EUROPA-
KOMMISSIONEN

Bruxelles, den 16.12.2020
COM(2020) 823 final

2020/0359 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV

om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen og om ophævelse af direktiv (EU) 2016/1148

(EØS-relevant tekst)

{SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}

BEGRUNDELSE

1. BAGGRUND FOR FORSLAGET

• Forslagets begrundelse og formål

Dette forslag er en del af en pakke af foranstaltninger til yderligere at forbedre offentlige og private enheders, kompetente myndigheders og Unionens samlede modstandsdygtighed og beredskabskapacitet inden for cybersikkerhed og beskyttelse af kritisk infrastruktur. Det er i overensstemmelse med Kommissionens prioriteter om at gøre Europa klar til den digitale tidsalder og opbygge en fremtidssikret økonomi, der tjener alle. Cybersikkerhed er en prioritet i Kommissionens reaktion på covid-19-krisen. Pakken omfatter en ny strategi for cybersikkerhed med det formål at styrke Unionens strategiske autonomi med henblik på at forbedre dens modstandsdygtighed og kollektive reaktion og opbygge et åbent og globalt internet. Endelig indeholder pakken et forslag til direktiv om modstandsdygtigheden hos kritiske operatører af væsentlige tjenester, som har til formål at afbøde fysiske trusler mod sådanne operatører.

Dette forslag bygger på og ophæver direktiv (EU) 2016/1148 om sikkerhed i net- og informationssystemer (NIS-direktivet), som er den første EU-retsakt om cybersikkerhed og indeholder retlige foranstaltninger, der skal styrke det generelle cybersikkerhedsniveau i Unionen. NIS-direktivet har 1) bidraget til at forbedre cybersikkerhedskapaciteten på nationalt plan ved at kræve, at medlemsstaterne vedtager nationale cybersikkerhedsstrategier og udpeger cybersikkerhedsmyndigheder, 2) øget samarbejdet mellem medlemsstaterne på EU-plan ved at oprette forskellige fora, der letter udvekslingen af strategiske og operationelle oplysninger og 3) forbedret offentlige og private enheders cyberrobusthed i syv specifikke sektorer (energi, transport, bankvæsen, finansielle markedsinfrastrukturer, sundhedspleje, drikkevandsforsyning og -distribution samt digitale infrastrukturer) og på tværs af tre digitale tjenester (onlinemarkedspladser, onlinesøgemaskiner og cloud computing-tjenester) ved at kræve, at medlemsstaterne sikrer, at operatører af væsentlige tjenester og udbydere af digitale tjenester indfører cybersikkerhedskrav og foretager underretninger om hændelser.

Forslaget moderniserer de eksisterende retlige rammer under hensyntagen til den øgede digitalisering af det indre marked i de senere år og et trusselsbillede for cybersikkerheden, der udvikler sig løbende. Begge disse udviklinger er blevet yderligere forstærket, siden covid-19-krisen satte ind. Forslaget tager også fat på en række svagheder, der forhindrede NIS-direktivet i at frigøre sit fulde potentiale.

Til trods for sine bemærkelsesværdige resultater har NIS-direktivet, som banede vejen for en betydelig ændring i tankegangen i forbindelse med den institutionelle og lovgivningsmæssige tilgang til cybersikkerhed i mange medlemsstater, også vist sig at have sine begrænsninger. Den digitale omstilling af samfundet (intensiveret af covid-19-krisen) har udvidet trusselsbilledet og skaber nye udfordringer, som kræver tilpassede og innovative løsninger. Antallet af cyberangreb stiger fortsat, og der kommer stadig mere sofistikerede angreb fra en bred vifte af kilder i og uden for EU.

I den evaluering af NIS-direktivets funktion, der blev foretaget med henblik på konsekvensanalysen, blev der peget på følgende spørgsmål: 1) den lave cybermodstandsdygtighed blandt virksomheder, der er aktive i EU, 2) inkonsekvent modstandsdygtighed på tværs af medlemsstater og sektorer og 3) det lave niveau af fælles situationsbevidsthed og manglen på fælles kriserespons. Visse større hospitaler i en medlemsstat falder f.eks. ikke ind under NIS-direktivets anvendelsesområde og er derfor ikke forpligtet til at gennemføre de deraf følgende sikkerhedsforanstaltninger, mens næsten alle udbydere af sundhedstjenester i en anden medlemsstat er omfattet af NIS-sikkerhedskravene.

Da forslaget er et initiativ inden for programmet for målrettet og effektiv regulering (REFIT), har det til formål at mindske den reguleringsmæssige byrde for de kompetente myndigheder og overholdelsesomkostningerne for offentlige og private enheder. Dette opnås især ved at ophæve de kompetente myndigheders forpligtelse til at identificere operatører af væsentlige tjenester og ved at øge graden af harmonisering af sikkerheds- og underretningskrav for at lette overholdelsen af lovgivningen for enheder, der leverer grænseoverskridende tjenester. Samtidig vil de kompetente myndigheder også få tildelt en række nye opgaver, herunder tilsyn med enheder i sektorer, der hidtil ikke har været omfattet af NIS-direktivet.

- **Sammenhæng med de gældende regler på samme område**

Dette forslag er en del af en bredere vifte af eksisterende retlige instrumenter og kommende initiativer på EU-plan, der har til formål at øge offentlige og private enheders modstandsdygtighed over for trusler.

På cybersikkerhedsområdet er der navnlig tale om direktiv (EU) 2018/1972 om en europæisk kodeks for elektronisk kommunikation (hvis bestemmelser vedrørende cybersikkerhed vil blive erstattet af bestemmelserne i nærværende forslag) og forslaget til forordning om digital operationel modstandsdygtighed i den finansielle sektor (COM(2020) 595 final), som vil blive betragtet som lex specialis i forhold til det foreliggende forslag, når begge retsakter er trådt i kraft.

På området fysisk sikkerhed supplerer dette forslag forslaget til direktiv om kritiske enheders modstandsdygtighed, som reviderer direktiv 2008/114/EF om indkredsning og udpegning af europæisk kritisk infrastruktur og vurdering af behovet for at beskytte den bedre (ECI-direktivet), hvori der fastlægges en EU-procedure for identifikation og udpegning af europæisk kritisk infrastruktur og fastlægges en tilgang til forbedring af beskyttelsen heraf. I juli 2020 vedtog Kommissionen strategien for EU's sikkerhedsunion[1], hvori man anerkendte den stigende sammenkobling og indbyrdes afhængighed mellem fysiske og digitale infrastrukturer. Den understregede behovet for en mere sammenhængende og konsekvent tilgang mellem ECI-direktivet og direktiv (EU) 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen.

Forslaget er derfor nøje afstemt med forslaget til direktiv om kritiske enheders modstandsdygtighed, der har til formål at styrke kritiske enheders modstandsdygtighed over for fysiske trusler i en lang række sektorer. Forslaget har til formål at sikre, at kompetente myndigheder i henhold til begge retsakter træffer supplerende foranstaltninger og udveksler oplysninger efter behov vedrørende cyberrobusthed og manglende cyberrobusthed, og at særligt kritiske operatører i de sektorer, der anses for at være "væsentlige" i henhold til det foreliggende forslag, også er underlagt mere generelle forpligtelser til at øge modstandsdygtigheden med vægten lagt på ikkecyberrelaterede risici.

- **Sammenhæng med Unionens politik på andre områder**

Som beskrevet i meddelelsen "Europas digitale fremtid i støbeskeen"[2] er det afgørende, at Europa høster alle fordelene ved den digitale tidsalder og styrker sin industri- og innovationskapacitet inden for sikre og etiske grænser. I den europæiske strategi for data fastsættes der fire søjler — databeskyttelse, grundlæggende rettigheder, sikkerhed og

[1] COM(2020) 605 final.
[2] COM(2020) 67 final.

cybersikkerhed– som væsentlige forudsætninger for et samfund, der styrkes ved brugen af data.

I sin beslutning af 12. marts 2019 opfordrede Europa-Parlamentet "Kommissionen til at vurdere behovet for yderligere at udvide NIS-direktivets anvendelsesområde til andre kritiske sektorer og tjenester, der ikke er omfattet af sektorspecifik lovgivning"[3]. Rådet udtrykte i sine konklusioner af 9. juni 2020 tilfredshed med "[...] Kommissionens planer om at sikre konsekvente regler for markedsoperatører og fremme sikker, solid og passende informationsudveksling om trusler såvel som hændelser, herunder gennem en revision af direktivet om net- og informationssystemer (NIS-direktivet), for at forfølge muligheder for at forbedre cyberrobustheden og sikre en mere effektiv reaktion på cyberangreb, navnlig om væsentlige økonomiske og samfundsmæssige aktiviteter, samtidig med at medlemsstaternes kompetencer, herunder ansvaret for deres nationale sikkerhed, respekteres[4]." Den foreslåede retsakt gælder desuden med forbehold af anvendelsen af konkurrencereglerne som fastsat i traktaten om Den Europæiske Unions funktionsmåde (TEUF).

Eftersom en betydelig del af truslerne mod cybersikkerheden stammer fra lande uden for EU, er der behov for en sammenhængende tilgang til internationalt samarbejde. Dette direktiv udgør en referencemodel, der skal fremmes i forbindelse med EU's samarbejde med tredjelande, navnlig når der ydes ekstern teknisk bistand.

