra gemensamma tillsynsåtgärder. När medlemsstater utövar jurisdiktion bör de inte påföra efterlevnadskontrollåtgärder eller sanktioner mer än en gång för samma beteende, i överensstämmelse med principen *ne bis in idem*.

(114) För att ta hänsyn till den gränsöverskridande karaktären hos de tjänster och den verksamhet som utförs av leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, entiteter som tillhandahåller domännamnsregistreringstjänster, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster samt leverantörer av marknadsplatser online, sökmotorer och plattformar för sociala nätverkstjänster bör endast en medlemsstat ha jurisdiktion över dessa entiteter. Jurisdiktion bör tilldelas den medlemsstat där den berörda entiteten 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 anses ligga i den medlemsstat där besluten om åtgärder för att hantera cybersäkerhetsrisker i huvudsak fattas i unionen. Detta motsvarar vanligtvis platsen för entiteternas huvudkontor i unionen. Om en sådan medlemsstat inte kan fastställas eller om sådana beslut inte fattas i unionen bör det huvudsakliga etableringsstället anses vara beläget i den medlemsstat där cybersäkerhetsoperationer utförs. Om en sådan medlemsstat inte kan fastställas bör det huvudsakliga etableringsstället anses vara beläget i den medlemsstat där entiteten har etableringsstället med flest anställda i unionen. Om tjänsterna utförs av en koncern bör det kontrollerande företagets huvudsakliga etableringsställe betraktas som koncernens huvudsakliga etableringsställe.

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

(116) Om en leverantör av DNS-tjänster, en registreringsenhet för toppdomäner, en entitet som tillhandahåller domännamnsregistreringstjänster, en leverantör av molntjänster, en leverantör av datacentraltjänster, en leverantör av nätverk för leverans av innehåll, driftsentreprenad, en leverantör av hanterade säkerhetstjänster eller en leverantör av en marknadsplats online, en sökmotor eller en plattform för sociala nätverkstjänster, vilken inte är etablerad i unionen, erbjuder tjänster inom unionen bör den utse en företrädare i unionen. I syfte att fastställa om en sådan entitet erbjuder tjänster inom unionen bör det kontrolleras om 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 eller andra kontaktuppgifter är tillgängliga i unionen, eller att ett språk används som allmänt används i det tredjeland där entiteten är etablerad, bör inte betraktas som 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 det språket, 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 de behöriga myndigheterna eller CSIRT-enheterna att vända sig till 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.

(117) För att säkerställa en tydlig överblick över leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, entiteter som tillhandahåller domännamnsregistreringstjänster, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster samt leverantörer av marknadsplatser online, sökmotorer och plattformar för sociala nätverkstjänster, vilka tillhandahåller tjänster i unionen som omfattas av detta direktivs tillämpningsområde, bör Enisa skapa och upprätthålla ett register över sådana entiteter på grundval av information från medlemsstaterna, i förekommande fall via nationella mekanismer som inrättats för entiteter att registrera sig. De gemensamma kontaktpunkterna bör till Enisa vidarebefordra informationen och eventuella ändringar av densamma. För att säkerställa att den information som ska ingå i registret är korrekt och fullständig kan medlemsstaterna till Enisa lämna in den information som finns tillgänglig i nationella register om dessa entiteter. Enisa och medlemsstaterna bör vidta åtgärder för att underlätta kompatibilitet mellan sådana register, samtidigt som skydd av konfidentiell eller säkerhetsskyddsklassificerade uppgifter säkerställs. Enisa bör införa lämplig klassificering av information och förvaltningsprotokoll för att säkerställa den utlämnade informationens säkerhet och konfidentialitet och begränsa åtkomsten till samt lagringen och överföringen av sådan information till de avsedda användarna.

(118) Om uppgifter som är säkerhetsskyddsklassificerade enligt unionsrätt eller nationell rätt utbyts, rapporteras eller på annat sätt delas enligt detta direktiv, bör motsvarande regler för hantering av säkerhetsskyddsklassificerade uppgifter tillämpas. Vidare bör Enisa ha infrastruktur, förfaranden och regler för att hantera känsliga och säkerhetsskyddsklassificerade uppgifter i enlighet med tillämpliga säkerhetsregler för skydd av säkerhetsskyddsklassificerade EU-uppgifter.

(119) I och med att cyberhoten blir mer komplexa och sofistikerade är god upptäckt av sådana hot och förebyggande åtgärder mot dem 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 till 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 olika faktorer ha hindrat sådant utbyte av underrättelser, särskilt osäkerheten om förenligheten med konkurrens- och ansvarsreglerna.

(120) Entiteter bör uppmuntras och bistås av medlemsstaterna för att kollektivt utnyttja sina individuella kunskaper och praktiska erfarenheter på strategisk, taktisk och operativ nivå i syfte att förbättra sin förmåga att på lämpligt sätt förebygga, upptäcka, reagera på eller återhämta sig från incidenter eller begränsa deras verkningar. Det är därför nödvändigt att på unionsnivå möjliggöra framväxten av arrangemang för frivilligt informationsutbyte om cybersäkerhet. I detta syfte bör medlemsstaterna aktivt bistå och uppmuntra entiteter, såsom de som erbjuder cybersäkerhetstjänster och forskning, samt relevanta entiteter som inte omfattas av detta direktiv, att delta i sådana arrangemang för informationsutbyte om cybersäkerhet. Dessa arrangemang bör fastställas i enlighet med unionens konkurrensregler och unionens dataskyddslagstiftning.

(121) Behandling av personuppgifter i den utsträckning som är nödvändig och proportionell för att säkerställa säkerhet i nätverks- och informationssystem genom väsentliga och viktiga entiteter kan anses vara laglig på grund av att sådan behandling är förenlig med en rättslig förpliktelse som åvilar den personuppgiftsansvarige i enlighet med kraven i artikel 6.1 c och artikel 6.3 i förordning (EU) 2016/679. Behandling av personuppgifter kan även vara nödvändig på grund av berättigade intressen hos väsentliga och viktiga entiteter, samt tillhandahållare av säkerhetsteknik och säkerhetstjänster som agerar på dessa entiteters vägnar, i enlighet med artikel 6.1 f i förordning (EU) 2016/679, bland annat när sådan behandling är nödvändig för arrangemang för informationsutbyte om cybersäkerhet eller frivillig underrättelse om relevant information i enlighet med detta direktiv. Åtgärder som rör förebyggande, upptäckt, identifiering, begränsning, analys och hantering av incidenter, åtgärder för att öka medvetenheten om specifika cyberhot, informationsutbyte i samband med avhjälpande av sårbarheter och samordnat meddelande av sårbarhetsinformation, frivilligt informationsutbyte om sådana incidenter samt cyberhot och sårbarheter, angreppsindikatorer, taktik, tekniker och förfaranden, cybersäkerhetsvarningar och konfigurationsverktyg kan kräva behandling av vissa kategorier av personuppgifter, såsom ip-adresser, webbadresser (URL), domännamn, e-postadresser och tidsstämplar, när dessa avslöjar personuppgifter. Personuppgiftsbehandling av behöriga myndigheter, gemensamma kontaktpunkter och CSIRT-enheter kan utgöra en rättslig förpliktelse eller anses vara nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den ansvariges myndighetsutövning i enlighet med artikel 6.1 c eller e och artikel 6.3 i förordning (EU) 2016/679 eller på grund av ett berättigat intresse hos de väsentliga och viktiga entiteterna enligt vad som avses i artikel 6.1 f i den förordningen. Vidare kan nationell rätt innehålla bestämmelser som tillåter att behöriga myndigheter, gemensamma kontaktpunkter och CSIRT-enheter, i den utsträckning som är nödvändig och proportionell för att säkerställa säkerhet i nätverks- och informationssystem hos väsentliga och viktiga entiteter, behandlar särskilda kategorier av personuppgifter i enlighet med artikel 9 i förordning (EU) 2016/679, särskilt genom att föreskriva lämpliga och särskilda åtgärder för att skydda fysiska personers grundläggande rättigheter och intressen, däribland tekniska begränsningar för vidareutnyttjande av sådana uppgifter samt användning av moderna säkerhetsåtgärder och integritetsbevarande åtgärder, såsom pseudonymisering, eller kryptering där anonymisering avsevärt kan påverka det eftersträvade ändamålet.

(122) 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 dessa entiteter och de behöriga myndigheterna. Väsentliga entiteter bör därför omfattas av ett heltäckande tillsynssystem med förhandstillsyn och efterhandstillsyn, medan viktiga entiteter bör omfattas av enklare tillsyn, endast i efterhand. Viktiga entiteter bör därför inte vara skyldiga att systematiskt dokumentera efterlevnad av riskhanteringsåtgärderna för cybersäkerhet, medan de behöriga myndigheterna bör tillämpa en reaktiv efterhandstillsyn och därmed inte ha någon allmän skyldighet att utöva tillsyn över dessa entiteter. Efterhandstillsynen av viktiga entiteter kan utlösas av bevis, indikationer eller uppgifter som har kommit till de behöriga myndigheternas kännedom och som enligt dessa myndigheter tyder på potentiella överträdelser av 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.

(123) Behöriga myndigheters utförande av tillsynsuppgifter bör inte i onödan hämma den berörda entitetens affärsverksamhet. När behöriga myndigheter utför sina tillsynsuppgifter avseende väsentliga entiteter, bland annat genom inspektioner på plats och distansbaserad tillsyn, utredning av överträdelser av detta direktiv, säkerhetsrevisioner eller säkerhetsskanningar, bör de minimera konsekvenserna för den berörda entitetens affärsverksamhet.

(124) 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 ansats. 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 inspektion på plats, riktade säkerhetsrevisioner eller säkerhetsskanningar, vilken typ av information som ska begäras och detaljnivån på denna information. Sådana

tillsynsmetoder skulle även kunna åtföljas av arbetsprogram och utvärderas och ses över regelbundet, inklusive med avseende på aspekter som resursfördelning och resursbehov. När det gäller offentliga förvaltningsentiteter bör tillsynsbefogenheterna utövas i överensstämmelse med nationella lagstiftningsmässiga och institutionella ramar.

(125) De behöriga myndigheterna bör säkerställa att deras tillsynsuppgifter med avseende på väsentliga och viktiga entiteter utförs av utbildad personal, som bör ha de nödvändiga färdigheterna för att utföra dessa uppgifter, särskilt i fråga om att genomföra inspektioner på plats och distansbaserad tillsyn, bland annat identifiering av svagheter i databaser, maskinvara, brandväggar, kryptering och nätverk. Inspektionerna och tillsynen bör utföras på ett objektivt sätt.

(126) I vederbörligen motiverade fall bör den behöriga myndigheten, när den fått kännedom om ett betydande cyberhot eller en överhängande risk, kunna fatta omedelbara beslut om efterlevnadskontroll i syfte att förhindra eller reagera på en incident.

(127) För att efterlevnadskontrollen ska bli effektiv bör det fastställas en minimiförteckning över efterlevnadskontrollbefogenheter som kan utövas för brott mot de riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter som föreskrivs i detta direktiv, med en tydlig och konsekvent ram för sådan efterlevnadskontroll i hela unionen. Vederbörlig hänsyn bör tas till arten, allvarlighetsgraden och varaktigheten av överträdelsen av detta direktiv, de materiella eller immateriella skador som orsakats, om överträdelsen var avsiktlig eller berodde på försumlighet, åtgärder som vidtagits för att förhindra eller begränsa de materiella eller immateriella skadorna, graden av ansvar eller relevanta tidigare överträdelser, graden av samarbete med den behöriga myndigheten och andra försvårande eller förmildrande omständigheter. Efterlevnadskontrollåtgärderna, inklusive administrativa sanktionsavgifter, bör vara proportionella och påförandet av dem bör omfattas av lämpliga rättssäkerhetsgarantier i enlighet med de allmänna principerna i unionsrätten och Europeiska unionens stadga om de grundläggande rättigheterna (*stadgan*), inbegripet rätten till ett effektivt rättsmedel och till en opartisk domstol, oskuldspresumtion och rätten till försvar.

(128) Detta direktiv ålägger inte medlemsstaterna att föreskriva att fysiska personer med ansvar för att säkerställa att en entitet efterlever direktivet ska omfattas av straffrättsligt eller civilrättsligt ansvar för skada som åsamkats tredjeparter till följd av en överträdelse av direktivet.

(129) 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.

(130) Om en administrativ sanktionsavgift påförs en väsentlig eller viktig entitet som är 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 en administrativ sanktionsavgift påförs en person som inte är ett företag, bör den behöriga myndigheten 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.

(131) Medlemsstaterna bör kunna 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 Europeiska unionens domstols tolkning.

(132) När detta direktiv inte harmoniserar administrativa sanktioner eller när så är nödvändigt i andra fall, till exempel i händelse av en allvarlig överträdelse av detta direktiv, bör medlemsstaterna genomföra ett system med effektiva, proportionella och avskräckande sanktioner. Dessa påföljders art, och frågan om de är straffrättsliga eller administrativa, bör fastställas i nationell rätt.

(133) För att de sanktioner som är tillämpliga på överträdelser av efterlevnadskontrollåtgärder detta direktiv ska bli mer effektiva och avskräckande bör de behöriga myndigheterna ges befogenhet att tillfälligt upphäva eller begära tillfälligt upphävande av en certifiering eller auktorisation för en del av eller alla relevanta tjänster som tillhandahålls av en väsentlig entitet samt begära införande av ett tillfälligt förbud för en fysisk person som har ledningsansvar på nivån för verkställande direktör eller juridiskt ombud att utöva ledande funktioner. Med tanke på deras stränghet och påverkan på entiteternas verksamheter och i sista hand på användarna bör sådana tillfälliga upphävanden eller förbud endast tillämpas proportionellt mot överträdelsens allvarlighetsgrad och med beaktande av omständigheterna i varje enskilt fall, inbegripet om överträdelsen var avsiktlig eller berodde på försumlighet, samt åtgärder som vidtagits för att förhindra eller begränsa de materiella eller immateriella skadorna. Sådana tillfälliga upphävanden eller förbud 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 den berörda entiteten vidtar nödvändiga åtgärder för att avhjälpa de brister eller uppfylla de krav från den behöriga myndigheten för vilka de tillfälliga upphävandena eller förbuden tillämpades. Införandet av sådana tillfälliga upphävanden eller förbud bör omfattas av lämpliga rättssäkerhetsgarantier i enlighet med de allmänna principerna i unionsrätten och stadgan, inbegripet rätten till ett effektivt rättsmedel och till en opartisk domstol, oskuldspresumtion och rätten till försvar.

(134) För att säkerställa att entiteter fullgör sina skyldigheter enligt detta direktiv bör medlemsstaterna samarbeta med och bistå varandra med avseende på tillsyns- och efterlevnadskontrollåtgärder, särskilt om en entitet tillhandahåller tjänster i mer än en medlemsstat eller om dess nätverks- och informationssystem är belägna i en annan medlemsstat än den där den tillhandahåller tjänster. När den tillfrågade behöriga myndigheten tillhandahåller bistånd bör den vidta åtgärder för tillsyns- och efterlevnadskontrollåtgärder i enlighet med nationell rätt. För att säkerställa ett välfungerande ömsesidigt bistånd enligt detta direktiv bör de behöriga myndigheterna använda samarbetsgruppen som ett forum där de kan diskutera fall och enskilda biståndsansökningar.

(135) För att säkerställa effektiv tillsyn och efterlevnadskontroll, framför allt i en situation 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 entitet som är föremålet för den begäran och som tillhandahåller tjänster eller som har ett nätverks- och informationssystem inom den medlemsstatens territorium.

(136) Detta direktiv bör fastställa regler för samarbete mellan de behöriga myndigheterna och tillsynsmyndigheterna enligt förordning (EU) 2016/679 för att hantera överträdelser av detta direktiv som rör personuppgifter.

(137) Detta direktiv bör syfta till att säkerställa en hög ansvarsnivå för riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter för väsentliga och viktiga entiteter. Därför bör ledningsorganen för väsentliga och viktiga entiteter godkänna riskåtgärderna för cybersäkerhet och övervaka deras genomförande.

(138) För att säkerställa en hög gemensam cybersäkerhetsnivå i unionen på grundval av detta direktiv bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen med avseende på att komplettera detta direktiv genom att ange vilka kategorier av väsentliga och viktiga entiteter som ska vara skyldiga att använda vissa certifierade IKT-produkter, IKT-tjänster och IKT-processer eller erhålla ett certifikat enligt en europeisk ordning för cybersäkerhetscertifiering. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning ([22]). För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter erhåller Europaparlamentet och rådet alla handlingar samtidigt som medlemsstaternas experter, och deras experter ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.

([22]) EUT L 123, 12.5.2016, s. 1.

(139) För att säkerställa enhetliga villkor för genomförandet av detta direktiv bör kommissionen tilldelas genomförandebefogenheter för att fastställa de förfaranden som krävs för samarbetsgruppens verksamhet och de tekniska och metodologiska kraven samt sektorskraven avseende riskhanteringsåtgärder för cybersäkerhet, samt ytterligare precisera typen av information samt formatet och förfarandet för underrättelser om incidenter, cyberhot och tillbud och för kommunikation om betydande cyberhot, samt i vilka fall en incident ska betraktas som betydande. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011 ([23]).