2. RETSGRUNDLAG, NÆRHEDSPRINCIPPET OG PROPORTIONALITETSPRINCIPPET

- **Retsgrundlag**

Retsgrundlaget for NIS-direktivet er artikel 114 i traktaten om Den Europæiske Unions funktionsmåde, hvis formål er det indre markeds oprettelse og funktion ved at styrke foranstaltningerne til indbyrdes tilnærmelse af de nationale regler. Som EU-Domstolen fastslog i sin dom i sag C-58/08 Vodafone m.fl., er anvendelsen af artikel 114 i TEUF berettiget, når der er forskelle mellem nationale regler, der har direkte indvirkning på det indre markeds funktion. Domstolen fastslog ligeledes, at når en retsakt baseret på artikel 114 i TEUF allerede har fjernet enhver hindring for samhandelen på det område, den harmoniserer, kan EU-lovgiver ikke fratages muligheden for at tilpasse denne retsakt til samtlige ændrede omstændigheder eller ny viden, henset til den opgave, den har til at sikre beskyttelsen af de almene hensyn, der er anerkendt i traktaten. Endelig fastslog Domstolen, at de foranstaltninger med henblik på indbyrdes tilnærmelse, der er omhandlet i artikel 114 TEUF, har til formål at give en skønsmargen med hensyn til, hvilken tilnærmelsesmetode der er bedst egnet til at opnå det ønskede resultat, afhængigt af den generelle sammenhæng og de særlige omstændigheder på området, der skal harmoniseres. Den foreslåede retsakt vil fjerne hindringer for og forbedre det indre markeds oprettelse og funktion for væsentlige og vigtige enheder ved at fastlægge klare og almindeligt gældende regler om anvendelsesområdet for NIS-direktivet, der harmoniserer de regler, som finder anvendelse på styring af cybersikkerhedsrisici og underretning om hændelser. De nuværende forskelle på dette område, både på lovgivnings- og tilsynsniveau samt på det nationale plan og EU-plan, udgør hindringer for det indre marked, fordi enheder, der udøver grænseoverskridende aktiviteter, står over for forskellige og muligvis overlappende reguleringsmæssige krav og/eller

[3] https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_DA.html.
[4] https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/da/pdf.

anvendelsen af disse på bekostning af udøvelsen af deres etableringsfrihed og retten til fri udveksling af tjenesteydelser. Forskellige regler har også en negativ indvirkning på konkurrencevilkårene i det indre marked, når der er tale om enheder af samme type i forskellige medlemsstater.

- **Nærhedsprincippet (for områder, der ikke er omfattet af enekompetence)**

Modstandsdygtigheden over for cybertrusler i hele Unionen kan ikke være effektiv, hvis der gribes ind på en uensartet måde gennem nationale eller regionale siloer. NIS-direktivet afhjalp til dels denne mangel ved at fastlægge en ramme for net- og informationssystemernes sikkerhed på nationalt plan og EU-plan. Omsættelsen og gennemførelsen af direktivet afslørede imidlertid også iboende mangler og begrænsninger i visse bestemmelser eller tilgange, f.eks. den uklare afgrænsning af direktivets anvendelsesområde, der førte til betydelige forskelle i omfanget og dybden af EU's faktiske indgreb på medlemsstatsplan. Siden covid-19-krisen er den europæiske økonomi desuden blevet endnu mere afhængig af net- og informationssystemer end nogensinde før, og sektorer og tjenester er i stigende grad indbyrdes forbundne. En EU-indsats, der går videre end de nuværende foranstaltninger i NIS-direktivet, er primært begrundet i: i) de NIS-relaterede truslers og udfordringers stadig mere grænseoverskridende karakter, ii) potentialet i Unionens indsats med hensyn til at forbedre og fremme effektive og koordinerede nationale politikker og iii) bidraget fra samordnede og samarbejdsbaserede politiske tiltag til effektiv beskyttelse af personoplysninger og privatlivets fred.

- **Proportionalitetsprincippet**

De regler, der foreslås i dette direktiv, går ikke ud over, hvad der er nødvendigt for at nå de specifikke mål på tilfredsstillende vis. Den planlagte tilpasning og strømlining af sikkerhedsforanstaltninger og rapporteringsforpligtelser vedrører medlemsstaternes og virksomhedernes anmodninger om at forbedre den nuværende ramme.

Forslaget tager hensyn til den allerede eksisterende praksis i medlemsstaterne. Et højere beskyttelsesniveau, der opnås gennem sådanne strømlinede og koordinerede krav, står i rimeligt forhold til de stadig større risici, som de står over for, herunder dem, der udgør et grænseoverskridende element. De er rimelige og svarer generelt til de involverede enheders interesse i at sikre kontinuiteten og kvaliteten af deres tjenester. Omkostningerne ved at sikre systematisk samarbejde mellem medlemsstaterne vil være små sammenlignet med de økonomiske og samfundsmæssige tab og skader forårsaget af cybersikkerhedshændelser. Desuden viser de høringer af interesserede parter, der blev afholdt i forbindelse med evalueringen af NIS-direktivet, herunder resultaterne af den åbne offentlige høring og målrettede undersøgelser, at der er støtte til revisionen af NIS-direktivet i overensstemmelse med ovennævnte retningslinjer.

- **Valg af retsakt**

Forslaget vil yderligere strømline de forpligtelser, der pålægges virksomhederne, og sikre en højere grad af harmonisering af disse. Samtidig har forslaget til formål at give medlemsstaterne den fleksibilitet, der er nødvendig for at tage hensyn til særlige nationale forhold (f.eks. muligheden for at identificere yderligere væsentlige eller vigtige enheder, der ligger uden for det referencescenarie, som er fastsat i retsakten). Det kommende retlige instrument bør derfor være et direktiv, da dette retlige instrument giver mulighed for målrettet forbedret harmonisering og en vis grad af fleksibilitet for de kompetente myndigheder.

3. RESULTATER AF EFTERFØLGENDE EVALUERINGER, HØRINGER AF INTERESSEREDE PARTER OG KONSEKVENSANALYSER

- **Efterfølgende evalueringer/kvalitetskontrol af gældende lovgivning**

Kommissionen har gennemført en evaluering af NIS-direktivets[5] funktionsmåde. Den har analyseret dets relevans, EU-merværdi, sammenhæng, virkningsfuldhed og effektivitet. Hovedresultaterne af analysen er følgende:

- NIS-direktivets anvendelsesområde er for begrænset med hensyn til de omfattede sektorer, primært på grund af: i) øget digitalisering i de senere år og en højere grad af indbyrdes forbundethed og ii) NIS-direktivets anvendelsesområde afspejler ikke længere alle digitaliserede sektorer, der leverer vigtige tjenester til økonomien og samfundet som helhed.
- NIS-direktivet er ikke tilstrækkeligt klart med hensyn til anvendelsesområdet for operatører af væsentlige tjenester, og dets bestemmelser skaber ikke tilstrækkelig klarhed med hensyn til den nationale kompetence over for udbydere af digitale tjenester. Dette har ført til en situation, hvor visse typer af enheder ikke er blevet identificeret i alle medlemsstater og derfor ikke er forpligtet til at indføre sikkerhedsforanstaltninger og foretage underretninger om hændelser.
- Med fastsættelsen af krav til sikkerheds- og hændelsesunderretninger for operatører af væsentlige tjenester i NIS-direktivet fik medlemsstaterne vide skønsbeføjelser. Evalueringen viser, at medlemsstaterne i nogle tilfælde har gennemført disse krav på særdeles forskellig vis, hvilket har medført yderligere byrder for virksomheder, der opererer i mere end én medlemsstat.
- NIS-direktivets tilsyns- og håndhævelsesordning er ineffektiv. Medlemsstaterne har f.eks. været meget tilbageholdende med at indføre sanktioner over for enheder, der undlader at indføre sikkerhedskrav eller foretage underretninger om hændelser. Dette kan have negative konsekvenser for individuelle enheders cyberrobusthed.
- De økonomiske og menneskelige ressourcer, som medlemsstaterne har afsat til at udføre deres opgaver (såsom identifikation af eller tilsyn med operatører af væsentlige tjenester), og dermed de forskellige modenhedsniveauer i forbindelse med cybersikkerhedsrisici, varierer meget. Dette øger forskellene i cyberrobusthed mellem medlemsstaterne yderligere.
- Medlemsstaterne udveksler ikke systematisk oplysninger med hinanden, hvilket navnlig har negative konsekvenser for effektiviteten af cybersikkerhedsforanstaltningerne og for niveauet af fælles situationsbevidsthed på EU-plan. Dette er også tilfældet for udveksling af oplysninger mellem private enheder og for samarbejdet mellem samarbejdsstrukturer på EU-plan og private enheder.

- **Høringer af interesserede parter**

Kommissionen har hørt en lang række interesserede parter. Medlemsstaterne og de interesserede parter blev opfordret til at deltage i den åbne offentlige høring og i de undersøgelser og workshopper, der blev afholdt af Wavestone, CEPS og ICF, som Kommissionen har hyret til at gennemføre en undersøgelse til støtte for evalueringen af NIS-direktivet. De hørte interesserede parter omfattede kompetente myndigheder, EU-organer, der

[5] [Bilag 5 til konsekvensanalysen].

beskæftiger sig med cybersikkerhed, operatører af væsentlige tjenester, udbydere af digitale tjenester, enheder, der leverer tjenester uden for anvendelsesområdet for det nuværende NIS-direktiv, brancheorganisationer samt forbrugerorganisationer og borgere.

Desuden har Kommissionen været i løbende kontakt med de kompetente myndigheder, der er ansvarlige for gennemførelsen af NIS-direktivet. Samarbejdsgruppen har i vid udstrækning behandlet forskellige tværgående og sektorspecifikke gennemførelsesaspekter. Endelig har Kommissionen under sine NIS-landebesøg i 2019 og 2020 interviewet 154 offentlige og private enheder samt 117 kompetente myndigheder.

- **Indhentning og brug af ekspertbistand**

Kommissionen har indgået kontrakt med et konsortium bestående af Wavestone, CEPS og ICF, som skal støtte Kommissionen i forbindelse med evalueringen af NIS-direktivet[6]. Kontrahenten har ikke kun været i kontakt med de interesserede parter, der er direkte berørt af NIS-direktivet, gennem målrettede undersøgelser og workshopper, men har også hørt en bred vifte af eksperter inden for cybersikkerhed, såsom cybersikkerhedsforskere og fagfolk inden for cybersikkerhedsindustrien.