(140) Detta direktiv bör med jämna mellanrum ses över av kommissionen i samråd med berörda parter, främst i syfte att avgöra huruvida det är lämpligt att föreslå ändringar med hänsyn till samhällsutvecklingen, den politiska utvecklingen, den tekniska utvecklingen eller ändrade marknadsvillkor. Som en del av de översynerna bör kommissionen bedöma vilken relevans de berörda entiteternas storlek och de sektorer, delsektorer och typer av entiteter som avses i bilagorna till detta direktiv har för ekonomins och samhällets funktion när det gäller cybersäkerhet. Kommissionen bör bland annat bedöma huruvida leverantörer som omfattas av tillämpningsområdet för detta direktiv vilka klassificeras som mycket stora onlineplattformar i den mening som avses i artikel 33 i Europaparlamentets och rådets förordning (EU) 2022/2065 ([24]) kan identifieras som väsentliga entiteter enligt detta direktiv.

(141) Detta direktiv skapar nya uppgifter för Enisa och stärker därigenom dess roll, och kan också leda till att Enisa tvingas utföra sina befintliga uppgifter enligt förordning (EU) 2019/881 på en högre nivå än tidigare. För att säkerställa att Enisa har de ekonomiska resurser och den personal som krävs för att utföra befintliga och nya uppgifter och uppnå en eventuellt högre nivå på genomförandet av dessa uppgifter till följd av dess utökade roll, bör dess budget ökas i motsvarande grad. För att säkerställa en effektiv resursanvändning bör Enisa dessutom ges större flexibilitet när det gäller möjligheten att fördela resurser internt, i syfte att kunna utföra sina uppgifter och infria förväntningarna på ett ändamålsenligt sätt.

(142) 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.

(143) Detta direktiv respekterar de grundläggande rättigheterna och iakttar de principer som erkänns i stadgan, i synnerhet rätten till respekt för privatliv och kommunikationer, skydd av personuppgifter, näringsfriheten, rätten till egendom, rätten till ett effektivt rättsmedel och till en opartisk domstol, oskuldspresumtion och rätten till försvar. Rätten till ett effektivt rättsmedel inbegriper mottagarna av tjänster som tillhandahålls av väsentliga och viktiga entiteter. Detta direktiv bör genomföras i enlighet med dessa rättigheter och principer.

(144) Europeiska datatillsynsmannen har hörts i enlighet med artikel 42.1 i Europaparlamentets och rådets förordning (EU) 2018/1725 ([25]) och avgav ett yttrande den 11 mars 2021 ([26]).

([23]) 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).

([24]) Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (rättsakten om digitala tjänster) (EUT L 277, 27.10.2022, s. 1).

([25]) Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG (EUT L 295, 21.11.2018, s. 39).

([26]) EUT C 183, 11.5.2021, s. 3.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Innehåll

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

2. Direktivet fastställer i detta syfte följande:

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

b) Riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter för entiteter av den typ som avses i bilaga I eller II samt för entiteter som identifieras som kritiska entiteter enligt direktiv (EU) 2022/2557.

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

d) Skyldigheter för medlemsstaterna när det gäller tillsyn och efterlevnadskontroll.

Artikel 2

Tillämpningsområde

1. Detta direktiv är tillämpligt på offentliga eller privata entiteter av den typ som avses i bilaga I eller II som betecknas som medelstora företag enligt artikel 2 i bilagan till kommissionens rekommendation 2003/361/EG eller överstiger de trösklar för medelstora företag som avses i punkt 1 i den artikeln och som tillhandahåller sina tjänster eller bedriver sin verksamhet i unionen.

Artikel 3.4 i bilagan till den rekommendationen är inte tillämplig med avseende på detta direktiv.

2. Oavsett entiteternas storlek är detta direktiv också tillämpligt på entiteter av en typ som avses i bilaga I eller II, i följande fall:

a) Om tjänster tillhandahålls av

   i) tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster,

   ii) tillhandahållare av betrodda tjänster,

   iii) registreringsenheter för toppdomäner och leverantörer av domännamnssystemtjänster.

b) Om entiteten är den enda leverantören i en medlemsstat av en tjänst som är väsentlig för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet.

c) Om en störning av den tjänst som entiteten tillhandahåller kan ha en betydande påverkan på skyddet för människors liv och hälsa, allmän säkerhet eller folkhälsa.

d) Om en störning av den tjänst som entiteten tillhandahåller kan medföra betydande systemrisker, särskilt för de sektorer där sådana störningar kan få gränsöverskridande konsekvenser.

e) Entiteten är kritisk på grund av sin särskilda betydelse på nationell eller regional nivå för en särskild sektor eller typ av tjänst, eller för andra sektorer i medlemsstaten som är beroende av denna entitet.

f) Om entiteten är en offentlig förvaltningsentitet

i) på statlig nivå såsom de definieras av en medlemsstat i enlighet med nationell rätt, eller

ii) på regional nivå såsom de definieras av en medlemsstat i enlighet med nationell rätt, som enligt en riskbaserad bedömning tillhandahåller tjänster vars störning kan ha en betydande effekt på kritisk samhällelig eller ekonomisk verksamhet.

3. Oavsett entiteternas storlek är detta direktiv tillämpligt på entiteter som identifieras som kritiska entiteter enligt direktiv (EU) 2022/2557.

4. Oavsett entiteternas storlek är detta direktiv tillämpligt på entiteter som tillhandahåller domännamnsregistreringstjänster.

5. Medlemsstaterna får föreskriva att detta direktiv ska tillämpas på

a) offentliga förvaltningsentiteter på lokal nivå,

b) utbildningsinstitut, särskilt om de utför kritisk forskningsverksamhet.

6. Detta direktiv påverkar inte medlemsstaternas ansvar för att skydda nationell säkerhet och deras befogenhet att skydda andra väsentliga statliga funktioner, inbegripet att säkerställa statens territoriella integritet och upprätthålla lag och ordning.

7. Detta direktiv är inte tillämpligt på offentliga förvaltningsentiteter som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott.

8. Medlemsstaterna får undanta särskilda entiteter som bedriver verksamhet på områdena nationell säkerhet, allmän säkerhet, försvar eller brottsbekämpning, inbegripet förebyggande, utredning, upptäckt och lagföring av brott, eller som tillhandahåller tjänster uteslutande till en offentlig förvaltningsentitet som avses i punkt 7 i den här artikeln, från skyldigheterna i artikel 21 eller 23 med avseende på sådan verksamhet eller sådana tjänster. I sådana fall ska de tillsyns- och efterlevnadskontrollåtgärder som avses i kapitel VII inte tillämpas på denna specifika verksamhet eller dessa specifika tjänster. Om entiteterna bedriver verksamhet eller tillhandahåller tjänster uteslutande av den typ som avses i den här punkten, får medlemsstaterna besluta att befria dessa entiteter också från skyldigheterna i artiklarna 3 och 27.

9. Punkterna 7 och 8 är inte tillämpliga om en entitet agerar som tillhandahållare av betrodda tjänster.

10. Detta direktiv är inte tillämpligt på entiteter som medlemsstaterna har undantagit från tillämpningsområdet för förordning (EU) 2022/2554 i enlighet med artikel 2.4 i den förordningen.

11. De skyldigheter som fastställs i detta direktiv ska inte medföra tillhandahållande av information vars utlämnande strider mot väsentliga intressen i fråga om medlemsstaternas nationella säkerhet, allmänna säkerhet eller försvar.

12. Detta direktiv påverkar inte tillämpningen av förordning (EU) 2016/679, direktiv 2002/58/EG, Europaparlamentets och rådets direktiv 2011/93/EU ([27]) och 2013/40/EU ([28]) och direktiv (EU) 2022/2557.

13. Utan att det påverkar tillämpningen av artikel 346 i EUF-fördraget ska information som är konfidentiell enligt unionsbestämmelser eller 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 berörda entiteters säkerhets- och affärsintressen skyddas.

([27]) 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).

([28]) 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).

14. Entiteter, behöriga myndigheter, gemensamma kontaktpunkter och CSIRT-enheter ska behandla personuppgifter i den utsträckning som krävs för tillämpningen av detta direktiv och i enlighet med förordning (EU) 2016/679, i synnerhet ska sådan behandling baseras på artikel 6 i denna.

Behandlingen av personuppgifter enligt detta direktiv av tillhandahållare av allmänna elektroniska kommunikationsnät eller tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster ska utföras i enlighet med unionens dataskydds- och integritetslagstiftning, särskilt direktiv 2002/58/EG.

Artikel 3

Väsentliga och viktiga entiteter

1. Med avseende på tillämpningen av detta direktiv ska följande entiteter anses vara väsentliga entiteter:

a) Entiteter av en typ som avses i bilaga I som överstiger trösklarna för medelstora företag som fastställs i artikel 2.1 i bilagan till rekommendation 2003/361/EG.

b) Kvalificerade tillhandahållare av betrodda tjänster och registreringsenheter för toppdomäner samt leverantörer av DNS-tjänster, oavsett storlek.

c) Tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster som betraktas som medelstora företag enligt artikel 2 i bilagan till rekommendation 2003/361/EG.

d) Offentliga förvaltningsentiteter som avses i artikel 2.2 f i.

e) Alla andra entiteter av en typ som avses i bilaga I eller II som av en medlemsstat identifierats som väsentliga entiteter i enlighet med artikel 2.2 b–e.

f) Entiteter som identifierats som kritiska entiteter enligt direktiv (EU) 2022/2557, som avses i artikel 2.3 i det här direktivet.

g) Entiteter som medlemsstaterna före den 16 januari 2023 har identifierat som leverantörer av samhällsviktiga tjänster i enlighet med direktiv (EU) 2016/1148 eller nationell rätt, om så föreskrivs av medlemsstaten.

2. Vid tillämpningen av detta direktiv ska alla entiteter av en typ som avses i bilaga I eller II och som inte betraktas som väsentliga entiteter enligt punkt 1 i denna artikel betraktas som viktiga entiteter. Detta inkluderar entiteter som av en medlemsstat identifierats som viktiga entiteter i enlighet med artikel 2.2 b–e.

3. Senast den 17 april 2025 ska medlemsstaterna upprätta en förteckning över väsentliga och viktiga entiteter samt entiteter som tillhandahåller domännamnsregistreringstjänster. Medlemsstaterna ska regelbundet och minst vartannat år därefter se över förteckningen och när det är lämpligt uppdatera den.

4. Vid upprättandet av den förteckning som avses i punkt 3 ska medlemsstaterna ålägga de entiteter som avses i den punkten att lämna minst följande information till de behöriga myndigheterna:

a) Entitetens namn.

b) Adress och aktuella kontaktuppgifter, inklusive e-postadresser, IP-adresser och telefonnummer.

c) I tillämpliga fall, den eller de relevanta sektorer och delsektorer som avses i bilaga I eller II.

d) I tillämpliga fall, en förteckning över de medlemsstater där de tillhandahåller tjänster som omfattas av detta direktiv.

De entiteter som avses i punkt 3 ska meddela alla ändringar av de uppgifter som de lämnat in enligt första stycket i denna punkt utan dröjsmål och under alla omständigheter inom två veckor från datumet för ändringen.

Kommissionen ska, med bistånd från Europeiska unionens cybersäkerhetsbyrå (Enisa), utan onödigt dröjsmål tillhandahålla riktlinjer och mallar för de skyldigheter som fastställs i denna punkt.

Medlemsstaterna får inrätta nationella mekanismer som gör det möjligt för entiteterna att registrera sig själva.

5. Senast den 17 april 2025 och därefter vartannat år ska de behöriga myndigheterna

a) underrätta kommissionen och samarbetsgruppen om antalet väsentliga och viktiga entiteter som förtecknats enligt punkt 3 för varje sektor och delsektor som avses i bilaga I eller II, och

b) lämna relevant information till kommissionen om antalet väsentliga och viktiga entiteter som identifierats i enlighet med artikel 2.2 b–e, den sektor och delsektor som avses i bilaga I eller II som de tillhör, den typ av tjänst som de tillhandahåller och de bestämmelser i artikel 2.2 b–e i enlighet med vilka de identifierades.

6. Fram till den 17 april 2025 och på begäran av kommissionen får medlemsstaterna meddela kommissionen namnen på de väsentliga och viktiga entiteter som avses i punkt 5 b.

Artikel 4

Sektorsspecifika unionsrättsakter

1. Om det i sektorsspecifika unionsrättsakter föreskrivs att väsentliga eller viktiga entiteter ska anta riskhanteringsåtgärder för cybersäkerhet eller underrätta om betydande incidenter, 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 VII, 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 unionsrättsakter.

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

a) riskhanteringsåtgärderna för cybersäkerhet minst är likvärdiga som de åtgärder som föreskrivs i artikel 21.1 och 21.2, eller

b) respektive sektorsspecifik unionsrättsakt föreskriver omedelbar, och när det är lämpligt automatisk och direkt, tillgång till incidentunderrättelser från CSIRT-enheterna, de behöriga myndigheterna eller de gemensamma kontaktpunkterna enligt detta direktiv och om kraven på underrättelse av betydande incidenter har minst samma verkan som de krav som fastställs i artikel 23.1–23.6 i detta direktiv.

3. Kommissionen ska senast den 17 juli 2023 tillhandahålla riktlinjer som klargör tillämpningen av punkterna 1 och 2. Kommissionen ska regelbundet se över dessa riktlinjer. Vid utarbetandet av dessa riktlinjer ska kommissionen ta hänsyn till eventuella synpunkter från samarbetsgruppen och Enisa.

Artikel 5

Minimiharmonisering

Detta direktiv hindrar inte medlemsstaterna från att anta eller behålla bestämmelser som säkerställer en högre cybersäkerhetsnivå, förutsatt att sådana bestämmelser står i överensstämmelse med medlemsstaternas förpliktelser enligt unionsrätten.

Artikel 6

Definitioner

I detta direktiv gäller följande definitioner:

1. nätverks- och informationssystem:

   a) Ett elektroniskt kommunikationsnät enligt definitionen 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.

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

3. *cybersäkerhet*: cybersäkerhet enligt definitionen i artikel 2.1 i förordning (EU) 2019/881.

4. *nationell strategi för cybersäkerhet*: en enhetlig ram i en medlemsstat med strategiska mål och prioriteringar på cybersäkerhetsområdet och en styrningsram för att uppnå dem i den medlemsstaten.

5. *tillbud*: en händelse som kunde ha undergrävt tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem, men som framgångsrikt hindrades från att utvecklas eller som inte uppstod.

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

7. *storskalig cybersäkerhetsincident*: en incident som orsakar störningar som är så omfattande att den berörda medlemsstaten inte kan hantera dem eller som har en betydande påverkan på minst två medlemsstater.

8. *incidenthantering*: alla åtgärder och förfaranden som syftar till att förebygga, upptäcka, analysera, begränsa eller reagera på och återhämta sig från en incident.

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

10. *cyberhot*: ett cyberhot enligt definitionen i artikel 2.8 i förordning (EU) 2019/881.

11. *betydande cyberhot*: ett cyberhot som, på grund av dess tekniska egenskaper, kan antas ha potential att ha en allvarlig påverkan på en entitets nätverks- och informationssystem eller användarna av entitetens tjänster genom att vålla betydande materiell eller immateriell skada.

12. *IKT-produkt*: en IKT-produkt enligt definitionen i artikel 2.12 i förordning (EU) 2019/881.

13. *IKT-tjänst*: en IKT-tjänst enligt definitionen i artikel 2.13 i förordning (EU) 2019/881.

14. *IKT-process*: en IKT-process enligt definitionen i artikel 2.14 i förordning (EU) 2019/881.

15. *sårbarhet*: en svaghet, känslighet eller brist hos IKT-produkter eller IKT-tjänster som kan utnyttjas genom ett cyberhot.

16. *standard*: en standard enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EU) nr 1025/2012 ([29]).

17. *teknisk specifikation*: en teknisk specifikation enligt definitionen i artikel 2.4 i förordning (EU) nr 1025/2012.

([29]) 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).

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

19. *domännamnssystem* eller *DNS*: ett hierarkiskt distribuerat namnsystem som möjliggör identifieringen av tjänster och resurser på internet, vilket gör det möjligt för slutanvändarenheter att använda internetrouting- och internetuppkopplingstjänster för att nå dessa tjänster och resurser.

20. *leverantör av DNS-tjänster*: en entitet som tillhandahåller

    a) allmänna rekursiva tjänster för att lösa domännamnsfrågor till internetslutanvändare, eller

    b) auktoritativa tjänster för att lösa domännamnsfrågor för användning av tredje part, med undantag för rotnamnsservrar.

21. *registreringsenhet för toppdomäner* eller *TLD-registreringsenhet*: 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, oberoende av huruvida någon aspekt av denna drift utförs av enheten själv eller har utkontrakterats, dock inte situationer där toppdomäner används av en registreringsenhet endast för dess eget bruk.