- **Konsekvensanalyse**

Dette forslag ledsages af en konsekvensanalyse[7], som blev forelagt Udvalget for Forskriftskontrol den 23. oktober 2020 og modtog en positiv udtalelse med bemærkninger fra Udvalget for Forskriftskontrol den 20. november 2020. Udvalget anbefalede forbedringer på nogle områder med henblik på: 1) bedre at afspejle den rolle, som grænseoverskridende afsmittende virkninger spiller i problemanalysen, 2) bedre at forklare, hvad det vil medføre, at initiativet betragtes som en succes, 3) yderligere at begrunde listen over politiske løsningsmodeller og 4) at give yderligere oplysninger om omkostningerne ved de foreslåede foranstaltninger. Konsekvensanalysen blev tilpasset for at tage højde for disse punkter samt mere detaljerede bemærkninger fra Udvalget for Forskriftskontrol. Den indeholder nu mere detaljerede forklaringer af den rolle, som grænseoverskridende afsmittende virkninger spiller på cybersikkerhedsområdet, et klarere overblik over, hvordan succes kan måles, en mere detaljeret redegørelse for udformningen af og logikken bag de forskellige politiske løsningsmodeller og foranstaltninger, der overvejes inden for disse løsningsmodeller, en mere detaljeret redegørelse for de aspekter, der er analyseret i forbindelse med NIS-direktivets sektorspecifikke anvendelsesområde, og yderligere præciseringer vedrørende omkostninger.

Kommissionen overvejede en række politiske løsningsmodeller for at forbedre de retlige rammer inden for cyberrobusthed og reaktion på hændelser:

- "Ingen foranstaltninger": NIS-direktivet vil forblive uændret, og der vil ikke blive truffet andre foranstaltninger af ikkelovgivningsmæssig karakter for at rette op på de problemer, der er identificeret i forbindelse med evalueringen af NIS-direktivet.
- Løsningsmodel 1: Der vil ikke ske nogen ændringer på lovgivningsniveau. I stedet vil Kommissionen udstede henstillinger og retningslinjer (f.eks. om identifikation af operatører af væsentlige tjenester, sikkerhedskrav, procedurer for underretning om

[6] Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) — N° 2020-665. Wavestone, CEPS og ICF.

[7] **[Link to final document and the summary sheet to be added (link til endeligt dokument og resumé tilføjes)].**

hændelser og tilsyn) efter høring af samarbejdsgruppen, EU's Agentur for Cybersikkerhed (ENISA) og, hvis det er relevant, netværket af enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er).

- Løsningsmodel 2: Denne løsningsmodel indebærer målrettede ændringer af NIS-direktivet, herunder en udvidelse af anvendelsesområdet og flere andre ændringer, der har til formål at indføre visse umiddelbare løsninger på de konstaterede problemer, skabe større klarhed og yderligere harmonisering (f.eks. bestemmelser om harmonisering af tærskelværdier for identifikation). Det ændrede NIS-direktiv vil dog fortsat indeholde de vigtigste byggesten, tilgangen og begrundelsen.
- Løsningsmodel 3: Dette scenario indebærer systemiske og strukturelle ændringer af NIS-direktivet (i form af et nyt direktiv) med henblik på en mere grundlæggende ændring af tilgangen for at dække et større segment af økonomierne i hele Unionen, men med et mere fokuseret tilsyn rettet mod store og centrale aktører. Det vil også strømline de forpligtelser, der pålægges virksomhederne, og sikre en højere grad af harmonisering af disse, skabe en mere effektiv ramme for operationelle aspekter samt skabe et klart grundlag for øget fælles ansvar og ansvarlighed for forskellige interessenter i forbindelse med cybersikkerhedsforanstaltninger.

Konsekvensanalysen konkluderer, at den foretrukne løsningsmodel er løsningsmodel 3 (dvs. systemiske og strukturelle ændringer af NIS-rammen). Med hensyn til effektivitet vil den foretrukne løsningsmodel klart fastlægge anvendelsesområdet for NIS-direktivet, som udvides til et mere repræsentativt udsnit af EU's økonomier og samfund, og strømlining af kravene sammen med en tydeligere defineret ramme for tilsyn og håndhævelse, der sigter mod at øge overholdelsesgraden. Det omfatter også foranstaltninger, der har til formål at forbedre tilgangen til politikopbygning på medlemsstatsniveau og ændre paradigmet herfor, fremme nye rammer for risikostyring i forbindelse med leverandørrelationer og koordineret offentliggørelse af sårbarheder. Samtidig skaber den foretrukne løsningsmodel et klart grundlag for delt ansvar og ansvarlighed og omfatter mekanismer, der har til formål at fremme større tillid mellem medlemsstaterne, både myndighederne og erhvervslivet, tilskynde til informationsudveksling og sikre en mere operationel tilgang såsom gensidig bistand og peerevalueringsmekanismer. Denne løsningsmodel vil også skabe en EU-krisestyringsramme, der bygger på det operationelle EU-netværk, som blev lanceret for nylig, og vil sikre større inddragelse af ENISA inden for dets nuværende mandat for at opnå et præcist overblik over Unionens tilstand med hensyn til cybersikkerhed.

For så vidt angår effektivitet vil den foretrukne løsningsmodel ganske vist medføre yderligere overholdelses- og håndhævelsesomkostninger for virksomheder og medlemsstater, men den vil også føre til effektive afvejninger og synergier med det bedste potentiale blandt alle de analyserede politiske løsningsmodeller og sikre en øget og konsekvent grad af cyberrobusthed hos centrale enheder i hele Unionen, hvilket i sidste ende vil føre til omkostningsbesparelser for både virksomheder og samfundet. Denne løsningsmodel vil medføre en vis ekstra administrativ byrde og overholdelsesomkostninger for medlemsstaternes myndigheder. På mellemlang og lang sigt vil den dog samlet set også medføre betydelige fordele i form af øget samarbejde mellem medlemsstaterne, herunder på operationelt plan, og, ved hjælp af gensidig bistand, tilskynde til peerevalueringsmekanismer og bedre overblik over og interaktion med centrale virksomheder, en generel forøgelse af cybersikkerhedskapaciteten på nationalt og regionalt plan. Den foretrukne løsningsmodel vil også i vid udstrækning sikre sammenhæng med anden lovgivning og andre initiativer eller politiske foranstaltninger, herunder sektorspecifikke lex specialis.

Afhjælpning af den nuværende mangel på cybersikkerhedsberedskab på medlemsstatsniveau og på virksomhedsniveau og i andre organisationer kan føre til effektivitetsgevinster og reduktion af ekstraomkostninger som følge af cybersikkerhedshændelser.

- For væsentlige og vigtige enheder kan en styrkelse af cybersikkerhedsberedskabet resultere i en begrænsning af det potentielle indtægtstab som følge af afbrydelser — herunder som følge af industrispionage — og kan reducere de store udgifter til ad hoc-trusselsbegrænsning. Sådanne gevinster vil sandsynligvis opveje de nødvendige investeringsomkostninger. En mindre fragmentering af det indre marked vil også føre til mere lige vilkår for operatørerne.
- For medlemsstaterne kan det yderligere mindske risikoen for stigende budgetudgifter til ad hoc-trusselsbegrænsning og yderligere omkostninger i tilfælde af nødsituationer i forbindelse med cybersikkerhedshændelser.
- For borgerne forventes det, at håndteringen af cybersikkerhedshændelser vil resultere i et lavere indkomsttab som følge af økonomiske forstyrrelser.

Det øgede cybersikkerhedsniveau i medlemsstaterne og virksomhedernes og myndighedernes evne til at reagere hurtigt på en hændelse og afbøde dens konsekvenser vil sandsynligvis føre til en stigning i borgernes generelle tillid til den digitale økonomi, hvilket kan have en positiv indvirkning på vækst og investeringer.

En styrkelse af det generelle cybersikkerhedsniveau vil sandsynligvis føre til øget sikkerhed og gnidningsløs uafbrudt drift af væsentlige tjenester, som er af afgørende betydning for samfundet. Initiativet kan også bidrage til andre samfundsmæssige virkninger såsom lavere niveauer af cyberkriminalitet og terrorisme og øget civilbeskyttelse. Ved at øge cyberberedskabet for virksomheder og andre organisationer kan man undgå potentielle økonomiske tab som følge af cyberangreb og dermed fjerne behovet for at skulle afskedige medarbejdere.

En styrkelse af det generelle cybersikkerhedsniveau kan også føre til forebyggelse af miljørisici/miljøskader i tilfælde af et angreb på en væsentlig tjeneste. Dette kan især gælde for energi-, vandforsynings- og distributionssektoren samt transportsektoren. Ved at styrke cybersikkerhedskapaciteterne kan initiativet føre til øget brug af den seneste generation af IKT-infrastrukturer og -tjenester, som også er miljømæssigt mere bæredygtige, og til udskiftning af ineffektive og mindre sikre eksisterende infrastrukturer. Dette forventes også at bidrage til at nedbringe antallet af bekostelige cyberhændelser og frigøre ressourcer til bæredygtige investeringer.

- **Målrettet regulering og forenkling**

Forslaget indeholder en generel undtagelse for mikrovirksomheder og små enheder fra anvendelsesområdet for NIS og en mere lempelig ordning for efterfølgende tilsyn for et stort antal af de nye enheder under det reviderede anvendelsesområde (såkaldt vigtige enheder). Disse foranstaltninger har til formål at minimere og afbalancere den byrde, der pålægges virksomheder og offentlige myndigheder. Desuden erstatter forslaget det komplekse identifikationssystem for operatører af væsentlige tjenester med en generelt gældende forpligtelse og indfører en højere grad af harmonisering af sikkerheds- og rapporteringsforpligtelser, hvilket vil mindske overholdelsesbyrden, navnlig for enheder, der leverer grænseoverskridende tjenester.

Forslaget minimerer overholdelsesomkostningerne for SMV'er, da enhederne kun skal træffe de foranstaltninger, der er nødvendige for at sikre et sikkerhedsniveau for net- og informationssystemer, der svarer til den risiko, der er forbundet hermed.

- **Grundlæggende rettigheder**

EU har forpligtet sig at sikre til et højt niveau af beskyttelse af de grundlæggende rettigheder. Alle frivillige ordninger for udveksling af oplysninger mellem enheder, som dette direktiv fremmer, vil blive gennemført i sikre miljøer under fuld overholdelse af Unionens databeskyttelsesregler, navnlig Europa-Parlamentets og Rådets forordning (EU) 2016/679[8].