22. *entitet som erbjuder domännamnsregistreringstjänster*: en registrar som verkar på uppdrag av en regeringsenhet eller ett ombud för en registreringsenhet, såsom återförsäljare och leverantörer av integritetsregistreringstjänster och proxyregistreringstjänster.

23. *digital tjänst*: en tjänst enligt definitionen i artikel 1.1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535 ([30]).

24. *betrodd tjänst*: en betrodd tjänst enligt definitionen i artikel 3.16 i förordning (EU) nr 910/2014.

25. *tillhandahållare av betrodda tjänster*: en tillhandahållare av betrodda tjänster enligt definitionen i artikel 3.19 i förordning (EU) nr 910/2014.

26. *kvalificerad betrodd tjänst*: en kvalificerad betrodd tjänst enligt definitionen i artikel 3.17 i förordning (EU) nr 910/2014.

27. *kvalificerad tillhandahållare av betrodda tjänster*: en kvalificerad tillhandahållare av betrodda tjänster enligt definitionen i artikel 3.20 i förordning (EU) nr 910/2014.

28. *marknadsplats online*: en marknadsplats online enligt definitionen i artikel 2 n i Europaparlamentets och rådets direktiv 2005/29/EG ([31]).

29. *sökmotor*: en sökmotor enligt definitionen i artikel 2.5 i Europaparlamentets och rådets förordning (EU) 2019/1150 ([32]).

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

([30]) 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).

([31]) 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).

([32]) 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).

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

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

33. *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.

34. *företrädare*: en i unionen etablerad fysisk eller juridisk person som uttryckligen har utsetts att agera för en leverantör av DNS-tjänster, en registreringsenhet för toppdomäner, en entitet som tillhandahåller domännamnsregistreringstjänster, en leverantör av molntjänster, en leverantör av datacentraltjänster, en leverantör av nätverk för leverans av innehåll, driftsentreprenad, en leverantör av hanterade säkerhetstjänster, en leverantör av marknadsplatser online, av sökmotorer eller av en plattform för sociala nätverkstjänster som inte är etablerad i unionen, till vilka en 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.

35. *offentlig förvaltningsentitet*: en entitet som erkänts som sådan i en medlemsstat i enlighet med nationell rätt, med undantag för rättsväsendet, parlament och centralbanker, 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, regionala myndigheter eller andra offentligrättsliga organ, står under administrativ tillsyn av dessa 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.

36. *allmänt elektroniskt kommunikationsnät*: ett allmänt elektroniskt kommunikationsnät enligt definitionen i artikel 2.8 i direktiv (EU) 2018/1972.

37. *elektronisk kommunikationstjänst*: en elektronisk kommunikationstjänst enligt definitionen i artikel 2.4 i direktiv (EU) 2018/1972.

38. *entitet*: en 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.

39. *driftsentreprenad*: en entitet som tillhandahåller tjänster som rör installation, förvaltning, drift eller underhåll av IKT-produkter, IKT-nät, IKT-infrastruktur, IKT-tillämpningar eller andra nätverks- och informationssystem, via bistånd eller aktiv administration antingen i kundernas lokaler eller på distans.

40. *leverantör av hanterade säkerhetstjänster*: en leverantör av hanterade säkerhetstjänster som utför eller tillhandahåller stöd för verksamhet som rör hantering av cybersäkerhetsrisker.

41. *forskningsorganisation*: en entitet vars främsta mål är att bedriva tillämpad forskning eller experimentell utveckling i syfte att utnyttja resultaten av denna forskning i kommersiellt syfte, men som inte inbegriper utbildningsinstitutioner.

KAPITEL II

SAMORDNADE RAMVERK FÖR CYBERSÄKERHET

Artikel 7

Nationell strategi för cybersäkerhet

1. Varje medlemsstat ska anta en nationell strategi för cybersäkerhet som tillhandahåller strategiska mål, de resurser som krävs för att uppnå dessa mål och relevanta politiska och reglerande åtgärder, i syfte att uppnå och upprätthålla en hög cybersäkerhetsnivå. Den nationella strategin för cybersäkerhet ska inbegripa

a) mål och prioriteringar för medlemsstatens strategi för cybersäkerhet som särskilt omfattar de sektorer som avses i bilagorna I och II,

b) en styrningsram för att uppnå de mål och prioriteringar som avses i led a i denna punkt, inbegripet de politiska åtgärder som avses i punkt 2,

c) en styrningsram som klargör roller och ansvarsområden för relevanta intressenter på nationell nivå och som stöder samarbetet och samordningen på nationell nivå mellan de gemensamma myndigheterna, de gemensamma kontaktpunkterna och CSIRT-enheterna enligt detta direktiv, samt samordningen och samarbetet mellan dessa organ och behöriga myndigheter enligt sektorsspecifika unionsrättsakter,

d) en mekanism för att identifiera relevanta tillgångar och en bedömning av riskerna i den medlemsstaten,

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

f) en förteckning över de olika myndigheter och intressenter som är involverade i genomförandet av den nationella strategin för cybersäkerhet,

g) en politisk ram för förbättrad samordning mellan de behöriga myndigheterna enligt detta direktiv och de behöriga myndigheterna enligt direktiv (EU) 2022/2557, i syfte att utbyta information om risker, cyberhot och incidenter och icke-cyberrelaterade risker, hot och incidenter och utföra tillsynsuppgifter, beroende på vad som är lämpligt,

h) en plan, med nödvändiga åtgärder, för att höja medborgarnas allmänna medvetenhet om cybersäkerhetshot.

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

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

b) Riktlinjer för att inkludera och specificera cybersäkerhetsrelaterade krav för IKT-produkter och IKT-tjänster vid offentlig upphandling, inbegripet vad gäller cybersäkerhetscertifiering, kryptering och användning av cybersäkerhetsprodukter med öppen källkod.

c) Riktlinjer för hantering av sårbarheter, inbegripet främjande och underlättande av samordnad delgivning av information om sårbarheter enligt artikel 12.1.

d) Riktlinjer för att upprätthålla den allmänna tillgängligheten, integriteten och konfidentialiteten hos den offentliga kärnan i det öppna internet, inbegripet, i tillämpliga fall, cybersäkerheten hos undervattenskablar.

e) Riktlinjer för att främja utveckling och integrering av relevant avancerad teknik som syftar till att genomföra moderna riskhanteringsåtgärder för cybersäkerhet.

f) Riktlinjer för att främja och utveckla cybersäkerhetsutbildning, cybersäkerhetskompetens, medvetandehöjande åtgärder och forsknings- och utvecklingsinitiativ, samt vägledning om god praxis och kontroll för cyberhygien som riktar sig till medborgare, intressenter och entiteter.

g) Riktlinjer för stöd till akademiska institutioner och forskningsinstitut för att utveckla, förbättra och främja användningen av cybersäkerhetsverktyg och säker nätinfrastruktur.

h) Riktlinjer, inbegripet relevanta förfaranden och lämpliga verktyg för informationsutbyte för att stödja ett frivilligt informationsutbyte om cybersäkerhet mellan entiteter i enlighet med unionsrätten.

i) Riktlinjer som stärker cyberresiliensen och cyberhygienen hos små och medelstora företag, särskilt de som inte omfattas av detta direktiv, genom att tillhandahålla lättillgänglig vägledning och stöd för deras specifika behov.

j) Riktlinjer för att främja ett aktivt cyberskydd.

3. Medlemsstaterna ska meddela sina nationella strategier för cybersäkerhet till kommissionen inom tre månader från det att de antagits. Härvid får medlemsstaterna undanta information 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 uppdatera dem. Enisa ska på medlemsstaternas begäran bistå medlemsstaterna vid utarbetandet eller uppdateringen av en nationell strategi för cybersäkerhet och centrala resultatindikatorer för bedömningen av strategin, i syfte att anpassa den till de krav och skyldigheter som fastställs i detta direktiv.

Artikel 8

Behöriga myndigheter och gemensamma kontaktpunkter

1. Varje medlemsstat ska utse eller inrätta en eller flera behöriga myndigheter med ansvar för cybersäkerhet och för de tillsynsuppgifter som avses i kapitel VII (behöriga myndigheter).

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

3. Varje medlemsstat ska utse eller inrätta en gemensam kontaktpunkt. Om en medlemsstat bara utser eller inrättar en behörig myndighet i enlighet med punkt 1, 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, när det är lämpligt, kommissionen och Enisa samt ett sektorsövergripande samarbete med andra behöriga myndigheter i medlemsstaten.

5. Medlemsstaterna ska säkerställa att deras behöriga myndigheter och gemensamma kontaktpunkter har tillräckliga resurser för att på ett ändamålsenligt och effektivt sätt utföra de uppgifter de tilldelas och därigenom uppnå målen med detta direktiv.

6. Varje medlemsstat ska utan onödigt dröjsmål meddela kommissionen identiteten för den behöriga myndighet som avses i punkt 1 och den gemensamma kontaktpunkt som avses i punkt 3, dessa myndigheters uppgifter samt eventuella senare ändringar. Varje medlemsstat ska offentliggöra sin behöriga myndighets identitet. Kommissionen ska upprätta en förteckning över offentligt tillgängliga gemensamma kontaktpunkter.

Artikel 9

Nationella ramar för hantering av cybersäkerhetskriser

1. Varje medlemsstat ska utse eller inrätta en eller flera behöriga myndigheter med ansvar för hanteringen av storskaliga cybersäkerhetsincidenter och kriser (cyberkrishanteringsmyndigheter). Medlemsstaterna ska säkerställa att dessa myndigheter har tillräckliga resurser för att kunna utföra sina uppgifter på ett ändamålsenligt och effektivt sätt. Medlemsstaterna ska säkerställa samstämmighet med befintliga ramar för allmän nationell krishantering.

2. Om en medlemsstat utser eller inrättar mer än en cyberkrishanteringsmyndighet enligt punkt 1 ska den tydligt ange vilken av dessa myndigheter som ska samordna hanteringen av storskaliga cybersäkerhetsincidenter och kriser.

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

4. Varje medlemsstat ska anta en nationell plan för hanteringen av storskaliga cybersäkerhetsincidenter och kriser där mål och villkor för hanteringen av storskaliga cybersäkerhetsincidenter och kriser fastställs. Planen ska särskilt innehålla följande:

a) Målen för nationella beredskapsåtgärder och beredskapsverksamheter.

b) Cyberkrishanteringsmyndigheternas uppgifter och ansvarsområden.

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

d) Nationella beredskapsåtgärder, inbegripet övningar och utbildningsverksamhet.

e) Berörda offentliga och privata intressenter 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 cybersäkerhetsincidenter och kriser på unionsnivå.

5. Inom tre månader från det att den cyberkrishanteringsmyndighet som avses i punkt 1 har utsetts eller inrättats ska varje medlemsstat meddela kommissionen sin myndighets identitet samt alla senare ändringar. Medlemsstaterna ska till kommissionen och Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe) lämna relevant information avseende kraven i punkt 4 om sina nationella planer för hanteringen av storskaliga cybersäkerhetsincidenter och kriser inom tre månader från det att dessa planer antagits. Medlemsstaterna får undanta information om och i den utsträckning det är nödvändigt för den nationella säkerheten.

Artikel 10

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

1. Varje medlemsstat ska utse eller inrätta en eller flera CSIRT-enheter. CSIRT-enheterna får utses eller inrättas inom en behörig myndighet. CSIRT-enheterna ska uppfylla kraven i artikel 11.1, ska omfatta minst de sektorer, delsektorer och typer av entiteter som avses i bilagorna I och II och ska ansvara för incidenthantering i enlighet med ett tydligt fastställt förfarande.

2. Medlemsstaterna ska säkerställa att varje CSIRT-enhet har tillräckliga resurser för att på ett ändamålsenligt sätt kunna utföra sina uppgifter enligt artikel 11.3.

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 intressenter. För detta ändamål ska medlemsstaterna säkerställa att varje CSIRT-enhet bidrar till införandet av säkra verktyg för informationsutbyte.

4. CSIRT-enheterna ska samarbeta och, när det är lämpligt, utbyta relevant information i enlighet med artikel 29 med sektoriella eller sektorsövergripande grupper av väsentliga och viktiga entiteter.

5. CSIRT-enheterna ska delta i sakkunnigbedömningar som organiseras i enlighet med artikel 19.

6. Medlemsstaterna ska säkerställa ett ändamålsenligt, effektivt och säkert samarbete mellan sina CSIRT-enheter i CSIRT-nätverket.

7. CSIRT-enheter får upprätta samarbetsförbindelser med tredjeländers nationella enheter för hantering av it-säkerhetsincidenter. Som en del av sådana samarbetsförbindelser ska medlemsstaterna underlätta ett ändamålsenligt, effektivt och säkert informationsutbyte med dessa nationella enheter för hantering av it-säkerhetsincidenter i tredjeländer, med hjälp av relevanta protokoll för informationsutbyte, inbegripet Traffic Light Protocol. CSIRT-enheter får utbyta relevant information med tredjeländers nationella enheter för hantering av it-säkerhetsincidenter, inbegripet personuppgifter i enlighet med unionens dataskyddslagstiftning.

8. CSIRT-enheter får samarbeta med tredjeländers nationella enheter för hantering av it-säkerhetsincidenter eller motsvarande organ i tredjeländer, särskilt i syfte att ge dem cybersäkerhetsstöd.

9. Varje medlemsstat ska utan onödigt dröjsmål meddela kommissionen identiteten för den CSIRT-enhet som avses i punkt 1 i denna artikel och för den CSIRT-enhet som utsetts till samordnare i enlighet med artikel 12.1, deras respektive uppgifter i förhållande till de väsentliga och viktiga entiteterna samt alla senare ändringar.

10. Medlemsstaterna får begära Enisas bistånd vid inrättandet av sina CSIRT-enheter.

Artikel 11

Krav på CSIRT-enheter och deras tekniska kapacitet och uppgifter

1. CSIRT-enheter ska uppfylla följande krav:

a) CSIRT-enheterna ska säkerställa en hög nivå av tillgänglighet för sina kommunikationskanaler 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) CSIRT-enheternas lokaler och de informationssystem som de använder sig av ska vara belägna på säkra platser.

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

d) CSIRT-enheterna ska säkerställa verksamhetens konfidentialitet och trovärdighet.

e) CSIRT-enheterna ska ha tillräckligt med personal för att säkerställa att deras tjänster är ständigt tillgängliga och de ska säkerställa att personalen har fått lämplig utbildning.

f) CSIRT-enheterna ska utrustas med redundanta system och reservlokaler för att säkerställa kontinuiteten i deras tjänster.

De ska kunna delta i internationella samarbetsnätverk.

2. Medlemsstaterna ska säkerställa att deras CSIRT-enheter tillsammans har nödvändig teknisk kapacitet för att utföra de uppgifter som avses i punkt 3. Medlemsstaterna ska säkerställa att tillräckliga resurser anslås till deras CSIRT-enheter för att säkerställa en tillräcklig personalstyrka för att göra det möjligt för CSIRT-enheterna att utveckla sin tekniska kapacitet.

3. CSIRT-enheterna ska ha följande uppgifter:

a) Övervakning och analys av cyberhot, sårbarheter och incidenter på nationell nivå och, på begäran, tillhandahållande av stöd till berörda väsentliga och viktiga entiteter avseende realtidsövervakning eller nära realtidsövervakning av deras nätverks- och informationssystem.

b) Tillhandahållande av tidiga varningar, larm, meddelanden och spridning av information till väsentliga och viktiga entiteter samt till behöriga myndigheter och andra relevanta intressenter om cyberhot, sårbarheter och incidenter, om möjligt i nära realtid.

c) Vidtagande av åtgärder till följd av incidenter och, i tillämpliga fall, tillhandahållande av stöd till de berörda väsentliga och viktiga entiteterna.

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

e) Tillhandahållande, på begäran av den väsentliga eller viktiga entiteten, av en proaktiv skanning av den berörda entitetens nätverks- och informationssystem i syfte att upptäcka sårbarheter med en potentiellt betydande påverkan.

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

g) I tillämpliga fall, fungera som processamordnare för den samordnade delgivningen av information om sårbarheter enligt artikel 12.1.

h) Bidrag till införandet av säkra verktyg för informationsutbyte enligt artikel 10.3.

CSIRT-enheterna får utföra en proaktiv, icke-inkräktande skanning av väsentliga och viktiga entiteters allmänt tillgängliga nätverks- och informationssystem. Sådan skanning ska utföras för att upptäcka sårbara eller osäkert konfigurerade nätverks- och informationssystem och informera de berörda enheterna. Sådan skanning får inte ha någon negativ inverkan på hur entiteternas tjänster fungerar.

När CSIRT-enheterna utför de uppgifter som avses i första stycket får de prioritera särskilda uppgifter på grundval av en riskbaserad metod.

4. CSIRT-enheterna ska upprätta samarbetsförbindelser med relevanta intressenter inom den privata sektorn i syfte att uppnå målen för detta direktiv.

5. För att underlätta det samarbete som avses i punkt 4 ska CSIRT-enheterna främja antagande och användning av gemensamma eller standardiserade metoder, klassificeringssystem och taxonomier när det gäller

a) förfaranden för incidenthantering,

b) krishantering, och

c) samordnad delgivning av information om sårbarheter enligt artikel 12.1.

Artikel 12

Samordnad delgivning av information om sårbarheter och en europeisk sårbarhetsdatabas

1. Varje medlemsstat ska utse en av sina CSIRT-enheter till samordnare för den samordnade delgivningen av informationen om sårbarheter. Den CSIRT-enhet som utsetts till samordnare ska fungera som betrodd mellanhand och vid behov underlätta interaktionen mellan en fysisk eller juridisk person som rapporterar en sårbarhet och tillverkaren eller leverantören av de potentiellt sårbara IKT-produkterna eller IKT-tjänsterna, på begäran av endera parten. Den CSIRT-enhet som utsetts till samordnare ska bland annat

a) identifiera och kontakta de berörda entiteterna,

b) stödja de fysiska eller juridiska personer som rapporterar en sårbarhet, och

c) förhandla om tidsramar för delgivning av information och hantera sårbarheter som påverkar flera entiteter.

Medlemsstaterna ska säkerställa att fysiska eller juridiska personer kan, anonymt om de så begär, rapportera en sårbarhet till den CSIRT-enhet som utsetts till samordnare. Den CSIRT-enhet som utsetts till samordnare ska säkerställa att skyndsamma uppföljningsåtgärder vidtas med avseende på den rapporterade sårbarheten och ska säkerställa anonymiteten för den fysiska eller juridiska person som rapporterar sårbarheten. Om en rapporterad sårbarhet kan ha en betydande påverkan på entiteter i fler än en medlemsstat, ska den CSIRT-enhet som utsetts till samordnare i varje berörd medlemsstat, när det är lämpligt, samarbeta med andra CSIRT-enheter som utsetts till samordnare inom CSIRT-nätverket.

2. Enisa ska, efter samråd med samarbetsgruppen, utveckla och underhålla en europeisk sårbarhetsdatabas. I detta syfte ska Enisa inrätta och underhålla lämpliga informationssystem, riktlinjer och förfaranden och anta nödvändiga tekniska och organisatoriska åtgärder för att säkerställa den europeiska sårbarhetsdatabasens säkerhet och integritet, särskilt för att göra det möjligt för entiteter, oberoende om de omfattas av tillämpningsområdet för detta direktiv, 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. Alla intressenter ska få tillgång till informationen om de sårbarheter som finns i den europeiska sårbarhetsdatabasen. Databasen ska innehålla

a) information som beskriver sårbarheten,

b) den berörda IKT-produkten eller IKT-tjänsten och hur allvarlig sårbarheten är med tanke på de omständigheter under vilka den kan utnyttjas,

c) tillgången till relaterade programfixar och, i avsaknad av tillgängliga programfixar, vägledning som tillhandahållits av behöriga myndigheter eller CSIRT-enheter riktad till användare av sårbara IKT-produkter och IKT-tjänster om hur riskerna med meddelade sårbarheter kan begränsas.

Artikel 13

Samarbete på nationell nivå

1. Om de är separata ska de behöriga myndigheterna, den gemensamma kontaktpunkten och CSIRT-enheterna i en och samma medlemsstat samarbeta sinsemellan när det gäller fullgörandet av skyldigheter enligt detta direktiv.

2. Medlemsstaterna ska säkerställa att deras CSIRT-enheter eller, i tillämpliga fall, deras behöriga myndigheter, mottar underrättelser om betydande incidenter enligt artikel 23, och incidenter, cyberhot och tillbud enligt artikel 30.

3. Medlemsstaterna ska säkerställa att deras CSIRT-enheter eller, i tillämpliga fall, deras behöriga myndigheter informerar sina gemensamma kontaktpunkter om de underrättelser om incidenter, cyberhot och tillbud som lämnas in i enlighet med detta direktiv.

4. För att säkerställa att de behöriga myndigheternas, de gemensamma kontaktpunkternas och CSIRT-enheternas uppgifter och skyldigheter utförs på ett effektivt sätt, ska medlemsstaterna, i den utsträckning det är möjligt, säkerställa ett lämpligt samarbete mellan dessa organ och brottsbekämpande myndigheter, dataskyddsmyndigheter, nationella myndigheter enligt förordningarna (EG) nr 300/2008 och (EU) 2018/1139, tillsynsorganen enligt förordning (EU) nr 910/2014, behöriga myndigheter enligt förordning (EU) 2022/2554, nationella regleringsmyndigheter enligt direktiv (EU) 2018/1972, behöriga myndigheter enligt direktiv (EU) 2022/2557 samt behöriga myndigheter enligt andra sektorsspecifika unionsrättsakter, i den medlemsstaten.

5. Medlemsstaterna ska säkerställa att deras behöriga myndigheter enligt detta direktiv och deras behöriga myndigheter enligt direktiv (EU) 2022/2557 regelbundet samarbetar och utbyter information avseende identifieringen av kritiska entiteter, om risker, cyberhot och incidenter samt icke-cyberrelaterade risker, hot och incidenter som berör väsentliga entiteter som identifierats som kritiska i enlighet med direktiv (EU) 2022/2557, samt om de åtgärder som vidtagits till följd av sådana risker, hot och incidenter. Medlemsstaterna ska också säkerställa att deras behöriga myndigheter enligt detta direktiv och deras behöriga myndigheter enligt förordning (EU) nr 910/2014, förordning (EU) 2022/2554 och direktiv (EU) 2018/1972 regelbundet utbyter relevant information, även när det gäller relevanta incidenter och cyberhot.

6. Medlemsstaterna ska förenkla rapporteringen med tekniska medel för de underrättelser som avses i artiklarna 23 och 30.

KAPITEL III

SAMARBETE PÅ UNIONSNIVÅ OCH PÅ INTERNATIONELL NIVÅ

Artikel 14

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 7.

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 myndigheterna i enlighet med förordning (EU) 2022/2554 får delta i samarbetsgruppens verksamhet i enlighet med artikel 47.1 i den förordningen.

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

Kommissionen ska tillhandahålla sekretariatet.

4. Samarbetsgruppen ska ha följande uppgifter:

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

b) Tillhandahålla vägledning till behöriga myndigheter angående utarbetande och genomförande av strategier för den samordnade delgivningen av information om sårbarheter som avses i artikel 7.2 c.

c) 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, samt identifiering av väsentliga och viktiga entiteter i enlighet med artikel 2.2 b–e.

d) Utbyta råd och samarbeta med kommissionen om framväxande politiska initiativ för cybersäkerhet samt om den övergripande förenligheten mellan sektorsspecifika cybersäkerhetskrav.

e) Utbyta råd och samarbeta med kommissionen om utkast till delegerade akter eller genomförandeakter som antas i enlighet med detta direktiv.

f) Utbyta bästa praxis och information med relevanta institutioner, organ och byråer på unionsnivå.

g) Diskutera genomförandet av sektorsspecifika unionsrättsakter som innehåller bestämmelser om cybersäkerhet.

h) När så är lämpligt, diskutera de rapporter från sakkunnigbedömningar som avses i artikel 19.9 samt utarbeta slutsatser och rekommendationer.

i) Genomföra samordnade säkerhetsriskbedömningar av kritiska leveranskedjor i enlighet med artikel 22.1.

j) Diskutera fall av ömsesidigt bistånd, inbegripet erfarenheter och resultat av sådan gränsöverskridande gemensam tillsynsverksamhet som avses i artikel 37.

k) På begäran av en eller flera berörda medlemsstater, diskutera särskilda begäranden om ömsesidigt bistånd som avses i artikel 37.

l) Tillhandahålla strategisk vägledning till CSIRT-nätverket och EU-CyCLONe om specifika framväxande frågor.

m) Utbyta åsikter om politiken för uppföljningsåtgärder efter storskaliga cybersäkerhetsincidenter och kriser på grundval av lärdomarna från CSIRT-nätverket och EU-CyCLONe.

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

o) Anordna regelbundna gemensamma möten med relevanta privata intressenter från hela unionen för att diskutera samarbetsgruppens verksamhet och inhämta synpunkter på framväxande politiska frågor.

p) Diskutera det arbete som utförts i samband med cybersäkerhetsövningar, inbegripet det arbete som utförs av Enisa.

q) Fastställa metoder och organisatoriska aspekter för de sakkunnigbedömningar som avses i artikel 19.1 samt fastställa en självbedömningsmetod för medlemsstaterna i enlighet med artikel 19.5, med bistånd av kommissionen och Enisa, och, i samarbete med kommissionen och Enisa, utarbeta uppförandekoder som ligger till grund för de utsedda cyberssäkerhetsexperternas arbetsmetoder i enlighet med artikel 19.6.

r) Utarbeta rapporter för den översyn som avses i artikel 40 om de erfarenheter som förvärvats på strategisk nivå och från sakkunnigbedömningar.

s) Regelbundet diskutera och genomföra en bedömning av läget när det gäller cyberhot eller cyberincidenter, såsom utpressningsprogram.

Samarbetsgruppen ska överlämna de rapporter som avses i första stycket led r till kommissionen, Europaparlamentet och rådet.

5. Medlemsstaterna ska säkerställa att deras företrädare i samarbetsgruppen samarbetar på ett ändamålsenligt, effektivt och säkert sätt.

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

7. Samarbetsgruppen ska senast den 1 februari 2024 och därefter vartannat år utarbeta ett arbetsprogram för de åtgärder som ska vidtas för att genomföra dess mål och uppgifter.

8. Kommissionen får anta genomförandeakter i vilka de förfaranden som krävs för samarbetsgruppens verksamhet fastställs.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2.

Kommissionen ska utbyta råd och samarbeta med samarbetsgruppen om de utkast till genomförandeakter som avses i första stycket i denna punkt i enlighet med punkt 4 e.

9. Samarbetsgruppen ska regelbundet och under alla omständigheter minst en gång om året sammanträda med den grupp för kritiska entiteters motståndskraft som inrättats enligt direktiv (EU) 2022/2557, för att främja och underlätta strategiskt samarbete och informationsutbyte.

Artikel 15

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 de CSIRT-enheter som utsetts eller inrättats i enlighet med artikel 10 och incidenthanteringsorganisationen för unionens institutioner, organ och byråer (Cert-EU). Kommissionen ska som observatör delta i CSIRT-nätverket. Enisa ska tillhandahålla sekretariatet och aktivt bidra med stöd till samarbetet mellan CSIRT-enheterna.

3. CSIRT-nätverket ska ha följande uppgifter:

a) Utbyta information om CSIRT-enheternas kapacitet.

b) Underlätta delning, överföring och utbyte av teknik och relevanta åtgärder, strategier, verktyg, processer, bästa praxis och ramar mellan CSIRT-enheterna.

c) Utbyta relevant information om incidenter, tillbud, cyberhot, risker och sårbarheter.

d) Utbyta information med avseende på publikationer och rekommendationer om cybersäkerhet.

e) Säkerställa interoperabilitet när det gäller specifikationer och protokoll för informationsutbyte.

f) På begäran av en medlem av CSIRT-nätverket som potentiellt berörs av en incident, utbyta och diskutera information om den incidenten och relaterade cyberhot, risker och sårbarheter.

g) På begäran av en medlem av CSIRT-nätverket, diskutera och om möjligt genomföra en samordnad åtgärd till följd av en incident som har identifierats inom den medlemsstatens jurisdiktion.

h) Ge medlemsstaterna stöd när det gäller att hantera gränsöverskridande incidenter i enlighet med detta direktiv.

i) Samarbeta och utbyta bästa praxis med och ge stöd till CSIRT-enheter som utsetts till samordnare i enlighet med artikel 12.1 när det gäller hanteringen av samordnad information om sårbarheter som kan ha en betydande påverkan på entiteter i mer än en medlemsstat.

j) 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 plan för hantering av storskaliga cybersäkerhetsincidenter och kriser som avses i artikel 9.4 på begäran av en medlemsstat.

k) Informera samarbetsgruppen om sin verksamhet och om ytterligare former av operativt samarbete som diskuteras enligt led j och vid behov begära vägledning i detta avseende.

l) Utvärdera cybersäkerhetsövningar, bland annat sådana som anordnas av Enisa.

m) På begäran av en enskild CSIRT-enhet diskutera den enhetens kapacitet och beredskap.

n) Samarbeta och utbyta information med säkerhetscentrum (SOC) på regional nivå och unionsnivå, för att förbättra den gemensamma situationsmedvetenheten om incidenter och cyberhot i hela unionen.

o) När så är lämpligt, diskutera de rapporter från sakkunnigbedömningar som avses i artikel 19.9.

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

4. CSIRT-nätverket ska senast den 17 januari 2025 och därefter vartannat år, i samband med den översyn som avses i artikel 40, bedöma de framsteg som gjorts när det gäller det operativa samarbetet och anta en rapport. Rapporten ska särskilt innehålla slutsatser och rekommendationer om resultaten av de sakkunnigbedömningar som avses i artikel 19, som utförs med avseende på de nationella CSIRT-enheterna. Rapporten ska lämnas till samarbetsgruppen.

5. CSIRT-nätverket ska anta sin arbetsordning.

6. CSIRT-nätverket och EU-CyCLONe ska komma överens om förfaranden och samarbeta på grundval av dessa.

Artikel 16

Det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe)

1. EU-CyCLONe inrättas för att stödja en samordnad hantering av storskaliga cybersäkerhetsincidenter och kriser på operativ nivå och säkerställa ett regelbundet utbyte av relevant information mellan medlemsstaterna och unionens institutioner, organ och byråer.

2. EU-CyCLONe ska bestå av företrädare för medlemsstaternas myndigheter för hantering av cyberkriser samt, i fall där en potentiell eller pågående storskalig cybersäkerhetsincident har eller sannolikt kommer att ha en betydande påverkan på tjänster och verksamhet som omfattas av detta direktiv, kommissionen. I andra fall ska kommissionen delta som observatör i arbetet inom EU-CyCLONe.

Enisa ska tillhandahålla EU-CyCLONes 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 som observatörer.

3. EU-CyCLONe ska ha följande uppgifter:

a) Öka beredskapen för hantering av storskaliga cybersäkerhetsincidenter och kriser.

b) Utveckla en gemensam situationsmedvetenhet om storskaliga cybersäkerhetsincidenter och kriser.

c) Bedöma konsekvenserna och effekterna av relevanta storskaliga cybersäkerhetsincidenter och kriser och föreslå möjliga begränsningsåtgärder.

d) Samordna hanteringen av storskaliga cybersäkerhetsincidenter och kriser och ge stöd till beslutsfattande på politisk nivå i samband med sådana incidenter och kriser.

e) På begäran av en berörd medlemsstat, diskutera de nationella planer för hantering av storskaliga nationella cybersäkerhetsincidenter och kriser som avses i artikel 9.4.

4. EU-CyCLONe ska anta sin arbetsordning.

5. EU-CyCLONe ska regelbundet rapportera till samarbetsgruppen om hanteringen av storskaliga cybersäkerhetsincidenter och kriser, samt om trender, med särskild inriktning på deras inverkan på väsentliga och viktiga entiteter.

6. EU-CyCLONe ska samarbeta med CSIRT-nätverket på grundval av överenskomna förfaranden i enlighet med artikel 15.6.

7. Senast den 17 juli 2024 och därefter var 18:e månad ska EU-CyCLONe lägga fram en rapport för Europaparlamentet och rådet med en bedömning av sitt arbete.

Artikel 17

Internationellt samarbete

Unionen får, när det är lämpligt, 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. Sådana avtal ska vara förenliga med unionens dataskyddslagstiftning.

Artikel 18

Rapport om cybersäkerhetssituationen i unionen

1. Enisa ska, i samarbete med kommissionen och samarbetsgruppen, vartannat år anta en rapport om cybersäkerhetssituationen i unionen samt lämna in den till och lägga fram den för Europaparlamentet. Rapporten ska, bland annat, göras tillgänglig i maskinläsbart format och innehålla följande:

a) En riskbedömning av cybersäkerheten på unionsnivå, med beaktande av cyberhotbilden.

b) En bedömning av utvecklingen av cybersäkerhetskapaciteten i den offentliga och privata sektorn i hela unionen.

c) En bedömning av den allmänna nivån av cybersäkerhetsmedvetenhet och cyberhygien bland medborgare och entiteter, inbegripet små och medelstora företag.

d) En aggregerad bedömning av resultaten av de sakkunnigbedömningar som avses i artikel 19.

e) En aggregerad bedömning av nivån på cybersäkerhetskapaciteten och cybersäkerhetsresurserna i hela unionen, inbegripet på sektorsnivå, samt av i vilken utsträckning medlemsstaternas nationella cybersäkerhetsstrategier är anpassade till varandra.

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

3. Enisa ska, i samarbete med kommissionen, samarbetsgruppen och CSIRT-nätverket, utarbeta metoderna, bland annat de relevanta variablerna, såsom kvalitativa och kvantitativa indikatorer, för den aggregerade bedömning som avses i punkt 1 e.