4. VIRKNINGER FOR BUDGETTET

Se finansieringsoversigten

5. ANDRE FORHOLD

- **Planer for gennemførelsen og foranstaltninger til overvågning, evaluering og rapportering**

Forslaget indeholder en generel plan for overvågning og evaluering af indvirkningen på de specifikke mål, som kræver, at Kommissionen foretager en evaluering tidligst [54 måneder] efter forordningens ikrafttrædelsesdato og aflægger rapport til Europa-Parlamentet og Rådet om sine vigtigste konklusioner.

Denne revision skal foretages i overensstemmelse med Kommissionens retningslinjer for bedre regulering.

- **Nærmere redegørelse for de enkelte bestemmelser i forslaget**

Forslaget er bygget op omkring flere vigtige politikområder, som er indbyrdes forbundne og har til formål at højne cybersikkerhedsniveauet i Unionen.

Genstand og anvendelsesområde (artikel 1 og artikel 2)

Det gælder navnlig, at direktivet indeholder a) forpligtelser om, at medlemsstaterne skal vedtage en national cybersikkerhedsstrategi, udpege kompetente nationale myndigheder, centrale kontaktpunkter og CSIRT'er, b) bestemmelser om, at medlemsstaterne skal fastsætte forpligtelser om risikostyring og rapportering vedrørende cybersikkerhed for enheder, der benævnes væsentlige enheder i bilag I og vigtige enheder i bilag II, og c) bestemmelser om, at medlemsstaterne skal fastsætte forpligtelser vedrørende udveksling af cybersikkerhedsoplysninger.

Det finder anvendelse på visse offentlige eller private væsentlige enheder, der opererer inden for de sektorer, som er opført i bilag I (energi, transport, bankvæsen, finansielle markedsinfrastrukturer, sundhed, drikkevand, spildevand, digital infrastruktur, offentlig forvaltning og rummet) og visse vigtige enheder, der opererer inden for de sektorer, der er opført i bilag II (post- og kurertjenester, affaldshåndtering, fremstilling, fremstilling og distribution af kemikalier, fødevareproduktion, -forarbejdning og -distribution,

[8] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

fremstillingsvirksomhed og digitale udbydere). Mikrovirksomheder og små enheder som omhandlet i Kommissionens henstilling 2003/361/EF af 6. maj 2003 er udelukket fra direktivets anvendelsesområde, undtagen udbydere af elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester, tillidstjenesteudbydere, topdomænenavneregistraturer og offentlig forvaltning samt visse andre enheder såsom den eneste udbyder af en tjeneste i en medlemsstat.

Nationale rammer for cybersikkerhed (artikel 5-11)

Medlemsstaterne skal vedtage en national cybersikkerhedsstrategi, der definerer de strategiske mål og passende politiske og reguleringsmæssige foranstaltninger med henblik på at opnå og opretholde et højt cybersikkerhedsniveau.

Direktivet fastlægger også en ramme for koordineret underretning om sårbarheder og pålægger medlemsstaterne at udpege CSIRT'er, der skal fungere som betroede formidlere og lette samspillet mellem de underrettende enheder og producenter eller udbydere af IKT-produkter og -tjenester. ENISA skal udvikle og vedligeholde et europæisk sårbarhedsregister for de konstaterede sårbarheder.

Medlemsstaterne skal indføre nationale rammer for styring af cybersikkerhedskriser, bl.a. ved at udpege nationale kompetente myndigheder med ansvar for håndteringen af væsentlige cybersikkerhedshændelser og -kriser.

Medlemsstaterne skal også udpege en eller flere nationale kompetente myndigheder inden for cybersikkerhed til at varetage tilsynsopgaverne i henhold til dette direktiv og et nationalt centralt kontaktpunkt for cybersikkerhed (SPOC) til at varetage en forbindelsesfunktion for at sikre grænseoverskridende samarbejde mellem medlemsstaternes myndigheder. Medlemsstaterne skal også udpege CSIRT'er.

Samarbejde (artikel 12-16)

Ved direktivet nedsættes der en samarbejdsgruppe, der skal støtte og lette det strategiske samarbejde og udvekslingen af oplysninger mellem medlemsstaterne og udvikle tillid. Der oprettes også et CSIRT-netværk, der skal bidrage til udviklingen af tillid mellem medlemsstaterne og fremme et hurtigt og effektivt operationelt samarbejde.

Der oprettes et europæisk netværk af cybersikkerhedsorganisationer (EU-CyCLONe) for at støtte den koordinerede håndtering af væsentlige cybersikkerhedshændelser og -kriser og sikre regelmæssig udveksling af oplysninger mellem medlemsstaterne og EU-institutionerne.

ENISA skal i samarbejde med Kommissionen hvert andet år udsende en rapport om cybersikkerhedssituationen i Unionen.

Kommissionen skal etablere et peerevalueringssystem, der giver mulighed for regelmæssige peerevalueringer af medlemsstaternes politikker for cybersikkerhed.

Forpligtelser vedrørende risikostyring og rapportering i forbindelse med cybersikkerhed (artikel 17-23)

I henhold til direktivet skal medlemsstaterne fastsætte bestemmelser om, at ledelsesorganer i alle enheder, der er omfattet af anvendelsesområdet, skal godkende de

risikohåndteringsforanstaltninger vedrørende cybersikkerhed, der træffes af de respektive enheder, og følge specifik cybersikkerhedsrelateret uddannelse.

Medlemsstaterne skal sikre, at enheder inden for anvendelsesområdet træffer passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at håndtere de cybersikkerhedsrisici, der er forbundet med sikkerheden i net- og informationssystemer. De skal også sikre, at enheder underretter de nationale kompetente myndigheder eller CSIRT'erne om enhver cybersikkerhedshændelse, der har en væsentlig indvirkning på leveringen af den tjeneste, de udbyder.

Topdomænenavneregistraturer og enheder, der leverer domænenavnsregistreringstjenester for topdomænet, indsamler og vedligeholder nøjagtige og fuldstændige oplysninger om domænenavnsregistrering. Desuden er sådanne enheder forpligtet til at give lovlige adgangssøgende effektiv adgang til registreringsdata.

Kompetence og registrering (artikel 24 og 25)

Som hovedregel anses væsentlige og vigtige enheder for at være underlagt jurisdiktionen i den medlemsstat, hvor de leverer deres tjenester. Visse typer af enheder (udbydere af DNS-tjenester, topdomænenavneregistraturer, udbydere af cloud computing-tjenester, udbydere af datacentertjenester og udbydere af indholdsleveringsnetværk samt visse digitale udbydere) anses dog for at være underlagt jurisdiktionen i den medlemsstat, hvor de har deres hovedforretningssted i Unionen. Dette skal sikre, at sådanne enheder ikke stilles over for en lang række forskellige retlige krav, eftersom de i særlig høj grad leverer tjenesteydelser på tværs af grænserne. ENISA skal oprette og føre et register over den sidstnævnte type enheder.

Udveksling af oplysninger (artikel 26 og 27)

Medlemsstaterne fastsætter regler, der gør det muligt for enheder at deltage i udveksling af cybersikkerhedsrelaterede oplysninger inden for rammerne af specifikke ordninger for udveksling af cybersikkerhedsoplysninger i overensstemmelse med artikel 101 i TEUF. Desuden tillader medlemsstaterne enheder, der ikke er omfattet af dette direktiv, frivilligt at foretage underretninger om væsentlige hændelser, cybertrusler eller nærvedhændelser.

Tilsyn og håndhævelse (artikel 28-34)

De kompetente myndigheder skal føre tilsyn med de enheder, der er omfattet af direktivet, og navnlig sikre, at de overholder kravene til sikkerhed og underretning om hændelser. Der skelnes mellem en forudgående tilsynsordning for væsentlige enheder og en ordning for efterfølgende tilsyn med vigtige enheder, idet det senere kræves, at de kompetente myndigheder træffer foranstaltninger, når de får forelagt dokumentation for eller tegn på, at en vigtig enhed ikke opfylder kravene til sikkerhed og underretning om hændelser.

Direktivet pålægger også medlemsstaterne at pålægge væsentlige og vigtige enheder administrative bøder og fastsætter visse maksimumsbøder.

Medlemsstaterne skal samarbejde og bistå hinanden efter behov, når enheder leverer tjenesteydelser i mere end én medlemsstat, eller når en enheds hovedvirksomhed eller dens repræsentant er beliggende i en bestemt medlemsstat, mens dens net- og informationssystemer er beliggende i en eller flere andre medlemsstater.

2020/0359 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV

om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen og om ophævelse af direktiv (EU) 2016/1148

(EØS-relevant tekst)

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 114,

under henvisning til forslag fra Europa-Kommissionen,

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg[9],

under henvisning til udtalelse fra Regionsudvalget[10],

efter den almindelige lovgivningsprocedure, og

ud fra følgende betragtninger:

(1) Europa-Parlamentets og Rådets direktiv (EU) 2016/1148[11] tog sigte på at opbygge cybersikkerhedskapaciteter i hele Unionen, afbøde trusler mod net- og informationssystemer, der anvendes til at levere væsentlige tjenester i nøglesektorer, og sikre kontinuiteten i sådanne tjenester, når de står over for cybersikkerhedshændelser, og dermed bidrage til Unionens økonomi og samfund, så de kan fungere effektivt.

(2) Siden ikrafttrædelsen af direktiv (EU) 2016/1148 er der gjort betydelige fremskridt med hensyn til at øge EU's modstandsdygtighed over for cybertrusler. Evalueringen af dette direktiv har vist, at det har fungeret som katalysator for den institutionelle og lovgivningsmæssige tilgang til cybersikkerhed i Unionen og har banet vejen for en betydelig holdningsændring. Direktivet har sikret færdiggørelsen af de nationale rammer ved at fastlægge nationale cybersikkerhedsstrategier, etablere nationale kapaciteter og gennemføre lovgivningsmæssige foranstaltninger, der omfatter væsentlige infrastrukturer og aktører, som hver medlemsstat har udpeget. Det har også bidraget til samarbejdet på EU-plan gennem oprettelsen af samarbejdsgruppen[12] og et netværk af nationale enheder, der håndterer IT-sikkerhedshændelser ("CSIRT-netværket")[13]. Uanset disse resultater har evalueringen af direktiv (EU) 2016/1148

---

9 EUT C , , s. .

10 EUT C , , s. .

11 Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (EUT L 194 af 19.7.2016, s. 1).