Artikel 19

Sakkunnigbedömningar

1. Samarbetsgruppen ska med bistånd av kommissionen och Enisa och, i relevanta fall, av CSIRT-nätverket, och senast den 17 januari 2025, fastställa metoden för och de organisatoriska aspekterna av sakkunnigbedömningar i syfte att dra lärdom av delade erfarenheter, stärka det ömsesidiga förtroendet, uppnå en hög gemensam cybersäkerhetsnivå samt stärka medlemsstaternas nödvändiga cybersäkerhetskapacitet och cybersäkerhetsriktlinjer för att genomföra detta direktiv. Deltagandet i sakkunnigbedömningar är frivilligt. Sakkunnigbedömningarna ska utföras av cybersäkerhetsexperter. Experterna för cybersäkerhet ska utses av minst två medlemsstater, andra än den medlemsstat som granskas.

Sakkunnigbedömningarna ska omfatta åtminstone ett av följande:

a) Genomförandenivån för de riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter som fastställs i artiklarna 21 och 23.

b) Kapacitetsnivån, inbegripet tillgängliga ekonomiska, tekniska och mänskliga resurser, och effektiviteten i de behöriga myndigheternas arbete.

c) CSIRT-enheternas operativa kapacitet.

d) Genomförandenivån för det ömsesidiga bistånd som avses i artikel 37.

e) Genomförandenivån för de arrangemang för informationsutbyte om cybersäkerhet som avses i artikel 29.

f) Särskilda frågor av gränsöverskridande eller sektorsövergripande karaktär.

2. Den metod som avses i punkt 1 ska innefatta objektiva, icke-diskriminerande, rättvisa och transparenta kriterier på grundval av vilka medlemsstaterna utser de cybersäkerhetsexperter som ska få utföra sakkunnigbedömningarna. Kommissionen och Enisa ska delta som observatörer i sakkunnigbedömningarna.

3. Medlemsstaterna får identifiera sådana särskilda frågor som avses i punkt 1 f, med avseende på en sakkunnigbedömning.

4. Innan en sakkunnigbedömning som avses i punkt 1 inleds ska medlemsstaterna meddela de deltagande medlemsstaterna omfattningen av sakkunnigbedömningen, inbegripet de särskilda frågor som identifierats i enlighet med punkt 3.

5. Innan sakkunnigbedömningen inleds får medlemsstaterna genomföra en självbedömning av de granskade aspekterna och tillhandahålla denna självbedömning till de utsedda experterna för cybersäkerhet. Samarbetsgruppen ska, med bistånd av kommissionen och Enisa, fastställa metoden för medlemsstaternas självbedömning.

6. Sakkunnigbedömningar ska inbegripa fysiska eller virtuella besök på plats och distansbaserade informationsutbyten. Med hänsyn till principen om gott samarbete ska den medlemsstat som är föremål för sakkunnigbedömningen förse de utsedda cybersäkerhetsexperterna med den information som krävs för bedömningen, utan att det påverkar unionsrätten eller nationell rätt om skydd av konfidentiella eller säkerhetsskyddsklassificerade uppgifter samt skyddet av väsentliga statliga funktioner, såsom nationell säkerhet. Samarbetsgruppen ska, i samarbete med kommissionen och Enisa, utarbeta lämpliga uppförandekoder till stöd för de utsedda cybersäkerhetsexperternas arbetsmetoder. All information som erhålls genom sakkunnigbedömningen får endast användas för dess ändamål. De cybersäkerhetsexperter som deltar i sakkunnigbedömningen får inte lämna ut känslig eller konfidentiell information som erhållits under sakkunnigbedömningen till någon tredje part.

7. När aspekter har varit föremål för en sakkunnigbedömning i en medlemsstat ska de inte bli föremål för ytterligare sakkunnigbedömning i den medlemsstaten under de två år som följer på slutförandet av sakkunnigbedömningen, om inte annat begärs av medlemsstaten eller beslutas efter ett förslag från samarbetsgruppen.

8. Medlemsstaterna ska säkerställa att de andra medlemsstaterna, samarbetsgruppen, kommissionen och Enisa får information om alla risker för intressekonflikter som rör utsedda cybersäkerhetsexperter innan sakkunnigbedömningen inleds. Den medlemsstat som är föremål för sakkunnigbedömningen får invända mot utnämningen av särskilda cybersäkerhetsexperter av vederbörligen motiverade skäl som meddelas den medlemsstat som utser dessa.

9. Cybersäkerhetsexperter som deltar i sakkunnigbedömningar ska utarbeta rapporter om resultat och slutsatser av dessa. De medlemsstater som är föremål för en sakkunnigbedömning får lämna synpunkter på de utkast till rapporter som berör dem och sådana synpunkter ska bifogas rapporterna. Rapporterna ska innefatta rekommendationer som möjliggör förbättringar när det gäller de aspekter som ingår i sakkunnigbedömningen. Rapporterna ska i relevanta fall överlämnas till samarbetsgruppen och CSIRT-nätverket. En medlemsstat som är föremål för sakkunnigbedömningen får besluta att offentliggöra sin rapport eller en redigerad version av den.

KAPITEL IV

ÅTGÄRDER FÖR RISKHANTERING OCH RAPPORTERINGSKRAV FÖR CYBERSÄKERHET

Artikel 20

Styrning

1. Medlemsstaterna ska säkerställa att väsentliga och viktiga entiteters ledningsorgan godkänner de riskhanteringsåtgärder för cybersäkerhet som dessa entiteter vidtar för att följa artikel 21, övervakar genomförandet av dem och kan ställas till svars för entiteternas överträdelser av den artikeln.

Tillämpningen av denna punkt påverkar inte nationell rätt när det gäller de ansvarsregler som är tillämpliga på offentliga institutioner, samt ansvaret för statligt anställda och valda eller utnämnda tjänstepersoner.

2. Medlemsstaterna ska säkerställa att medlemmarna i väsentliga och viktiga entiteters ledningsorgan är skyldiga att genomgå utbildning, och ska uppmuntra väsentliga och viktiga entiteter att regelbundet erbjuda liknande utbildning till sina anställda för att de ska få tillräckligt med kunskap och kompetens för att kunna identifiera risker och bedöma riskhanteringspraxis för cybersäkerhet och deras inverkan på de tjänster som tillhandahålls av entiteten.

Artikel 21

Riskhanteringsåtgärder för cybersäkerhet

1. Medlemsstaterna ska säkerställa att väsentliga och viktiga entiteter vidtar lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och för att förhindra eller minimera incidenters påverkan på mottagarna av deras tjänster och på andra tjänster.

Med beaktande av de senaste, och i tillämpliga fall, relevanta europeiska och internationella standarder samt genomförandekostnaderna, ska de åtgärder som avses i första stycket säkerställa en nivå på säkerheten i nätverks- och informationssystem som är lämplig i förhållande till den föreliggande risken. Vid bedömningen av dessa åtgärders proportionalitet ska vederbörlig hänsyn tas till entitetens grad av riskexponering, entitetens storlek samt sannolikheten för att incidenter inträffar och deras allvarlighetsgrad, inbegripet deras samhälleliga och ekonomiska konsekvenser.

2. De åtgärder som avses i punkt 1 ska baseras på en allriskansats som syftar till att skydda nätverks- och informationssystem och dessa systems fysiska miljö från incidenter, och ska minst inbegripa

a) strategier för riskanalys och informationssystemens säkerhet,

b) incidenthantering,

c) driftskontinuitet, exempelvis hantering av säkerhetskopiering och katastrofhantering, och krishantering,

d) säkerhet i leveranskedjan, inbegripet säkerhetsaspekter som rör förbindelserna mellan varje entitet och dess direkta leverantörer eller tjänsteleverantörer,

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

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

g) grundläggande praxis för cyberhygien och utbildning i cybersäkerhet,

h) strategier och förfaranden för användning av kryptografi och, när så är lämpligt, kryptering,

i) personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning,

j) användning inom entiteten, när så är lämpligt, av lösningar för multifaktorautentisering eller kontinuerlig autentisering, säkrade röst-, video- och textkommunikationer och säkrade nödkommunikationssystem.

3. Medlemsstaterna ska säkerställa att entiteter, när de överväger lämpliga åtgärder enligt punkt 2 d i denna artikel, beaktar de sårbarheter som är specifika för varje direktleverantör 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 entiteter, när de överväger lämpliga åtgärder enligt den punkten är skyldiga att beakta resultatet av de samordnade säkerhetsriskbedömningar av kritiska leveranskedjor som utförs i enlighet med artikel 22.1.

4. Medlemsstaterna ska säkerställa att en entitet som finner att den inte följer de åtgärder som föreskrivs i punkt 2 utan onödigt dröjsmål vidtar alla nödvändiga, lämpliga och proportionella korrigerande åtgärder.

5. Senast den 17 oktober 2024 ska kommissionen anta genomförandeakter för att fastställa de tekniska och metodologiska specifikationerna för de åtgärder som avses i punkt 2 med avseende på leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster, leverantörer av marknadsplatser online, sökmotorer och för plattformar för sociala nätverkstjänster samt kvalificerade tillhandahållare av betrodda tjänster.

Kommissionen får anta genomförandeakter för att fastställa tekniska och metodologiska krav samt, vid behov, sektorskrav för de åtgärder som avses i punkt 2 med avseende på andra väsentliga och viktiga entiteter än de som avses i första stycket i denna punkt.

När kommissionen utarbetar de genomförandeakter som avses i första och andra stycket i denna punkt ska den i största möjliga utsträckning följa europeiska och internationella standarder samt relevanta tekniska specifikationer. Kommissionen ska utbyta råd och samarbeta med samarbetsgruppen och Enisa om de utkast till genomförandeakter som avses i artikel 14.4 e.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2.

Artikel 22

Samordnade säkerhetsriskbedömningar på unionsnivå 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 och, vid behov, relevanta intressenter, identifiera de specifika kritiska IKT-tjänster, IKT-system eller IKT-produkter som kan bli föremål för den samordnade säkerhetsriskbedömning som avses i punkt 1.

Artikel 23

Rapporteringsskyldigheter

1. Varje medlemsstat ska säkerställa att väsentliga och viktiga entiteter utan onödigt dröjsmål underrättar sin CSIRT-enhet eller, i tillämpliga fall, sin behöriga myndighet i enlighet med punkt 4 om alla incidenter som har en betydande inverkan på tillhandahållandet av deras tjänster enligt punkt 3 (betydande incident). När så är lämpligt ska berörda entiteter utan onödigt dröjsmål underrätta mottagarna av deras tjänster om betydande incidenter som sannolikt inverkar negativt på tillhandahållandet av de tjänsterna. Varje medlemsstat ska säkerställa att dessa entiteter bland annat rapporterar information som gör det möjligt för CSIRT-enheten eller, i tillämpliga fall, den behöriga myndigheten att fastställa incidentens eventuella gränsöverskridande verkningar. Själva underrättelsen ska inte medföra ökat ansvar för den underrättande entiteten.

Om de berörda entiteterna underrättar den behöriga myndigheten om en betydande incident enligt första stycket ska medlemsstaten säkerställa att den behöriga myndigheten vidarebefordrar underrättelsen till CSIRT-enheten vid mottagandet.

Vid en gränsöverskridande eller sektorsövergripande betydande incident ska medlemsstaterna säkerställa att deras gemensamma kontaktpunkter i god tid förses med relevant information som meddelats i enlighet med punkt 4.

2. I tillämpliga fall ska medlemsstaterna säkerställa att väsentliga och viktiga entiteter utan onödigt dröjsmål underrättar 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 informera dessa mottagare om själva det betydande cyberhotet.

3. En incident ska anses vara betydande om

a) den har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller ekonomiska förluster för den berörda entiteten,

b) den har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiell eller immateriell skada.

4. När det gäller det underrättelseförfarande som avses i punkt 1 ska medlemsstaterna säkerställa att de berörda entiteterna lämnar följande till CSIRT-enheten eller, i tillämpliga fall, den behöriga myndigheten:

a) Utan onödigt dröjsmål och under alla omständigheter inom 24 timmar efter att ha fått kännedom om den betydande incidenten, en tidig varning som i tillämpliga fall ska ange om den betydande incidenten misstänks ha orsakats av olagliga eller avsiktligt skadliga handlingar eller kan ha gränsöverskridande verkningar.

b) Utan onödigt dröjsmål och under alla omständigheter inom 72 timmar efter att ha fått kännedom om den betydande incidenten, en incidentanmälan som, i tillämpliga fall, ska uppdatera den information som avses i led a och ange en inledande bedömning av den betydande incidenten, dess allvarlighetsgrad och konsekvenser samt, i förekommande fall, angreppsindikatorer.

c) På begäran av en CSIRT-enhet eller, i tillämpliga fall, den behöriga myndigheten, en delrapport om relevanta statusuppdateringar.

d) Senast en månad efter inlämningen av den incidentanmälan som avses i led b, en slutrapport som ska innehålla följande:

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

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

   iii) Tillämpade och pågående begränsande åtgärder.

   iv) I tillämpliga fall, incidentens gränsöverskridande verkningar.

e) I händelse av en pågående incident vid tidpunkten för inlämnandet av den slutrapport som avses i led d ska medlemsstaterna säkerställa att de berörda entiteterna tillhandahåller en lägesrapport vid den tidpunkten och en slutrapport inom en månad efter det att de hanterat incidenten.

Genom undantag från första stycket b ska en tillhandahållare av betrodda tjänster, när det gäller betydande incidenter som påverkar tillhandahållandet av de betrodda tjänsterna, utan onödigt dröjsmål och under alla omständigheter inom 24 timmar efter att ha fått kännedom om den betydande incidenten, underrätta CSIRT-enheten eller, i tillämpliga fall, den behöriga myndigheten.

5. CSIRT-enheten eller den behöriga myndigheten ska utan onödigt dröjsmål och om möjligt inom 24 timmar från mottagandet av den tidiga varning som avses i punkt 4 a lämna ett svar till den underrättande entiteten, inbegripet initial återkoppling om den betydande incidenten och, på entitetens begäran, vägledning eller operativa råd om genomförandet av möjliga begränsande åtgärder. Om CSIRT-enheten inte är den ursprungliga mottagaren av den underrättelse 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 den betydande incidenten misstänks vara av brottslig art ska CSIRT-enheten eller den behöriga myndigheten också tillhandahålla vägledning om rapporteringen av den betydande incidenten till de brottsbekämpande myndigheterna.

6. När så är lämpligt, och särskilt om den betydande incidenten berör två eller flera medlemsstater, ska CSIRT-enheten, den behöriga myndigheten eller den gemensamma kontaktpunkten utan onödigt dröjsmål informera andra berörda medlemsstater och Enisa om den betydande incidenten. Sådan information ska åtminstone inbegripa den typ av information som mottagits i enlighet med punkt 4. Därvid ska CSIRT-enheten, den behöriga myndigheten eller den gemensamma kontaktpunkten, i enlighet med unionsrätten eller nationell rätt, bevara entitetens säkerhets- och affärsintressen samt den tillhandahållna informationens konfidentialitet.

7. Om allmänhetens medvetenhet är nödvändig för att förhindra en betydande incident eller för att hantera en pågående betydande incident, eller om information om den betydande incidenten på annat sätt ligger i allmänhetens intresse, får en medlemsstats CSIRT-enhet eller, i tillämpliga fall, dess behöriga myndighet och, om det är lämpligt, CSIRT-enheterna eller de behöriga myndigheterna i andra berörda medlemsstater, efter samråd med den berörda entiteten, informera allmänheten om den betydande incidenten eller ålägga entiteten att göra detta.

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

9. Den gemensamma kontaktpunkten ska var tredje månad lämna in en sammanfattande rapport till Enisa med anonymiserade och aggregerade uppgifter om betydande incidenter, incidenter, cyberhot och tillbud om vilket underrättats i enlighet med punkt 1 i denna artikel och med artikel 30. För att bidra till att jämförbar information lämnas får Enisa anta teknisk vägledning om parametrarna för den information som ska tas med i den sammanfattande rapporten. Enisa ska var sjätte månad informera samarbetsgruppen och CSIRT-nätverket om sina slutsatser om de mottagna anmälningarna.

10. CSIRT-enheterna eller, i tillämpliga fall, de behöriga myndigheterna ska förse de behöriga myndigheterna enligt direktiv (EU) 2022/2557 med information om betydande incidenter, incidenter, cyberhot och tillbud om vilket underrättats i enlighet med punkt 1 i denna artikel och med artikel 30 av entiteter som identifierats som kritiska i enlighet med direktiv (EU) 2022/2557.

11. Kommissionen får anta genomförandeakter som närmare anger typen av information i och formatet och förfarandet för underrättelser som lämnas i enlighet med punkt 1 i denna artikel och med artikel 30 samt för underrättelser som lämnas i enlighet med punkt 2 i den här artikeln.

Senast den 17 oktober 2024 ska kommissionen, med avseende på leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster samt leverantörer av marknadsplatser online, sökmotorer eller av plattformar för sociala nätverkstjänster, anta genomförandeakter som närmare anger i vilka fall en incident ska anses vara betydande enligt punkt 3. Kommissionen får anta sådana genomförandeakter med avseende på andra väsentliga och viktiga entiteter.