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

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

afsløret iboende mangler, der forhindrer det i effektivt at tackle aktuelle og nye cybersikkerhedsudfordringer.

(3) Net- og informationssystemer har udviklet sig til et centralt element i hverdagen med den hurtige digitale omstilling og forbundethed i samfundet, herunder i forbindelse med grænseoverskridende udvekslinger. Denne udvikling har ført til en udvidelse af antallet og typen af trusler mod cybersikkerheden og skabt nye udfordringer, som kræver tilpassede, koordinerede og innovative svar i alle medlemsstater. Antallet, omfanget, den avancerede karakter, hyppigheden og virkningen af cybersikkerhedshændelser er stigende og udgør en alvorlig trussel mod net- og informationssystemernes funktion. Som følge heraf kan cyberhændelser hindre udøvelsen af økonomiske aktiviteter i det indre marked, medføre økonomiske tab, underminere brugernes tillid og forårsage store skader på Unionens økonomi og samfund. Cybersikkerhedsberedskab og -effektivitet er derfor mere afgørende for et velfungerende indre marked end nogensinde før.

(4) Retsgrundlaget for direktiv 1148/2016/EU var artikel 114 i traktaten om Den Europæiske Unions funktionsmåde (TEUF), hvis formål er det indre markeds oprettelse og funktion ved at styrke foranstaltninger til indbyrdes tilnærmelse af de nationale regler. De cybersikkerhedskrav, der pålægges enheder, som leverer tjenester eller økonomisk relevante aktiviteter, varierer betydeligt fra medlemsstat til medlemsstat med hensyn til typen af krav, detaljeringsgrad og tilsynsmetode. Disse forskelle medfører yderligere omkostninger og skaber vanskeligheder for virksomheder, der udbyder varer eller tjenesteydelser på tværs af grænserne. Krav, der stilles af en medlemsstat, og som er forskellige fra eller endog i konflikt med dem, der er pålagt af en anden medlemsstat, kan påvirke disse grænseoverskridende aktiviteter i væsentlig grad. Desuden vil muligheden for en suboptimal udformning eller gennemførelse af cybersikkerhedsstandarder i én medlemsstat sandsynligvis have konsekvenser for cybersikkerhedsniveauet i andre medlemsstater, navnlig i betragtning af de intense grænseoverskridende udvekslinger. Evalueringen af direktiv (EU) 2016/1148 har vist, at der er store forskelle i medlemsstaternes gennemførelse af det, herunder med hensyn til dets anvendelsesområde, hvis afgrænsning i vid udstrækning blev overladt til medlemsstaternes skøn. Direktiv (EU) 2016/1148 gav også medlemsstaterne meget vide skønsbeføjelser med hensyn til gennemførelsen af de sikkerheds- og hændelsesrapporteringsforpligtelser, der er fastsat deri. Disse forpligtelser blev derfor gennemført på vidt forskellige måder på nationalt plan. Lignende forskelle i gennemførelsen forekom i forhold til direktivets bestemmelser om tilsyn og håndhævelse.

(5) Alle disse forskelle medfører en fragmentering af det indre marked og kan have en negativ indvirkning på dets funktion og navnlig påvirke den grænseoverskridende levering af tjenester og cyberrobustheden som følge af anvendelsen af forskellige standarder. Dette direktiv har til formål at fjerne sådanne store forskelle mellem medlemsstaterne, navnlig ved at fastsætte minimumsregler for, hvordan en koordineret reguleringsramme fungerer, ved at fastlægge mekanismer for effektivt samarbejde mellem de ansvarlige myndigheder i hver medlemsstat, ved at ajourføre listen over sektorer og aktiviteter, der er omfattet af cybersikkerhedsforpligtelser, og ved at tilvejebringe effektive retsmidler og sanktioner, der er afgørende for en effektiv håndhævelse af disse forpligtelser. Derfor bør direktiv (EU) 2016/1148 ophæves og erstattes af dette direktiv.

(6) Dette direktiv er ikke til hinder for, at hver medlemsstat kan træffe de nødvendige foranstaltninger for at sikre beskyttelsen af sine væsentlige sikkerhedsinteresser,

opretholde den offentlige orden og sikkerhed samt tillade efterforskning, afsløring og retsforfølgelse af strafbare handlinger i overensstemmelse med EU-retten. I henhold til artikel 346 i TEUF er ingen medlemsstat forpligtet til at meddele oplysninger, hvis udbredelse efter dens opfattelse ville stride mod dens væsentlige sikkerhedsinteresser. I den forbindelse er nationale regler og EU-regler om beskyttelse af fortrolige oplysninger, hemmeligholdelsesaftaler og uformelle hemmeligholdelsesaftaler, f.eks. Traffic Light Protocol[14], af betydning.

(7) Med ophævelsen af direktiv (EU) 2016/1148 bør anvendelsesområdet for de enkelte sektorer udvides til at omfatte en større del af økonomien i lyset af overvejelserne i betragtning 4-6. De sektorer, der er omfattet af direktiv (EU) 2016/1148, bør derfor udvides til at omfatte sektorer og tjenesteydelser af vital betydning for vigtige samfundsmæssige og økonomiske aktiviteter i det indre marked. Reglerne bør ikke være forskellige, alt efter om enhederne er operatører af væsentlige tjenester eller udbydere af digitale tjenester. Denne differentiering har vist sig at være forældet, da den ikke afspejler sektorernes eller tjenesteydelsernes reelle betydning for de samfundsmæssige og økonomiske aktiviteter i det indre marked.

(8) I overensstemmelse med direktiv (EU) 2016/1148 havde medlemsstaterne ansvaret for at afgøre, hvilke enheder der opfylder kriterierne for at blive betragtet som operatører af væsentlige tjenester ("identifikationsproces"). For at fjerne de store forskelle mellem medlemsstaterne i denne henseende og garantere retssikkerhed med hensyn til risikostyringskravene og underretningsforpligtelserne for alle relevante enheder bør der fastsættes et ensartet kriterium for, hvilke enheder der er omfattet af dette direktivs anvendelsesområde. Dette kriterium bør bestå i anvendelsen af reglen om størrelsesloftet, ifølge hvilken alle mellemstore og store virksomheder, som omhandlet i Kommissionens henstilling 2003/361/EF[15], som opererer inden for de sektorer eller leverer den type tjenester, der er omfattet af dette direktiv, er omfattet af direktivets anvendelsesområde. Medlemsstaterne bør ikke være forpligtet til at opstille en liste over de enheder, der opfylder dette generelt gældende størrelsesrelaterede kriterium.

(9) Små enheder eller mikroenheder, der opfylder visse kriterier, som indikerer, at de spiller en central rolle for medlemsstaternes økonomier eller samfund eller for bestemte sektorer eller typer af tjenesteydelser, bør dog også være omfattet af dette direktiv. Medlemsstaterne bør være ansvarlige for at opstille en liste over sådanne enheder og forelægge den for Kommissionen.

(10) Kommissionen kan i samarbejde med samarbejdsgruppen udstede retningslinjer for gennemførelsen af de kriterier, der gælder for mikrovirksomheder og små virksomheder.

(11) Afhængigt af hvilken sektor de opererer i, eller hvilken type tjeneste de leverer, bør de enheder, der er omfattet af dette direktiv, inddeles i to kategorier: væsentlige og vigtige. Denne kategorisering bør tage hensyn til sektorens eller tjenesteydelsens kritiske betydning samt graden af afhængighed af andre sektorer eller typer af tjenester. Både væsentlige og vigtige enheder bør være underlagt de samme

---

[14] Traffic Light Protocol (TLP) giver en person, der deler oplysninger, mulighed for at informere sit publikum om eventuelle begrænsninger for videreformidlingen af disse oplysninger. Den anvendes i næsten alle CSIRT-fællesskaber samt visse informationsanalyse- og informationsdelingscentre (ISAC'er).

[15] Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder (EUT L 124 af 20.5.2003, s. 36).

risikostyringskrav og rapporteringsforpligtelser. Tilsyns- og sanktionsordningerne bør differentieres mellem disse to kategorier af enheder for at sikre en rimelig balance mellem krav og forpligtelser på den ene side og den administrative byrde, der følger af tilsynet med overholdelsen, på den anden side.

(12) Sektorspecifik lovgivning og sektorspecifikke instrumenter kan bidrage til at sikre et højt cybersikkerhedsniveau, samtidig med at der fuldt ud tages hensyn til disse sektorers særlige og komplekse karakter. Hvis en sektorspecifik EU-retsakt kræver, at væsentlige eller vigtige enheder vedtager foranstaltninger til håndtering af cybersikkerhedsrisici eller foretager underretninger om hændelser eller væsentlige cybertrusler med en virkning, der mindst svarer til de forpligtelser, der er fastsat i dette direktiv, bør disse sektorspecifikke bestemmelser, herunder om tilsyn og håndhævelse, finde anvendelse. Kommissionen kan udstede retningslinjer for gennemførelsen af lex specialis. Dette direktiv udelukker ikke vedtagelsen af yderligere sektorspecifikke EU-retsakter vedrørende foranstaltninger til håndtering af cybersikkerhedsrisici og hændelsesunderretninger. Dette direktiv berører ikke de eksisterende gennemførelsesbeføjelser, der er tillagt Kommissionen inden for en række sektorer, herunder transport og energi.