Kommissionen ska utbyta råd och samarbeta med samarbetsgruppen om de utkast till genomförandeakter som avses i första och andra stycket i denna punkt i enlighet med artikel 14.4 e.

Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 39.2.

Artikel 24

Användning av europeiska ordningar för cybersäkerhetscertifiering

1. För att visa att vissa krav enligt artikel 21 är uppfyllda får medlemsstaterna ålägga väsentliga och viktiga entiteter att använda särskilda IKT-produkter, IKT-tjänster och IKT-processer, som har utvecklats av den väsentliga eller viktiga entiteten eller upphandlats från tredje parter, som är certifierade enligt europeiska ordningar för cybersäkerhetscertifiering som antagits i enlighet med artikel 49 i förordning (EU) 2019/881. Medlemsstaterna ska dessutom uppmuntra väsentliga och viktiga entiteter att använda kvalificerade betrodda tjänster.

2. Kommissionen ges befogenhet att anta delegerade akter i enlighet med artikel 38 för att komplettera detta direktiv genom att ange 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 enligt en europeisk ordning för cybersäkerhetscertifiering som har antagits enligt artikel 49 i förordning (EU) 2019/881. Dessa delegerade akter ska antas om det har fastställts att cybersäkerhetsnivån är otillräcklig och ska omfatta en genomförandeperiod.

Innan kommissionen antar sådana delegerade akter ska den göra en konsekvensbedömning och genomföra samråd i enlighet med artikel 56 i förordning (EU) 2019/881.

3. I fall där det inte finns en lämplig europeisk ordning för cybersäkerhetscertifiering med avseende på tillämpningen av punkt 2 i denna artikel kan kommissionen, efter samråd med samarbetsgruppen och europeiska gruppen för cybersäkerhetscertifiering, begära att Enisa utarbetar ett förslag till certifieringsordning enligt artikel 48.2 i förordning (EU) 2019/881.

Artikel 25

Standardisering

1. För att främja en enhetlig tillämpning av artikel 21.1 och 21.2 ska medlemsstaterna, utan att föreskriva eller gynna användning av en viss typ av teknik, uppmuntra användningen av europeiska och internationella standarder och tekniska specifikationer av relevans för säkerheten i nätverks- och informationssystem.

2. Enisa ska i samarbete med medlemsstaterna och, när så är lämpligt, efter samråd med relevanta intressenter, utarbeta råd och riktlinjer för de tekniska områden som ska beaktas när det gäller punkt 1 samt för redan befintliga standarder, inklusive nationella standarder, som skulle göra det möjligt att täcka dessa områden.

KAPITEL V

JURISDIKTION OCH REGISTRERING

Artikel 26

Jurisdiktion och territorialitet

1. Entiteter som omfattas av detta direktivs tillämpningsområde ska anses omfattas av jurisdiktionen i den medlemsstat där de är etablerade, utom när det gäller följande:

a) Tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster, som ska anses omfattas av jurisdiktionen i den medlemsstat där de tillhandahåller sina tjänster.

b) Leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, entiteter som tillhandahåller domännamnsregistreringstjänster, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av hanterade tjänster och leverantörer av hanterade säkerhetstjänster samt leverantörer av marknadsplatser online, sökmotorer eller plattformar för sociala nätverkstjänster, vilka ska anses omfattas av jurisdiktionen i den medlemsstat där de har sitt huvudsakliga etableringsställe i unionen i enlighet med punkt 2.

c) Offentliga förvaltningsentiteter, som ska anses omfattas av jurisdiktionen i den medlemsstat som inrättade dem.

2. Vid tillämpning av detta direktiv ska en entitet som avses i punkt 1 b anses ha sitt huvudsakliga etableringsställe i unionen i den medlemsstat där besluten om riskhanteringsåtgärder för cybersäkerhet i huvudsak fattas. Om en sådan medlemsstat inte kan fastställas eller om sådana beslut inte fattas i unionen ska det huvudsakliga etableringsstället anses vara beläget i den medlemsstat där cybersäkerhetsoperationer utförs. Om en sådan medlemsstat inte kan fastställas ska det huvudsakliga etableringsstället anses vara beläget i den medlemsstat där den berörda entiteten har det etableringsställe som har flest anställda i unionen.

3. Om en entitet som avses i punkt 1 b 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 en utsedd företrädare i unionen enligt denna punkt får varje medlemsstat där entiteten tillhandahåller tjänster vidta rättsliga åtgärder mot entiteten för överträdelsen av detta direktiv.

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

5. De medlemsstater som har mottagit en begäran om ömsesidigt bistånd med avseende på en entitet som avses i punkt 1 b får, inom ramen för den 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 27

Register över entiteter

1. Enisa ska skapa och upprätthålla ett register över leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, entiteter som tillhandahåller domännamnsregistreringstjänster, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leveransleverans av innehåll, leverantörer av hanterade tjänster, leverantörer av hanterade säkerhetstjänster samt leverantörer av internetbaserade marknadsplatser online, internetbaserade sökmotorer och plattformar för sociala nätverkstjänster, på grundval av den information som mottagits från de gemensamma kontaktpunkterna i enlighet med punkt 4. Enisa ska på begäran ge de behöriga myndigheterna tillgång till detta register, samtidigt som skydd av informationens konfidentialitet säkerställs i tillämpliga fall.

2. Medlemsstaterna ska ålägga de entiteter som avses i punkt 1 att lämna följande uppgifter till de behöriga myndigheterna senast den 17 januari 2025:

a) Entitetens namn.

b) Den relevanta sektorn och delsektorn samt typen av entitet enligt bilaga I eller II i tillämpliga fall.

c) 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 26.3.

d) Aktuella kontaktuppgifter, inklusive e-postadresser och telefonnummer till entiteten och, i tillämpliga fall, till dess företrädare som utsetts i enlighet med artikel 26.3.

e) De medlemsstater där entiteten tillhandahåller tjänster.

f) Entitetens IP-adressintervall.

3. Medlemsstaterna ska säkerställa att de entiteter som avses i punkt 1 underrättar den behöriga myndigheten om alla ändringar av de uppgifter som de lämnat enligt punkt 2 utan dröjsmål och under alla omständigheter inom tre månader från dagen för ändringen.

4. När den gemensamma kontaktpunkten i den berörda medlemsstaten mottagit den information som avses i punkterna 2 och 3, med undantag för den information som avses i punkt 2 f, ska den utan dröjsmål vidarebefordra den informationen till Enisa.

5. Den information som avses i punkterna 2 och 3 i denna artikel ska, i tillämpliga fall, lämnas genom den nationella mekanism som avses i artikel 3.4 fjärde stycket.

Artikel 28

Databas över domännamnsregistreringsuppgifter

1. För att bidra till domännamnssystemets säkerhet, stabilitet och motståndskraft ska medlemsstaterna ålägga registreringsenheter för toppdomäner och de enheter som tillhandahåller domännamnsregistreringstjänster att samla in och upprätthålla korrekta och fullständiga registreringsuppgifter för domännamn i en särskild databas med tillbörlig aktsamhet i enlighet med unionens dataskyddslagstiftning när det gäller personuppgifter.

2. För tillämpningen av punkt 1 ska medlemsstaterna föreskriva att databasen med registreringsuppgifter för domännamn innehåller nödvändig information för att identifiera och kontakta innehavarna av domännamnen och de kontaktpunkter som administrerar domännamnen under toppdomänerna. Denna information ska omfatta följande:

a) Domännamn.

b) Registreringsdatum.

c) Registrantens namn, e-postadress och telefonnummer.

d) E-postadress och telefonnummer till den kontaktpunkt som administrerar domännamnet om dessa inte är desamma som för registranten.

3. Medlemsstaterna ska ålägga registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att ha strategier och förfaranden, inbegripet kontrollförfaranden, för att säkerställa att de databaser som avses i punkt 1 innehåller korrekt och fullständig information. Medlemsstaterna ska föreskriva att sådana strategier och förfaranden offentliggörs.

4. Medlemsstaterna ska ålägga registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att utan onödigt dröjsmål efter registreringen av ett domännamn offentliggöra registreringsuppgifter för domännamn som inte är personuppgifter.

5. Medlemsstaterna ska ålägga registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att ge åtkomst till specifika registreringsuppgifter för domännamn på lagliga och vederbörligen motiverade begäranden från legitima åtkomstsökande, i enlighet med unionens dataskyddslagstiftning. Medlemsstaterna ska ålägga registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att utan onödigt dröjsmål och under alla omständigheter inom 72 timmar från mottagandet besvarar en begäran om åtkomst. Medlemsstaterna ska föreskriva att strategier och förfaranden för utlämning av sådana uppgifter offentliggörs.

6. Fullgörandet av de skyldigheter som fastställs i punkterna 1–5 får inte leda till dubblerad insamling av registreringsuppgifter för domännamn. I detta syfte ska medlemsstaterna ålägga registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster att samarbeta med varandra.

KAPITEL VI

INFORMATIONSUTBYTE

Artikel 29

Arrangemang för informationsutbyte om cybersäkerhet

1. Medlemsstaterna ska säkerställa att entiteter som omfattas av tillämpningsområdet för detta direktiv och, i relevanta fall, andra relevanta entiteter som inte omfattas av detta direktivs tillämpningsområde på frivillig basis har möjlighet att utbyta relevant information om cybersäkerhet sinsemellan, inbegripet information om cyberhot, tillbud, sårbarheter, tekniker och förfaranden, angreppsindikatorer, fientlig taktik, specifik information om fientliga aktörer, cybersäkerhetsvarningar och rekommendationer avseende konfigurationsverktyg för cybersäkerhet för att upptäcka cyberattacker, om sådant informationsutbyte

a) syftar till att förebygga, upptäcka, reagera på eller återhämta sig från incidenter eller begränsa deras inverkan,

b) höjer cybersäkerhetsnivån, särskilt genom att öka medvetenheten om cyberhot, begränsa eller hindra sådana hots förmåga att sprida sig, stödja en rad defensiva förmågor, avhjälpande av sårbarheter och delgivning av information om sårbarheter, metoder för att upptäcka och förebygga hot, strategier för begränsning av hot eller reaktions- och återhämtningsfaser, eller genom att främja forskningssamverkan om cyberhot bland offentliga och privata entiteter.

2. Medlemsstaterna ska säkerställa att informationsutbytet sker inom grupper av väsentliga och viktiga entiteter, och i relevanta fall, deras leverantörer eller tjänsteleverantörer. Sådant utbyte ska genomföras med hjälp av arrangemang för informationsutbyte om cybersäkerhet med hänsyn till den potentiellt känsliga karaktären hos den information som utbyts.

3. Medlemsstaterna ska underlätta inrättandet av de arrangemang för informationsutbyte om cybersäkerhet som avses i punkt 2 i denna artikel. Sådana arrangemang får ange operativa aspekter, inbegripet användning av särskilda IKT-plattformar och automatiseringsverktyg, innehållet i och villkoren för de arrangemangen för informationsutbyte. Medlemsstaterna får, i samband med fastställandet av närmare bestämmelser om offentliga myndigheters deltagande i sådana arrangemang, införa villkor för den information som tillgängliggörs av behöriga myndigheter eller CSIRT-enheter. Medlemsstaterna ska erbjuda stöd för tillämpningen av sådana arrangemang i enlighet med de riktlinjer som avses i artikel 7.2 h.

4. Medlemsstaterna ska säkerställa att väsentliga och viktiga entiteter underrättar de behöriga myndigheterna om sitt deltagande i de arrangemang för informationsutbyte om cybersäkerhet som avses i punkt 2, när de ingår sådana arrangemang eller, om de utträder ur sådana arrangemang, när utträdet får verkan.

5. Enisa ska tillhandahålla stöd för inrättandet av de arrangemang för informationsutbyte om cybersäkerhet som avses i punkt 2 genom att utbyta bästa praxis och erbjuda vägledning.

Artikel 30

Frivillig underrättelse om relevant information

1. Medlemsstaterna ska säkerställa att underrättelser, utöver den underrättelseskyldighet som föreskrivs i artikel 23, kan lämnas in till CSIRT-enheterna eller, i tillämpliga fall, de behöriga myndigheterna, på frivillig basis av

a) väsentliga och viktiga entiteter med avseende på incidenter, cyberhot och tillbud,

b) andra entiteter än de som avses i led a, oberoende av om de omfattas av detta direktiv, vad gäller om betydande incidenter, cyberhot och tillbud.

2. Medlemsstaterna ska behandla de underrättelser som avses i punkt 1 i denna artikel i enlighet med det förfarande som anges i artikel 23. Medlemsstaterna får ge behandling av obligatoriska underrättelser företräde framför behandling av frivilliga underrättelser.

CSIRT-enheterna, och i tillämpliga fall, de behöriga myndigheterna ska vid behov informera de gemensamma kontaktpunkterna om underrättelser som mottagits i enlighet med denna artikel, och samtidigt säkerställa att informationen från den underrättande entiteten förblir konfidentiell och skyddas på lämpligt sätt. Utan att det påverkar förebyggande, utredning, avslöjande och lagföring av brott får frivillig rapportering inte leda till att den underrättande entiteten åläggs ytterligare skyldigheter som den inte skulle ha blivit föremål för om den inte hade lämnat in underrättelsen.

KAPITEL VII

TILLSYN OCH EFTERLEVNADSKONTROLL

Artikel 31

Allmänna aspekter på tillsyn och efterlevnadskontroll

1. Medlemsstaterna ska säkerställa att deras behöriga myndigheter på ett ändamålsenligt sätt övervakar och vidtar de åtgärder som krävs för att säkerställa att detta direktiv efterlevs.

2. Medlemsstaterna får tillåta sina behöriga myndigheter att prioritera tillsyn. Denna prioritering ska baseras på en riskbaserad metod. När de behöriga myndigheterna utövar sina tillsynsuppgifter enligt artiklarna 32 och 33 får de i detta syfte fastställa tillsynsmetoder som gör det möjligt att prioritera sådana uppgifter enligt en riskbaserad metod.

3. De behöriga myndigheterna ska ha ett nära samarbete med tillsynsmyndigheterna enligt förordning (EU) 2016/679 när de behandlar incidenter som medför personuppgiftsincidenter, utan att det påverkar tillsynsmyndigheternas befogenheter och uppgifter enligt den förordningen.

4. 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 införandet av efterlevnadskontrollåtgärder vid överträdelser av detta direktiv, har lämpliga befogenheter att utföra dessa uppgifter och är operativt oberoende i förhållande till de offentliga förvaltningsentiteter som övervakas. Medlemsstaterna får besluta att införa lämpliga, proportionella och effektiva tillsyns- och efterlevnadskontrollåtgärder med avseende på dessa entiteter i enlighet med de nationella rättsliga och institutionella ramarna.

Artikel 32

Tillsyns- och efterlevnadskontrollåtgärder 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 behöriga myndigheter, när de utövar sina tillsynsuppgifter avseende väsentliga entiteter, har befogenhet att åtminstone underställa dessa entiteter

a) inspektioner på plats och distansbaserad tillsyn, inklusive slumpvisa kontroller som utförs av utbildad personal,

b) regelbundna och riktade säkerhetsrevisioner som utförs av ett oberoende organ eller en behörig myndighet,

c) ad hoc-revisioner, inbegripet när detta är motiverat på grund av en betydande incident eller av en väsentlig entitets överträdelse av detta direktiv,

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

e) begäranden om sådan information som behövs för att bedöma de riskhanteringsåtgärder för cybersäkerhet som antagits av den berörda entiteten, inbegripet dokumenterade cybersäkerhetsstrategier, samt fullgörandet av skyldigheten att lämna information till de behöriga myndigheterna i enlighet med artikel 27,

f) begäranden om tillgång till uppgifter, handlingar och 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.

De riktade säkerhetsrevisioner som avses i första stycket led b ska baseras på riskbedömningar som utförs av den behöriga myndigheten eller den granskade entiteten, eller på annan tillgänglig riskrelaterad information.

Resultaten av alla riktade säkerhetsrevisioner ska göras tillgängliga för den behöriga myndigheten. Kostnaderna för sådana riktade säkerhetsrevisioner som utförs av ett oberoende organ ska betalas av den granskade entiteten, utom i vederbörligen motiverade fall när den behöriga myndigheten beslutar något annat.

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

4. Medlemsstaterna ska säkerställa att deras behöriga myndigheter, när de utövar sina befogenheter med avseende på efterlevnadskontroll gentemot väsentliga entiteter, åtminstone har befogenhet att

a) utfärda varningar om berörda entiteters överträdelser av detta direktiv,

b) anta bindande instruktioner, också om vilka åtgärder som krävs för att förebygga eller avhjälpa en incident, samt tidsgränser för genomförandet av sådana åtgärder och för rapporteringen om deras genomförande, eller ett föreläggande om att de berörda entiteterna ska avhjälpa konstaterade brister eller överträdelser av detta direktiv,

c) ålägga de berörda entiteterna att upphöra med beteenden som utgör en överträdelse av detta direktiv och att avstå från att upprepa sådana beteenden,

d) ålägga de berörda entiteterna att säkerställa att deras riskhanteringsåtgärder för cybersäkerhet överensstämmer med artikel 21 eller att fullgöra de rapporteringsskyldigheter som fastställs i artikel 23, på ett specificerat sätt och inom en angiven tidsperiod,

e) ålägga de berörda entiteterna att informera de fysiska eller juridiska personer till vilka de tillhandahåller tjänster eller utför 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 de berörda entiteterna att inom en rimlig tidsfrist genomföra de rekommendationer som lämnats till följd av en säkerhetsrevision,

g) utse en övervakningsansvarig med väldefinierade uppgifter för en fastställd tidsperiod för att övervaka att de berörda entiteterna efterlever artiklarna 21 och 23,

h) ålägga de berörda entiteterna att offentliggöra aspekter av överträdelser av detta direktiv på ett specificerat sätt,

i) påföra eller begära att relevanta organ eller domstolar i enlighet med nationell rätt påför administrativa sanktionsavgifter enligt artikel 34 utöver någon av de åtgärder som avses i leden a–h i denna punkt.

5. Om efterlevnadskontrollåtgärder som antas enligt punkt 4 a–d och f är ineffektiva ska medlemsstaterna säkerställa att deras behöriga myndigheter har befogenhet att fastställa en tidsfrist inom vilken en väsentlig entitet ska vidta nödvändiga åtgärder för att avhjälpa bristerna eller uppfylla 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 en domstol, i enlighet med nationell rätt, tillfälligt upphäver en certifiering eller auktorisation för en del av eller alla relevanta tjänster som tillhandahålls eller verksamheter som utövas av den väsentliga entiteten,

b) begära att relevanta organ eller domstolar, i enlighet med nationell rätt, inför ett tillfälligt förbud för varje fysisk person som på nivån för verkställande direktör eller juridiskt ombud har ledningsansvar i den väsentliga entiteten att utöva ledningsfunktioner i den entiteten.

Tillfälliga upphävanden eller förbud i enlighet med denna punkt ska tillämpas endast till dess att den berörda entiteten vidtar nödvändiga åtgärder för att avhjälpa bristerna eller uppfylla de krav från den behöriga myndigheten som gav upphov till sådana efterlevnadskontrollåtgärder. Sådana tillfälliga upphävanden eller förbud får komma i fråga endast om lämpliga rättssäkerhetsgarantier i enlighet med de allmänna principerna i unionsrätten och stadgan iakttas, inbegripet rätten till ett effektivt rättsmedel och en rättvis rättegång, oskuldspresumtion och rätten till försvar.

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

6. Medlemsstaterna ska säkerställa att varje fysisk person som ansvarar för eller agerar som juridiskt ombud för en väsentlig entitet har befogenhet att säkerställa att entiteten efterlever detta direktiv, på grundval av en befogenhet att företräda entiteten, att fatta beslut på dess vägnar eller att utöva kontroll över entiteten. Medlemsstaterna ska säkerställa att dessa fysiska personer kan hållas ansvariga för överträdelser av sitt uppdrag att säkerställa att detta direktiv efterlevs.

När det gäller offentliga förvaltningsentiteter påverkar inte denna punkt nationell rätt avseende det ansvar som åligger statligt anställda och valda eller utnämnda tjänstepersoner.

7. När de behöriga myndigheterna tillämpar efterlevnadskontrollåtgärder som avses i punkt 4 eller 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) Överträdelsens allvar och betydelsen av de bestämmelser som har överträtts, med beaktande av att bland annat följande alltid ska anses vara en allvarlig överträdelse:

   i) Upprepade överträdelser.

   ii) Underlåtenhet att underrätta om eller avhjälpa betydande incidenter.

   iii) Underlåtenhet att avhjälpa brister enligt bindande instruktioner från behöriga myndigheter.

   iv) Hindrande av revisioner eller övervakningsverksamhet som den behöriga myndigheten beordrat efter det att en överträdelse konstaterats.

   v) Tillhandahållande av falsk eller grovt felaktig information i fråga om riskhanteringsåtgärder för cybersäkerhet eller rapporteringsskyldigheter enligt artiklarna 21 och 23.

b) Överträdelsens varaktighet.

c) Eventuella tidigare relevanta överträdelser från den berörda entitetens sida.

d) Den materiella eller immateriella skada som uppstått, inbegripet finansiella eller ekonomiska förluster, effekter på andra tjänster och det antal användare som berörs.

e) Uppsåt eller oaktsamhet från den som har gjort sig skyldig till överträdelsen.

f) De åtgärder som entiteten har vidtagit för att förhindra eller begränsa den materiella eller immateriella skadan.

g) Efterlevnad av godkända uppförandekoder eller godkända certifieringsmekanismer.

h) I vilken utsträckning de fysiska eller juridiska personer som hålls ansvariga samarbetar med de behöriga myndigheterna.

8. De behöriga myndigheterna ska utförligt motivera sina efterlevnadskontrollåtgärder. Innan sådana åtgärder antas ska de behöriga myndigheterna underrätta de berörda entiteterna om sina preliminära slutsatser. De ska också ge dessa entiteter en rimlig tidsfrist för att lämna synpunkter, utom i vederbörligen motiverade fall där omedelbara åtgärder för att förhindra eller reagera på incidenter annars skulle hindras.

9. Medlemsstaterna ska säkerställa att deras behöriga myndigheter enligt detta direktiv informerar de relevanta behöriga myndigheterna inom samma medlemsstat i enlighet med direktiv (EU) 2022/2557 när de utövar sina befogenheter med avseende på tillsyn och efterlevnadskontroll för att säkerställa att en entitet som identifierats som en kritisk entitet i enlighet med direktiv (EU) 2022/2557 efterlever detta direktiv. När så är lämpligt får behöriga myndigheter enligt direktiv (EU) 2022/2557 begära att behöriga myndigheter enligt detta direktiv utövar sina befogenheter med avseende på tillsyn och efterlevnadskontroll gentemot en entitet som identifieras som en kritisk entitet i enlighet med direktiv (EU) 2022/2557.

10. Medlemsstaterna ska säkerställa att deras behöriga myndigheter enligt detta direktiv samarbetar med de relevanta behöriga myndigheterna i den berörda medlemsstaten enligt förordning (EU) 2022/2554. Medlemsstaterna ska särskilt säkerställa att deras behöriga myndigheter enligt detta direktiv informerar det tillsynsforum som inrättats enligt artikel 32.1 i förordning (EU) 2022/2554 när de utövar sina befogenheter med avseende på tillsyn och efterlevnadskontroll för att säkerställa att en väsentlig entitet som har identifierats som en kritisk tredjepartsleverantör av IKT-tjänster enligt artikel 31 i förordning (EU) 2022/2554 efterlever detta direktiv.

Artikel 33

Tillsyns- och efterlevnadskontrollåtgärder i fråga om viktiga entiteter

1. När medlemsstaterna får bevis, indikationer på eller information om att en viktig entitet påstås underlåta att fullgöra detta direktiv, särskilt artiklarna 21 och 23, ska de säkerställa att de behöriga myndigheterna vid behov vidtar åtgärder i form av tillsynsåtgärder i efterhand. Medlemsstaterna ska säkerställa att dessa åtgärder 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 viktiga entiteter, har befogenhet att åtminstone underställa dessa entiteter

a) inspektioner på plats och distansbaserad tillsyn i efterhand, som utförs av utbildad personal,

b) riktade säkerhetsrevisioner utförda av ett oberoende organ eller en behörig myndighet,

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

d) begäranden om information som behövs för att i efterhand bedöma de riskhanteringsåtgärder för cybersäkerhet som antagits av den berörda entiteten, inbegripet dokumenterade cybersäkerhetsstrategier, samt fullgörandet av skyldigheten att lämna information till de behöriga myndigheterna i enlighet med artikel 27,

e) begäranden om tillgång till uppgifter, handlingar och information som behövs för att utföra sina tillsynsuppgifter,

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

De riktade säkerhetsrevisioner som avses i första stycket led b ska baseras på riskbedömningar som utförs av den behöriga myndigheten eller den granskade entiteten, eller på annan tillgänglig riskrelaterad information.

Resultaten av alla riktade säkerhetsrevisioner ska göras tillgängliga för den behöriga myndigheten. Kostnaderna för sådana riktade säkerhetsrevisioner som utförs av ett oberoende organ ska betalas av den granskade entiteten, utom i vederbörligen motiverade fall när den behöriga myndigheten beslutar något annat.

3. När de behöriga myndigheterna utövar sina befogenheter enligt punkt 2 d, e eller f ska de ange syftet med en begäran och specificera den begärda informationen.

4. Medlemsstaterna ska säkerställa att de behöriga myndigheterna, när de utövar sina befogenheter med avseende på efterlevnadskontroll gentemot viktiga entiteter åtminstone har befogenhet att

a) utfärda varningar om de berörda entiteternas överträdelser av detta direktiv,

b) anta bindande instruktioner eller ett föreläggande om att de berörda entiteterna ska avhjälpa konstaterade brister eller överträdelser av detta direktiv,

c) ålägga de berörda entiteterna att upphöra med beteenden som utgör en överträdelse av detta direktiv och att avstå från att upprepa sådana beteenden,

d) ålägga de berörda entiteterna att säkerställa att deras riskhanteringsåtgärder för cybersäkerhet överensstämmer med artikel 21 eller att fullgöra de rapporteringsskyldigheter som fastställs i artikel 23, på ett specificerat sätt och inom en angiven tidsperiod,

e) ålägga de berörda entiteterna att informera de fysiska eller juridiska personer till vilka de tillhandahåller tjänster eller utför 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 de berörda entiteterna att inom en rimlig tidsfrist genomföra de rekommendationer som lämnats till följd av en säkerhetsrevision,

g) ålägga de berörda entiteterna att offentliggöra aspekter av överträdelser av detta direktiv på ett specificerat sätt,

h) påföra eller begära att relevanta organ eller domstolar i enlighet med nationell rätt påför administrativa sanktionsavgifter enligt artikel 34 utöver någon av de åtgärder som avses i leden a–g i denna punkt.

5. Artikel 32.6, 32.7 och 32.8 ska i tillämpliga delar tillämpas på de tillsyns- och efterlevnadskontrollåtgärder som föreskrivs i denna artikel för viktiga entiteter.

6. Medlemsstaterna ska säkerställa att deras behöriga myndigheter enligt detta direktiv samarbetar med de relevanta behöriga myndigheterna i den berörda medlemsstaten i enlighet med förordning (EU) 2022/2554. Medlemsstaterna ska särskilt säkerställa att deras behöriga myndigheter enligt detta direktiv informerar det tillsynsforum som inrättats enligt artikel 32.1 i förordning (EU) 2022/2554 när de utövar sina befogenheter med avseende på tillsyn och efterlevnadskontroll för att säkerställa att en viktig entitet som har identifierats som en kritisk tredjepartsleverantör av IKT-tjänster i enlighet med artikel 31 i förordning (EU) 2022/2554 efterlever detta direktiv.

Artikel 34

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 enligt denna artikel för överträdelser av detta direktiv är effektiva, proportionella och avskräckande, med beaktande av omständigheterna i varje enskilt fall.

2. Administrativa sanktionsavgifter ska påföras utöver någon av de åtgärder som avses i artikel 32.4 a–h, artikel 32.5 och artikel 33.4 a–g.

3. När beslut fattas om huruvida administrativa sanktionsavgifter ska påföras och om avgiftsbeloppet i varje enskilt fall, ska vederbörlig hänsyn tas till åtminstone de faktorer som anges i artikel 32.7.

4. Medlemsstaterna ska säkerställa att väsentliga entiteter som överträder artikel 21 eller 23, i enlighet med punkterna 2 och 3 i den här artikeln påförs administrativa sanktionsavgifter på högst 10 000 000 EUR eller högst 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.

5. Medlemsstaterna ska säkerställa att viktiga entiteter som överträder artikel 21 eller 23, i enlighet med punkterna 2 och 3 i den här artikeln påförs administrativa sanktionsavgifter på högst 7 000 000 EUR eller högst 1,4 % av den totala globala årsomsättningen under det föregående räkenskapsåret för det företag som den viktiga entiteten tillhör, beroende på vilken siffra som är högst.

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

7. Utan att det påverkar behöriga myndigheters befogenheter enligt artiklarna 32 och 33 får varje medlemsstat fastställa regler för huruvida och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga förvaltningsentiteter som omfattas av de skyldigheter som fastställs i detta direktiv.

8. Om administrativa sanktionsavgifter inte föreskrivs i en medlemsstats rättssystem ska den medlemsstaten säkerställa att denna artikel tillämpas på ett sådant sätt att förfarandet inleds av den behöriga myndigheten och sanktionsavgifterna sedan påförs av behöriga nationella domstolar, varvid det säkerställs att dessa rättsmedel är effektiva och har samma verkan som de administrativa sanktionsavgifter som påförs av de behöriga myndigheterna. De påförda sanktionsavgifterna ska i alla händelser vara effektiva, proportionella och avskräckande. Medlemsstaten ska underrätta kommissionen om bestämmelserna i de lagar som den antar i enlighet med denna punkt senast den 17 oktober 2024 och, utan dröjsmål, om eventuella senare ändringslagstiftning eller ändringar som berör dem.

Artikel 35

Överträdelser som innebär personuppgiftsincidenter

1. Om de behöriga myndigheterna under tillsyn eller efterlevnadskontroll får kännedom om att en väsentlig eller viktig entitets överträdelse av de skyldigheter som fastställs i artiklarna 21 och 23 i detta direktiv kan innebära en personuppgiftsincident, enligt definitionen i artikel 4.12 i förordning (EU) 2016/679, som ska anmälas i enlighet med artikel 33 i den förordningen, ska de utan onödigt dröjsmål informera de tillsynsmyndigheter som avses i artikel 55 eller 56 i den förordningen.

2. Om de tillsynsmyndigheter som avses i artikel 55 eller 56 i förordning (EU) 2016/679 påför administrativa sanktionsavgifter enligt artikel 58.2 i) i den förordningen ska de behöriga myndigheterna inte påföra administrativa sanktionsavgifter enligt artikel 34 i detta direktiv för en överträdelse som avses i punkt 1 i den här artikeln som följer av samma beteende som det som den administrativa sanktionsavgiften avsåg enligt artikel 58.2 i) i förordning (EU) 2016/679. De behöriga myndigheterna får emellertid tillämpa de efterlevnadskontrollåtgärder som föreskrivs i artikel 32.4 a–h, artikel 32.5 och artikel 33.4 a–g 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, ska den behöriga myndigheten informera den tillsynsmyndighet som är etablerad i dess egen medlemsstat om det potentiella dataintrång som avses i punkt 1.

Artikel 36

Sanktioner

Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av nationella åtgärder som antagits enligt detta direktiv och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska till kommissionen anmäla dessa regler och åtgärder senast den 17 januari 2025 samt utan dröjsmål eventuella ändringar som berör dem.

Artikel 37

Ömsesidigt bistånd

1. Om en entitet tillhandahåller tjänster i mer än en medlemsstat eller tillhandahåller tjänster i en eller flera medlemsstater och dess nätverks- och informationssystem är belägna i en eller flera andra medlemsstater ska de behöriga myndigheterna 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 tillhandahålla ömsesidigt bistånd till den andra behöriga myndigheten i proportion till sina egna resurser så att tillsyns- eller efterlevnadskontrollåtgärderna kan genomföras på ett ändamålsenligt, effektivt och konsekvent sätt.

Det ömsesidiga bistånd som avses i första stycket led c 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 inte avslå begäran om det inte fastställs att myndigheten antingen inte är behörig att tillhandahålla det begärda biståndet, att det begärda biståndet inte står i proportion till den behöriga myndighetens tillsynsuppgifter eller att begäran avser information eller omfattar verksamhet som, om den lämnas ut eller utförs, skulle strida mot den medlemsstatens väsentliga nationella säkerhetsintressen, allmänna säkerhet eller försvar. Innan den behöriga myndigheten avslår en sådan begäran ska den samråda med övriga berörda behöriga myndigheter samt, på begäran av en av de berörda medlemsstaterna, med kommissionen och Enisa.

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

KAPITEL VIII

DELEGERADE AKTER OCH GENOMFÖRANDEAKTER

Artikel 38

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.

2. Den befogenhet att anta delegerade akter som avses i artikel 24.2 ska ges till kommissionen för en period på fem år från och med den 16 januari 2023 .

3. Den delegering av befogenhet som avses i artikel 24.2 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i *Europeiska unionens officiella tidning*, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.

4. Innan kommissionen antar en delegerad akt ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet av den 13 april 2016 om bättre lagstiftning.

5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.

6. En delegerad akt som antas enligt artikel 24.2 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.

Artikel 39

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.

KAPITEL IX

SLUTBESTÄMMELSER

Artikel 40

Översyn

Senast den 17 oktober 2027 och därefter var 36:e månad ska kommissionen se över hur detta direktiv fungerar och rapportera resultatet till Europaparlamentet och rådet. Rapporten ska särskilt bedöma relevansen av de berörda enheternas storlek och sektorer, delsektorer och typer när det gäller den entitet som avses i bilagorna I och II för ekonomins och samhällets funktion när det gäller cybersäkerhet. För detta ändamål och för att ytterligare främja det strategiska och operativa samarbetet ska kommissionen beakta rapporterna från samarbetsgruppen och CSIRT-nätverket om de erfarenheter som förvärvats på strategisk och operativ nivå. Rapporten ska vid behov åtföljas av ett lagstiftningsförslag.