(13) Europa-Parlamentets og Rådets forordning XXXX/XXXX[16] bør betragtes som en sektorspecifik EU-retsakt i forbindelse med dette direktiv for så vidt angår enheder i den finansielle sektor. Bestemmelserne i forordning XXXX/XXXX om risikostyringsforanstaltninger vedrørende informations- og kommunikationsteknologi (IKT), håndtering af IKT-relaterede hændelser og navnlig underretning om hændelser samt om afprøvning af digital operationel modstandsdygtighed, informationsdeling og IKT-tredjepartsrisiko bør finde anvendelse i stedet for bestemmelserne i dette direktiv. Medlemsstaterne bør derfor ikke anvende bestemmelserne i dette direktiv om forpligtelser til risikostyring og rapportering vedrørende cybersikkerhed, informationsdeling samt tilsyn og håndhævelse på finansielle enheder, der er omfattet af forordning XXXX/XXXX. Samtidig er det vigtigt at opretholde stærke forbindelser og udveksle oplysninger med den finansielle sektor i henhold til dette direktiv. Med henblik herpå giver forordning XXXX/XXXX alle finansielle tilsynsmyndigheder, de europæiske tilsynsmyndigheder (ESA'er) for den finansielle sektor og de nationale kompetente myndigheder i henhold til forordning XXXX/XXXX mulighed for at deltage i strategiske politiske drøftelser og teknisk arbejde i samarbejdsgruppen samt udveksle oplysninger og samarbejde med de centrale kontaktpunkter, der er udpeget i henhold til dette direktiv, og med de nationale CSIRT'er. De kompetente myndigheder i henhold til forordning XXXX/XXXX bør også fremsende oplysninger om større IKT-relaterede hændelser til de centrale kontaktpunkter, der er udpeget i henhold til dette direktiv. Desuden bør medlemsstaterne fortsat medtage den finansielle sektor i deres cybersikkerhedsstrategier, og nationale CSIRT'er kan dække den finansielle sektor i deres aktiviteter.

(14) I betragtning af de indbyrdes forbindelser mellem cybersikkerhed og enheders fysiske sikkerhed bør der sikres en sammenhængende tilgang mellem Europa-Parlamentets og Rådets direktiv (EU) XXX/XXX[17] og dette direktiv. Med henblik herpå bør medlemsstaterne sikre, at kritiske enheder og tilsvarende enheder i henhold til direktiv

---

16 *[insert the full title and OJ publication reference when known (indsæt den fulde titel og EUT-reference, når den kendes)]*.

17 *[insert the full title and OJ publication reference when known (indsæt den fulde titel og EUT-reference, når den kendes)]*.

(EU) XXX/XXX betragtes som væsentlige enheder i henhold til dette direktiv. Medlemsstaterne bør også sikre, at deres cybersikkerhedsstrategier skaber en politisk ramme for øget koordinering mellem den kompetente myndighed i henhold til dette direktiv og den kompetente myndighed i henhold til direktiv (EU) XXX/XXX i forbindelse med udveksling af oplysninger om hændelser og cybertrusler og udøvelse af tilsynsopgaver. Myndigheder i henhold til begge direktiver bør samarbejde og udveksle oplysninger, navnlig i forbindelse med identifikation af kritiske enheder, cybertrusler, cybersikkerhedsrisici, hændelser, der påvirker kritiske enheder, samt om de cybersikkerhedsforanstaltninger, der træffes af kritiske enheder. Efter anmodning fra kompetente myndigheder i henhold til direktiv (EU) XXX/XXX bør kompetente myndigheder i henhold til dette direktiv have mulighed for at udøve deres tilsyns- og håndhævelsesbeføjelser over for en væsentlig enhed, der er udpeget som kritisk. Begge myndigheder bør samarbejde og udveksle oplysninger med henblik herpå.

(15) Opretholdelse og bevarelse af et pålideligt, modstandsdygtigt og sikkert domænenavnesystem (DNS) er en afgørende faktor for at bevare internettets integritet og er afgørende for dets fortsatte og stabile drift, som den digitale økonomi og det digitale samfund er afhængige af. Derfor bør dette direktiv finde anvendelse på alle udbydere af DNS-tjenester i DNS-oversættelseskæden, herunder operatører af rodnavneservere, navneservere for topdomæner (TLD), autoritative navneservere til domænenavne og rekursive resolvere.

(16) Cloud computing-tjenester bør omfatte tjenester, der giver mulighed for on demand-adgang og bred fjernadgang til en skalerbar og elastisk pulje af delelige og distribuerede computerressourcer. Disse computerressourcer omfatter ressourcer såsom netværk, servere og anden infrastruktur, operativsystemer, software, lagring, applikationer og tjenester. Ibrugtagningsmodellerne for cloud computing bør omfatte privat, samfundsmæssig, offentlig og hybrid cloud. Ovennævnte tjeneste- og ibrugtagningsmodeller har samme betydning som de tjeneste- og ibrugtagningsmodeller, der er defineret i ISO/IEC 17788: 2014-standarden. Cloud computing-brugerens mulighed for ensidigt selvforsynende databehandlingskapacitet, såsom servertid eller netlagring, uden nogen menneskelig interaktion fra udbyderen af cloud computing-tjenesters side, kan beskrives som on demand-administration. Udtrykket "bred fjernadgang" anvendes til at beskrive, at cloud-kapaciteten leveres over nettet og tilgås gennem mekanismer, der fremmer brugen af heterogene tynde eller tykke klientplatforme (herunder mobiltelefoner, tablets, bærbare computere og arbejdsstationer). Udtrykket "skalerbar" henviser til databehandlingsressourcer, der fordeles fleksibelt af udbyderen af cloud computing-tjenester, uanset ressourcernes geografiske placering, med henblik på at håndtere udsving i efterspørgslen. Udtrykket "elastisk pulje" bruges til at beskrive de IT-ressourcer, der tilvejebringes og stilles til rådighed alt efter efterspørgslen for hurtigt at øge eller mindske de tilgængelige ressourcer alt efter arbejdsbyrden. Udtrykket "delbar" bruges til at beskrive de IT-ressourcer, der leveres til flere brugere, som deler en fælles adgang til tjenesten, men hvor databehandlingen foretages særskilt for hver bruger, selv om tjenesten leveres fra samme elektroniske udstyr. Udtrykket "distribueret" anvendes til at beskrive de databehandlingsressourcer, der befinder sig på forskellige netforbundne computere eller enheder, og som kommunikerer og koordinerer indbyrdes ved at sende meddelelser.

(17) I lyset af fremkomsten af innovative teknologier og nye forretningsmodeller forventes nye udrulnings- og tjenestemodeller for cloud computing at dukke op på markedet som reaktion på nye kundebehov. I denne forbindelse kan cloud computing-tjenester

leveres i en meget distribueret form, endnu tættere på de steder, hvor dataene genereres eller indsamles, hvorved man bevæger sig væk fra den traditionelle model og i retning af en meget distribueret model ("edge computing").

(18) Tjenester, der udbydes af datacentertjenesteudbydere, leveres ikke altid i form af cloud computing-tjenester. Datacentre udgør derfor ikke altid en del af cloud computing-infrastrukturen. For at styre alle de risici, der er forbundet med sikkerheden i net- og informationssystemer, bør dette direktiv også omfatte udbydere af sådanne datacentertjenester, som ikke er cloud computing-tjenester. I dette direktiv bør begrebet "datacentertjeneste" omfatte levering af en tjeneste, der omfatter strukturer eller grupper af strukturer, som er beregnet til central indkvartering, sammenkobling og drift af informationsteknologi og netværksudstyr, der leverer datalagrings-, behandlings- og transporttjenester, samt alle faciliteter og infrastrukturer til energidistribution og miljøkontrol. Begrebet "datacentertjeneste" finder ikke anvendelse på interne datacentre, der ejes og drives af den pågældende enhed til eget brug.

(19) Udbydere af posttjenester som omhandlet i Europa-Parlamentets og Rådets direktiv 97/67/EF[18] samt udbydere af ekspres- og kurertjenester bør være omfattet af dette direktiv, hvis de leverer mindst ét led i postbefordringskæden og navnlig indsamling, sortering eller omdeling, herunder afhentning. Transporttjenester, der ikke udføres i forbindelse med et af disse trin, bør falde uden for posttjenesternes anvendelsesområde.

(20) Denne voksende indbyrdes afhængighed er resultatet af et stadig mere grænseoverskridende og indbyrdes afhængighedsskabende net af tjenester, der anvender centrale infrastrukturer i hele Unionen inden for sektorerne energi, transport, digital infrastruktur, drikkevand og spildevand, sundhed, visse aspekter af den offentlige forvaltning samt rummet, for så vidt som leveringen af visse tjenester, der er afhængige af jordbaserede infrastrukturer, som ejes, forvaltes og drives enten af medlemsstaterne eller af private parter, derfor ikke omfatter infrastruktur, der ejes, forvaltes eller drives af eller på vegne af Unionen som en del af dens rumprogrammer. Disse indbyrdes afhængighedsforhold betyder, at enhver afbrydelse, selv en, der oprindeligt var begrænset til én enhed eller én sektor, kan have kaskadevirkninger mere generelt, hvilket potentielt kan føre til vidtrækkende og langvarige negative virkninger for leveringen af tjenester i hele det indre marked. Covid-19-pandemien har vist, at vores stadig mere indbyrdes afhængige samfund er sårbare over for risici med lav sandsynlighed.

(21) I betragtning af forskellene i de nationale forvaltningsstrukturer og for at beskytte allerede eksisterende sektorspecifikke ordninger eller Unionens tilsyns- og tilsynsorganer bør medlemsstaterne kunne udpege mere end én national kompetent myndighed, der er ansvarlig for at udføre de opgaver, som er forbundet med sikkerheden i væsentlige og vigtige enheders net- og informationssystemer i henhold til dette direktiv. Medlemsstaterne bør kunne tildele en eksisterende myndighed denne rolle.

(22) For at lette grænseoverskridende samarbejde og kommunikation mellem myndigheder og muliggøre en effektiv gennemførelse af dette direktiv er det nødvendigt, at hver

[18] Europa-Parlamentets og Rådets direktiv 97/67/EF af 15. december 1997 om fælles regler for udvikling af Fællesskabets indre marked for posttjenester og forbedring af disse tjenesters kvalitet (EFT L 15 af 21.1.1998, s. 14).

medlemsstat udpeger et nationalt centralt kontaktpunkt med ansvar for koordinering af spørgsmål vedrørende sikkerheden i net- og informationssystemer og grænseoverskridende samarbejde på EU-plan.

(23) De kompetente myndigheder eller CSIRT'erne bør modtage anmeldelser af hændelser fra enheder på en effektiv måde. De centrale kontaktpunkter bør have til opgave at videresende anmeldelser af hændelser til de centrale kontaktpunkter i andre berørte medlemsstater. Inden for medlemsstaternes myndigheder bør de centrale kontaktpunkter for at sikre, at der forefindes et enkelt kontaktpunkt i hver medlemsstat, også være adressaterne for relevante oplysninger om hændelser vedrørende enheder i den finansielle sektor fra de kompetente myndigheder i henhold til forordning XXXX/XXXX, som de i givet fald bør kunne fremsende til de relevante nationale kompetente myndigheder eller CSIRT'er i henhold til dette direktiv.

(24) Medlemsstaterne bør være udstyret med både tilstrækkelig teknisk og organisatorisk kapacitet til at forebygge, detektere, reagere på og afhjælpe hændelser og risici i net- og informationssystemer. Medlemsstaterne bør derfor sikre sig, at de har velfungerende CSIRT'er, også kendt som IT-beredskabsenheder ("CERT'er"), som opfylder de væsentlige krav med henblik for at sikre effektive og kompatible kapaciteter til at reagere på hændelser og risici og til sikre et effektivt samarbejde på EU-plan. Med henblik på at styrke tillidsforholdet mellem enhederne og CSIRT'erne bør medlemsstaterne i tilfælde, hvor en CSIRT er en del af den kompetente myndighed, overveje en funktionel adskillelse mellem CSIRT'ernes operationelle opgaver, navnlig i forbindelse med udveksling af oplysninger og støtte til enhederne, og de kompetente myndigheders tilsynsaktiviteter.

(25) For så vidt angår personoplysninger bør CSIRT'er i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2016/679[19] for så vidt angår personoplysninger på vegne af og efter anmodning fra en enhed i henhold til dette direktiv være i stand til at foretage en proaktiv scanning af de net- og informationssystemer, der anvendes til levering af deres tjenester. Medlemsstaterne bør tilstræbe at sikre et ensartet niveau af teknisk kapacitet for alle sektorspecifikke CSIRT'er. Medlemsstaterne kan anmode Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) om bistand til at udvikle nationale CSIRT'er.

(26) I betragtning af betydningen af internationalt samarbejde om cybersikkerhed bør CSIRT'er kunne deltage i internationale samarbejdsnetværk i tillæg til de CSIRT-netværk, der er oprettet ved dette direktiv.

(27) I overensstemmelse med bilaget til Kommissionens henstilling (EU) 2017/1548 om koordineret reaktion på store cybersikkerhedshændelser og -kriser ("planen")[20] skal en væsentlig hændelse forstås som en hændelse med en betydelig indvirkning på mindst to medlemsstater, eller hvis forstyrrende virkninger overstiger en medlemsstats kapacitet til at reagere på den. Alt efter årsag og virkning kan væsentlige hændelser eskalere og udvikle sig til fuldgyldige kriser, der forhindrer det indre markeds korrekte funktion. I betragtning af sådanne begivenheders vidtrækkende omfang og i de fleste

[19] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1).

[20] Kommissionens henstilling (EU) 2017/1584 af 13. september 2017 om en koordineret reaktion på væsentlige cybersikkerhedshændelser og -kriser (EUT L 239 af 19.9.2017, s. 36).

tilfælde grænseoverskridende karakter bør medlemsstaterne og relevante EU-institutioner, -organer og -agenturer samarbejde på teknisk, operationelt og politisk plan for at koordinere indsatsen i hele Unionen.

(28) Eftersom udnyttelsen af sårbarheder i net- og informationssystemer kan forårsage betydelige forstyrrelser og skader, er hurtig identifikation og afhjælpning af disse sårbarheder en vigtig faktor med hensyn til at reducere cybersikkerhedsrisikoen. Enheder, der udvikler sådanne systemer, bør derfor indføre passende procedurer til håndtering af sårbarheder, når de opdages. Da sårbarheder ofte opdages og indberettes (afsløres) af tredjeparter (underrettende enheder), bør producenten eller udbyderen af IKT-produkter eller -tjenester også indføre de nødvendige procedurer for modtagelse af sårbarhedsoplysninger fra tredjeparter. I denne forbindelse indeholder de internationale standarder ISO/IEC 30111 og ISO/IEC 29417 vejledning om henholdsvis håndtering af sårbarheder og offentliggørelse af sårbarheder. Hvad angår oplysninger om sårbarheder er koordinering mellem de underrettende enheder og producenter eller udbydere af IKT-produkter eller -tjenester særlig vigtig. Koordineret offentliggørelse af sårbarheder angiver en struktureret proces, hvorigennem sårbarheder indberettes til organisationer på en måde, der gør det muligt for organisationen at diagnosticere og afhjælpe sårbarheden, inden detaljerede sårbarhedsoplysninger videregives til tredjeparter eller offentligheden. Koordineret offentliggørelse af sårbarheder bør også omfatte koordinering mellem den underrettende enhed og organisationen med hensyn til tidspunktet for afhjælpning og offentliggørelse af sårbarheder.

(29) Medlemsstaterne bør derfor træffe foranstaltninger til at fremme koordineret offentliggørelse af sårbarheder ved at fastlægge en relevant national politik. I denne forbindelse bør medlemsstaterne udpege en CSIRT til at påtage sig rollen som "koordinator", der fungerer som formidler mellem de underrettende enheder og producenter eller udbydere af IKT-produkter eller -tjenester, hvor det er nødvendigt. CSIRT-koordinatorens opgaver bør navnlig omfatte identifikation af og kontakt til berørte enheder, støtte til underrettende enheder, forhandling af tidsfrister for offentliggørelse og håndtering af sårbarheder, der påvirker flere organisationer (offentliggørelse af sårbarheder med flere parter). Hvis sårbarheder påvirker flere producenter eller udbydere af IKT-produkter eller -tjenester, der er etableret i mere end én medlemsstat, bør de udpegede CSIRT'er fra hver af de berørte medlemsstater samarbejde inden for CSIRT-netværket.

(30) Adgang til korrekte og rettidige oplysninger om sårbarheder, der påvirker IKT-produkter og -tjenester, bidrager til en forbedret risikostyring i forbindelse med cybersikkerhed. I denne henseende er kilder til offentligt tilgængelige oplysninger om sårbarheder et vigtigt redskab for enheder og deres brugere, men også for nationale kompetente myndigheder og CSIRT'er. Derfor bør ENISA oprette et sårbarhedsregister, hvor væsentlige og vigtige enheder og deres leverandører samt enheder, der ikke er omfattet af dette direktivs anvendelsesområde, på frivillig basis kan afsløre sårbarheder og fremlægge de sårbarhedsoplysninger, der gør det muligt for brugerne at træffe passende afhjælpende foranstaltninger.

(31) Selv om der findes lignende sårbarhedsregistre eller -databaser, hostes og vedligeholdes disse af enheder, der ikke er etableret i Unionen. Et europæisk sårbarhedsregister, der føres af ENISA, vil give større gennemsigtighed med hensyn til offentliggørelsesprocessen, inden sårbarheden offentliggøres officielt, og modstandsdygtighed i tilfælde af forstyrrelser eller afbrydelser af leveringen af tilsvarende tjenester. For at undgå dobbeltarbejde og tilstræbe komplementaritet i

videst muligt omfang bør ENISA undersøge muligheden for at indgå strukturerede samarbejdsaftaler med lignende registre i tredjelandes jurisdiktioner.

(32) Samarbejdsgruppen bør hvert andet år udarbejde et arbejdsprogram, der omfatter de foranstaltninger, som gruppen skal gennemføre for at nå sine mål og udføre sine opgaver. Tidsrammen for det første program, der vedtages i henhold til dette direktiv, bør tilpasses tidsrammen for det sidste program, der er vedtaget i henhold til direktiv (EU) 2016/1148, for at undgå potentielle afbrydelser af gruppens arbejde.

(33) Når samarbejdsgruppen udarbejder vejledningsdokumenter, bør den konsekvent: kortlægge nationale løsninger og erfaringer, vurdere virkningen af samarbejdsgruppens resultater på nationale tilgange, drøfte gennemførelsesudfordringer og formulere specifikke anbefalinger, der skal tackles gennem bedre gennemførelse af eksisterende regler.

(34) Samarbejdsgruppen bør fortsat være et fleksibelt forum og være i stand til at reagere på skiftende og nye politiske prioriteter og udfordringer, samtidig med at der tages hensyn til de disponible ressourcer. Den bør tilrettelægge regelmæssige fælles møder med relevante private interessenter fra hele Unionen for at drøfte gruppens aktiviteter og indsamle input om nye politiske udfordringer. For at styrke samarbejdet på EU-plan bør gruppen overveje at indbyde de EU-organer og -agenturer, der er involveret i cybersikkerhedspolitikken, såsom Det Europæiske Center til Bekæmpelse af IT-Kriminalitet (EC3), Den Europæiske Unions Luftfartssikkerhedsagentur (EASA) og Den Europæiske Unions Agentur for Rumprogrammet (EUSPA), til at deltage i dets arbejde.

(35) De kompetente myndigheder og CSIRT'er bør have beføjelse til at deltage i udvekslingsordninger for embedsmænd fra andre medlemsstater for at forbedre samarbejdet. De kompetente myndigheder bør træffe de foranstaltninger, der er nødvendige for at sætte embedsmænd fra andre medlemsstater i stand til at spille en effektiv rolle i den kompetente myndigheds aktiviteter.

(36) Unionen bør, hvor det er relevant, i overensstemmelse med artikel 218 i TEUF indgå internationale aftaler med tredjelande eller internationale organisationer, som giver disse mulighed for og tilrettelægger deres deltagelse i nogle af samarbejdsgruppens aktiviteter og CSIRT-netværket. Sådanne aftaler bør sikre tilstrækkelig databeskyttelse.

(37) Medlemsstaterne bør bidrage til oprettelsen af EU's krisereaktionsramme for cybersikkerhed som fastsat i henstilling (EU) 2017/1584 gennem de eksisterende samarbejdsnetværk, navnlig netværket af cyberkrisecentre (EU-CyCLONe), CSIRT-netværket og samarbejdsgruppen. EU-CyCLONe og CSIRT-netværket bør samarbejde på grundlag af proceduremæssige ordninger, der fastlægger de nærmere bestemmelser for dette samarbejde. EU-CyCLONe's forretningsorden bør yderligere præcisere, hvordan netværket skal fungere, herunder, men ikke begrænset til, roller, samarbejdsmetoder, interaktion med andre relevante aktører og modeller for informationsudveksling samt kommunikationsmidler. Med hensyn til krisestyring på EU-plan bør de relevante parter være afhængige af de integrerede ordninger for politisk kriserespons (IPCR). Kommissionen bør anvende den tværsektorielle krisekoordinationsproces på højt niveau i ARGUS til dette formål. Hvis krisen har en vigtig ekstern dimension eller berører den fælles sikkerheds- og forsvarspolitik (FSFP), bør EU-Udenrigstjenestens krisereaktionsmekanisme (CRM) aktiveres.