Artikel 41

Införlivande

1. Medlemsstaterna ska senast den 17 oktober 2024 anta och offentliggöra de bestämmelser som är nödvändiga för att följa detta direktiv. De ska genast underrätta kommissionen om detta.

De ska tillämpa dessa bestämmelser från och med den 18 oktober 2024.

2. När en medlemsstat antar de bestämmelser som avses i punkt 1 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 42

Ändring av förordning (EU) nr 910/2014

I förordning (EU) nr 910/2014 ska artikel 19 utgå med verkan från och med den 18 oktober 2024.

Artikel 43

Ändring av direktiv (EU) 2018/1972

I direktiv (EU) 2018/1972 ska artiklarna 40 och 41 utgå med verkan från och med den 18 oktober 2024.

Artikel 44

Upphävande

Direktiv (EU) 2016/1148 ska upphöra att gälla med verkan från och med den 18 oktober 2024.

Hänvisningar till det upphävda direktivet ska anses som hänvisningar till det här direktivet och ska läsas i enlighet med jämförelsetabellen i bilaga III.

Artikel 45

Ikraftträdande

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

Artikel 46

Adressater

Detta direktiv riktar sig till medlemsstaterna.

Utfärdat i Strasbourg den 14 december 2022.

På Europaparlamentets vägnar	*På rådets vägnar*
R. METSOLA	M. BEK
Ordförande	*Ordförande*

BILAGA I

HÖGKRITISKA SEKTORER

Sektor	Delsektor	Typ av entitet
1. Energi	a) Elektricitet	— Elföretag enligt definitionen i artikel 2.57 i Europaparlamentets och rådets direktiv (EU) 2019/944 ([1])som bedriver *leverans* enligt definitionen i artikel 2.12 i det direktivet
		— Systemansvariga för distributionssystem enligt definitionen i artikel 2.29 i direktiv (EU) 2019/944
		— Systemansvariga för överföringssystem enligt definitionen i artikel 2.35 i direktiv (EU) 2019/944
		— Producenter enligt definitionen i artikel 2.38 i direktiv (EU) 2019/944
		— Nominerade elmarknadsoperatörer enligt definitionen i artikel 2.8 i Europaparlamentets och rådets förordning (EU) 2019/943 ([2]) — Marknadsaktörer enligt definitionen i artikel 2.25 i förordning (EU) 2019/943 och som tillhandahåller aggregering, efterfrågeflexibilitet eller energilagringstjänster enligt definitionen i artikel 2.18, 2.20 och 2.59 i direktiv (EU) 2019/944 — Laddningsoperatörer som har ansvar för förvaltning och drift av en laddningspunkt och som tillhandahåller en laddningstjänst till slutanvändare, även när detta utförs på uppdrag av en leverantör av mobilitetstjänster och i dess namn
	b) Fjärrvärme eller fjärrkyla	— Operatörer av fjärrvärme eller fjärrkyla enligt definitionen i artikel 2.19 i Europaparlamentets och rådets direktiv (EU) 2018/2001 ([3])
	c) Olja	— Operatörer av oljeledningar
		— Operatörer av anläggningar för oljeproduktion, raffinaderier, bearbetningsanläggningar och anläggningar för lagring och överföring av olja
		— Centrala lagringsenheter enligt definitionen i artikel 2 f i rådets direktiv 2009/119/EG ([4])
	d) Gas	— Gashandelsföretag eller gashandlare enligt definitionen i artikel 2.8 i Europaparlamentets och rådets direktiv 2009/73/EG ([5])
		— Systemansvariga för distributionssystemet enligt definitionen i artikel 2.6 i direktiv 2009/73/EG
		— Systemansvariga för överföringssystemet enligt definitionen i artikel 2.4 i direktiv 2009/73/EG
		— Systemansvariga för lagringssystemet enligt definitionen i artikel 2.10 i direktiv 2009/73/EG
		— Systemansvariga för en LNG-anläggning enligt definitionen 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

Sektor	Delsektor	Typ av entitet
2. Transporter	a) Lufttransport	— Lufttrafikföretag enligt definitionen i artikel 3.4 i förordning (EG) nr 300/2008 och som används för kommersiella syften
		— Flygplatsens ledningsenheter enligt definitionen i artikel 2.2 i Europaparlamentets och rådets direktiv 2009/12/EG ([6]), flygplatser enligt definitionen i artikel 2.1 i det direktivet, inbegripet de huvudflygplatser som förtecknas i avsnitt 2 i bilaga II till Europaparlamentets och rådets förordning (EU) nr 1315/2013 ([7]), och enheter som driver närliggande anläggningar inom flygplatser
		— Operatörer inom trafikstyrning och trafikledning som tillhandahåller flygkontrolltjänst enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EG) nr 549/2004 ([8])
	b) Järnvägstransport	— Infrastrukturförvaltare enligt definitionen i artikel 3.2 i Europaparlamentets och rådets direktiv 2012/34/EU ([9])
		— Järnvägsföretag enligt definitionen i artikel 3.1 i direktiv 2012/34/EU, inbegripet tjänsteleverantörer enligt definitionen i artikel 3.12 i det direktivet
	c) Sjöfart	— Transportföretag som bedriver persontrafik och godstrafik på inre vattenvägar, till havs och längs kuster, enligt definitionerna för sjötransport i bilaga I till Europaparlamentets och rådets förordning (EG) nr 725/2004 ([10]), exklusive de enskilda fartyg som drivs av dessa företag
		— Ledningsenheter för hamnar enligt definitionen i artikel 3.1 i Europaparlamentets och rådets direktiv 2005/65/EG ([11]), inbegripet deras hamnanläggningar enligt definitionen i artikel 2.11 i förordning (EG) nr 725/2004, och enheter som sköter anläggningar och utrustning i hamnar
		— Operatörer av sjötrafikinformationstjänst (VTS) enligt definitionen i artikel 3 o i Europaparlamentets och rådets direktiv 2002/59/EG ([12])
	d) Vägtransport	— Vägmyndigheter enligt definitionen i artikel 2.12 i kommissionens delegerade förordning (EU) 2015/962 ([13]) med ansvar för trafikstyrning, med undantag för offentliga entiteter för vilka trafikstyrning eller driften av intelligenta transportsystem är en icke väsentlig del av deras allmänna verksamhet
		— Operatörer av intelligenta transportsystem enligt definitionen i artikel 4.1 i Europaparlamentets och rådets direktiv 2010/40/EU ([14])
3. Bankverksamhet		Kreditinstitut enligt definitionen i artikel 4.1 i Europaparlamentets och rådets förordning (EU) nr 575/2013 ([15])
4. Finansmarknads-infrastruktur		— Operatörer av handelsplatser enligt definitionen i artikel 4.24 i Europaparlamentets och rådets direktiv 2014/65/EU ([16])
		— Centrala motparter enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EU) nr 648/2012 ([17])

Sektor	Delsektor	Typ av entitet
5. Hälso- och sjukvårdssektorn		— Vårdgivare enligt definitionen i artikel 3 g i Europaparlamentets och rådets direktiv 2011/24/EU ([18])
		— EU-referenslaboratorier som avses i artikel 15 i Europaparlamentets och rådets förordning (EU) 20222/2371 ([19])
		— Entiteter som bedriver forskning och utveckling avseende läkemedel enligt definitionen i artikel 1.2 i Europaparlamentets och rådets direktiv 2001/83/EG ([20]) — Entiteter som tillverkar farmaceutiska basprodukter och läkemedel som avses i avsnitt C huvudgrupp 21 i Nace Rev. 2 — Entiteter som tillverkar medicintekniska produkter som anses vara kritiska vid ett hot mot folkhälsan (förteckning över kritiska medicintekniska produkter vid ett hot mot folkhälsan) i den mening som avses i artikel 22 i Europaparlamentets och rådets förordning (EU) 2022/123 ([21])
6. Dricksvatten		Leverantörer och distributörer av dricksvatten enligt definitionen i artikel 2.1 a i Europaparlamentets och rådets direktiv (EU) 2020/2184 ([22]) undantaget distributörer för vilka distribution av dricksvatten 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 eller industrispillvatten enligt definitionen i artikel 2.1–2.3 i rådets direktiv 91/271/EEG ([23]), undantaget företag som samlar ihop, släpper ut eller renar avloppsvatten från tätbebyggelse, hushållsspillvatten eller 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
		— Leverantörer av molntjänster
		— Leverantörer av datacentraltjänster
		— Leverantörer av nätverk för leverans av innehåll
		— Tillhandahållare av betrodda tjänster
		— Tillhandahållare av allmänna elektroniska kommunikationsnät
		— Tillhandahållare av allmänt tillgängliga elektroniska kommunikationstjänster
9. Förvaltning av IKT-tjänster (mellan företag)		— Leverantörer av hanterade tjänster — Leverantörer av hanterade säkerhetstjänster

Sektor	Delsektor	Typ av entitet
10. Offentlig förvaltning		— Offentliga förvaltningsentiteter hos nationella regeringar såsom de definieras av en medlemsstat i enlighet med nationell rätt
		— Offentliga förvaltningsentiteter på regional nivå såsom de definieras av en medlemsstat i enlighet med nationell rätt
11. Rymden		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

([1]) 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).
([2]) Europaparlamentets och rådets förordning (EU) 2019/943 av den 5 juni 2019 om den inre marknaden för el (EUT L 158, 14.6.2019, s. 54).
([3]) 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).
([4]) 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).
([5]) 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).
([6]) Europaparlamentets och rådets direktiv 2009/12/EG av den 11 mars 2009 om flygplatsavgifter (EUT L 70, 14.3.2009, s. 11).
([7]) 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).
([8]) 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).
([9]) 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).
([10]) 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).
([11]) Europaparlamentets och rådets direktiv 2005/65/EG av den 26 oktober 2005 om ökat hamnskydd (EUT L 310, 25.11.2005, s. 28).
([12]) 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 (EUT L 208, 5.8.2002, s. 10).
([13]) 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).
([14]) 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).
([15]) Europaparlamentets och rådets förordning (EU) nr 575/2013 av den 26 juni 2013 om tillsynskrav för kreditinstitut och om ändring av förordning (EU) nr 648/2012 (EUT L 176, 27.6.2013, s. 1).
([16]) 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).
([17]) 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).
([18]) 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).

(19) Europaparlamentets och rådets förordning (EU) 2022/2371 av den 23 november 2022 om allvarliga gränsöverskridande hot mot människors hälsa och om upphävande av beslut nr 1082/2013/EU (EUT L 314, 6.12.2022, s. 26).

(20) 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).

(21) Europaparlamentets och rådets förordning (EU) 2022/123 av den 25 januari 2022 om en förstärkt roll för Europeiska läkemedelsmyndigheten vid krisberedskap och krishantering avseende läkemedel och medicintekniska produkter (EUT L 20, 31.1.2022, s. 1).

(22) Europaparlamentets och rådets direktiv (EU) 2020/2184 av den 16 december 2020 om kvaliteten på dricksvatten (EUT L 435, 23.12.2020, s. 1).

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

BILAGA II

ANDRA KRITISKA SEKTORER

Sektor	Delsektor	Typ av entitet
1. Post- och budtjänster		Tillhandahållare av posttjänster enligt definitionen i artikel 2.1a i direktiv 97/67/EG, inbegripet tillhandahållare av budtjänster
2. Avfallshantering		Verksamhetsutövare som bedriver avfallshantering enligt definitionen i artikel 3.9 i Europaparlamentets och rådets direktiv 2008/98/EG ([1]), dock undantaget verksamhetsutövare vars huvudsakliga näringsverksamhet inte är av avfallshantering
3. Tillverkning, produktion och distribution av kemikalier		Företag som tillverkar ämnen och distribuerar ämnen eller blandningar som avses i artikel 3.9 och 3.14 i Europaparlamentets och rådets förordning (EG) nr 1907/2006 ([2]) samt företag som producerar varor enligt definitionen i artikel 3.3 i den förordningen genom att använda ämnen och blandningar
4. Produktion, bearbetning och distribution av livsmedel		Livsmedelsföretag enligt definitionen i artikel 3.2 i Europaparlamentets och rådets förordning (EG) nr 178/2002 ([3]) som bedriver 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 enligt definitionen i artikel 2.1 i Europaparlamentets och rådets förordning (EU) 2017/745 ([4])nligt definitionen i artikel 2.2 i Europaparlamentets och rådets förordning (EU) 2017/746 ([5]), med undantag av entiteter som tillverkar sådana medicintekniska produkter som avses i punkt 5 femte strecksatsen i bilaga I i detta direktiv
	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

Sektor	Delsektor	Typ av entitet
6. Digitala leverantörer		— Leverantörer av marknadsplatser online
		— Leverantörer av sökmotorer
		— Leverantörer av plattformar för sociala nätverkstjänster
7. Forskning		Forskningsorganisationer

([1]) 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).

([2]) 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).

([3]) 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).

([4]) 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).

([5]) 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).

BILAGA III

JÄMFÖRELSETABELL

Direktiv (EU) 2016/1148	Detta direktiv
Artikel 1.1	Artikel 1.1
Artikel 1.2	Artikel 1.2
Artikel 1.3	–
Artikel 1.4	Artikel 2.12
Artikel 1.5	Artikel 2.13
Artikel 1.6	Artikel 2.6 och 2.11
Artikel 1.7	Artikel 4
Artikel 2	Artikel 2.14
Artikel 3	Artikel 5
Artikel 4	Artikel 6
Artikel 5	–
Artikel 6	–
Artikel 7.1	Artikel 7.1 och 7.2
Artikel 7.2	Artikel 7.4
Artikel 7.3	Artikel 7.3
Artikel 8.1–8.5	Artikel 8.1–8.5
Artikel 8.6	Artikel 13.4
Artikel 8.7	Artikel 8.6
Artikel 9.1, 9.2 och 9.3	Artikel 10.1, 10.2 och 10.3
Artikel 9.4	Artikel 10.9
Artikel 9.5	Artikel 10.10
Artikel 10.1, 10.2 och 10.3 första stycket	Artikel 13.1, 13.2 och 13.3
Artikel 10.3 andra stycket	Artikel 23.9
Artikel 11.1	Artikel 14.1 och 14.2
Artikel 11.2	Artikel 14.3
Artikel 11.3	Artikel 14.4 första stycket leden a–q och led s och 14.7
Artikel 11.4	Artikel 14.4 första stycket led r och andra stycket
Artikel 11.5	Artikel 14.8
Artikel 12.1–12.5	Artikel 15.1–15.5
Artikel 13	Artikel 17
Artikel 14.1 och 14.2	Artikel 21.1–21.4
Artikel 14.3	Artikel 23.1
Artikel 14.4	Artikel 23.3
Artikel 14.5	Artikel 23.5, 23.6 och 23.8

Direktiv (EU) 2016/1148	Detta direktiv
Artikel 14.6	Artikel 23.7
Artikel 14.7	Artikel 23.11
Artikel 15.1	Artikel 31.1
Artikel 15.2 första stycket a	Artikel 32.2 e
Artikel 15.2 första stycket b	Artikel 32.2 g
Artikel 15.2 andra stycket	Artikel 32.3
Artikel 15.3	Artikel 32.4 b
Artikel 15.4	Artikel 31.3
Artikel 16.1 och 16.2	Artikel 21.1–21.4
Artikel 16.3	Artikel 23.1
Artikel 16.4	Artikel 23.3
Artikel 16.5	–
Artikel 16.6	Artikel 23.6
Artikel 16.7	Artikel 23.7
Artikel 16.8 och 16.9	Artiklarna 21.5 och 23.11
Artikel 16.10	–
Artikel 16.11	Artikel 2.1, 2.2 och 2.3
Artikel 17.1	Artikel 33.1
Artikel 17.2 a	Artikel 32.2 e
Artikel 17.2 b	Artikel 32.4 b
Artikel 17.3	Artikel 37.1 a och b
Artikel 18.1	Artikel 26.1 b och 26.2
Artikel 18.2	Artikel 26.3
Artikel 18.3	Artikel 26.4
Artikel 19	Artikel 25
Artikel 20	Artikel 30
Artikel 21	Artikel 36
Artikel 22	Artikel 39
Artikel 23	Artikel 40
Artikel 24	–
Artikel 25	Artikel 41
Artikel 26	Artikel 45
Artikel 27	Artikel 46
Bilaga I punkt 1	Artikel 11.1
Bilaga I punkt 2 a i–iv	Artikel 11.2 a–d

Direktiv (EU) 2016/1148	Detta direktiv
Bilaga I punkt 2 a v	Artikel 11.2 f
Bilaga I punkt 2 b	Artikel 11.4
Bilaga I punkt 2 c i och ii	Artikel 11.5 a
Bilaga II	Bilaga I
Bilaga III punkterna 1 och 2	Bilaga II punkt 6
Bilaga III punkt 3	Bilaga I punkt 8