(38) I dette direktiv henviser udtrykket "risiko" til risikoen for tab eller afbrydelse som følge af en cybersikkerhedshændelse og bør udtrykkes som en kombination af omfanget af et sådant tab eller en sådan afbrydelse og sandsynligheden for, at hændelsen indtræffer.

(39) I dette direktiv forstås udtrykket "nærvedhændelse" som en begivenhed, der potentielt kunne have forvoldt skade, men hvor det lykkedes at forhindre, at den indtraf fuldt ud.

(40) Risikostyringsforanstaltninger bør omfatte foranstaltninger til at identificere alle risici for hændelser, forebygge, detektere og håndtere hændelser og begrænse deres konsekvenser. Sikkerheden i net- og informationssystemer bør omfatte sikkerheden for lagrede, overførte og behandlede data.

(41) Med henblik på at undgå, at operatører af væsentlige og vigtige enheder pålægges en uforholdsmæssig stor økonomisk og administrativ byrde, bør kravene til risikohåndtering stå i et rimeligt forhold til den risiko, der er forbundet med det pågældende net- og informationssystem, under hensyntagen til sådanne foranstaltningers aktuelle stade.

(42) Væsentlige og vigtige enheder bør garantere sikkerheden i de net- og informationssystemer, som de anvender i forbindelse med deres aktiviteter. Der er primært tale om private net- og informationssystemer, der forvaltes af deres interne IT-personale, eller hvis sikkerhed er blevet outsourcet. Kravene til risikostyring og rapportering vedrørende cybersikkerhed i henhold til dette direktiv bør finde anvendelse på de relevante væsentlige og vigtige enheder, uanset om de udfører vedligeholdelsen af deres net- og informationssystemer internt eller outsourcer den.

(43) Håndtering af cybersikkerhedsrisici, der stammer fra en enheds forsyningskæde og dens forhold til sine leverandører, er særlig vigtig i betragtning af udbredelsen af hændelser, hvor enheder er blevet ofre for cyberangreb, og hvor ondsindede aktører har været i stand til at bringe sikkerheden i en enheds net- og informationssystemer i fare ved at udnytte sårbarheder, der påvirker tredjepartsprodukter og -tjenester. Enheder bør derfor vurdere og tage hensyn til den generelle kvalitet af deres leverandørers og tjenesteudbyderes produkter og cybersikkerhedspraksis, herunder deres sikre udviklingsprocedurer.

(44) Blandt tjenesteudbydere spiller forvaltede udbydere af sikkerhedstjenester (MSSP'er) på områder som reaktion på hændelser, penetrationstest, sikkerhedsrevisioner og konsulentbistand en særlig vigtig rolle med hensyn til at bistå enheder i deres bestræbelser på at opdage og reagere på hændelser. Disse MSSP'er har imidlertid også selv været mål for cyberangreb og udgør i kraft af deres tætte integration i operatørernes aktiviteter en særlig cybersikkerhedsrisiko. Enheder bør derfor udvise øget omhu ved udvælgelsen af en MSSP.

(45) Enheder bør også tage højde for cybersikkerhedsrisici, der stammer fra deres samspil og forbindelser med andre interessenter inden for et bredere økosystem. Navnlig bør enheder træffe passende foranstaltninger til at sikre, at deres samarbejde med akademiske institutioner og forskningsinstitutioner finder sted i overensstemmelse med deres cybersikkerhedspolitikker og følger god praksis med hensyn til sikker adgang til og formidling af oplysninger generelt og beskyttelse af intellektuel ejendom i særdeleshed. På samme måde bør enhederne i betragtning af dataenes betydning og værdi for enhedernes aktiviteter, træffe alle passende cybersikkerhedsforanstaltninger, når de benytter sig af datatransformations- og dataanalysetjenester fra tredjeparter.

(46) For yderligere at håndtere centrale risici i forsyningskæden og bistå enheder, der opererer i sektorer, som er omfattet af dette direktiv, med at håndtere cybersikkerhedsrisici i forsyningskæden og vedrørende leverandører hensigtsmæssigt, bør samarbejdsgruppen, der involverer relevante nationale myndigheder, i samarbejde med Kommissionen og ENISA foretage koordinerede sektorbaserede risikovurderinger af forsyningskæden, som det allerede er sket for 5G-net i henhold til henstilling (EU) 2019/534 om cybersikkerhed i 5G-net[21] med henblik på inden for hver enkelt sektor at identificere de kritiske IKT-tjenester, -systemer eller -produkter, relevante trusler og sårbarheder.

(47) Ved risikovurderingen af forsyningskæden bør der i lyset af kendetegnene ved den pågældende sektor tages hensyn til både tekniske og, hvor det er relevant, ikketekniske faktorer, herunder dem, der er defineret i henstilling (EU) 2019/534, i den EU-dækkende koordinerede risikovurdering af 5G-netsikkerhed og i EU-værktøjskassen om 5G-cybersikkerhed, som samarbejdsgruppen er nået til enighed om. For at udpege de forsyningskæder, der bør gøres til genstand for en koordineret risikovurdering, bør følgende kriterier tages i betragtning: i) i hvilket omfang væsentlige og vigtige enheder anvender og er afhængige af specifikke kritiske IKT-tjenester, -systemer eller -produkter, ii) relevansen af specifikke kritiske IKT-tjenester, -systemer eller -produkter til udførelse af kritiske eller følsomme funktioner, herunder behandling af personoplysninger, iii) adgangen til alternative IKT-tjenester, -systemer eller -produkter, iv) modstandsdygtigheden i den samlede forsyningskæde for IKT-tjenester, -systemer eller -produkter over for afbrydelser og v) for nye IKT-tjenester, -systemer eller -produkter, deres potentielle fremtidige betydning for enhedernes aktiviteter.

(48) For at strømline de retlige forpligtelser, der pålægges udbydere af offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester og tillidstjenesteydere i forbindelse med sikkerheden i deres net- og informationssystemer, og for at gøre det muligt for disse enheder og deres respektive kompetente myndigheder at drage fordel af de retlige rammer, der er fastsat i dette direktiv (herunder udpegelse af en CSIRT, der er ansvarlig for risiko- og hændelseshåndtering, kompetente myndigheders og organers deltagelse i samarbejdsgruppens og CSIRT-netværkets arbejde), bør de være omfattet af dette direktivs anvendelsesområde. De tilsvarende bestemmelser i Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014[22] og Europa-Parlamentets og Rådets direktiv (EU) 2018/1972[23] vedrørende indførelse af sikkerhedskrav og underretningspligt for disse typer enheder bør derfor ophæves. Reglerne om rapporteringsforpligtelser bør ikke berøre forordning (EU) 2016/679 og Europa-Parlamentets og Rådets direktiv 2002/58/EF[24].

(49) Hvor det er hensigtsmæssigt og for at undgå unødige afbrydelser, bør de kompetente myndigheder med ansvar for tilsyn og håndhævelse fortsat anvende eksisterende

---

21 Kommissionens henstilling (EU) 2019/534 af 26. marts 2019 Cybersikkerheden i forbindelse med 5G-net (EUT L 88 af 29.3.2019, s. 42).

22 Europa-Parlamentets og Rådets forordning (EU) nr. 910/2014 af 23. juli 2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked og om ophævelse af direktiv 1999/93/EF (EUT L 257 af 28.8.2014, s. 73).

23 Europa-Parlamentets og Rådets direktiv (EU) 2018/1972 af 11. december 2018 om oprettelse af en europæisk kodeks for elektronisk kommunikation (EUT L 321 af 17.12.2018, s. 36).

24 Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37).

nationale retningslinjer og national lovgivning, der er vedtaget med henblik på gennemførelse af reglerne vedrørende sikkerhedsforanstaltninger i artikel 40, stk. 1, i direktiv (EU) 2018/1972, samt af kravene i artikel 40, stk. 2, i nævnte direktiv om parametre vedrørende en hændelses indvirkning.

(50) I betragtning af nummeruafhængige interpersonelle kommunikationstjenesters stigende betydning er det nødvendigt at sikre, at sådanne tjenester også er omfattet af passende sikkerhedskrav i lyset af deres særlige karakter og økonomiske betydning. Leverandører af sådanne tjenester bør således også garantere et sikkerhedsniveau for net- og informationssystemer, der står i forhold til risikoen. Da udbydere af nummeruafhængige interpersonelle kommunikationstjenester normalt ikke udøver egentlig kontrol over transmissionen af signaler via net, kan risikoen i forbindelse med disse tjenester i visse henseender anses for at være lavere end i forbindelse med traditionelle elektroniske kommunikationstjenester. Det samme gælder interpersonelle kommunikationstjenester, der anvender numre, og som ikke udøver faktisk kontrol over signaltransmission.

(51) Det indre marked er mere afhængigt af internettets funktion end nogensinde før. Næsten alle væsentlige og vigtige enheders tjenester er afhængige af tjenester, der leveres over internettet. For at sikre en problemfri levering af tjenester, der udbydes af væsentlige og vigtige enheder, er det vigtigt, at offentlige elektroniske kommunikationsnet, som f.eks. internetbasisnettet eller undersøiske kommunikationskabler, har indført passende cybersikkerhedsforanstaltninger og foretager underretninger om hændelser i forbindelse hermed.

(52) Hvor det er relevant, bør enheder underrette deres tjenestemodtagere om særlige og væsentlige trusler og om de foranstaltninger, de kan træffe for at afbøde den deraf følgende risiko for dem selv. Kravet om at underrette disse modtagere om sådanne trusler bør ikke fritage enhederne for forpligtelsen til for egen regning at træffe passende og øjeblikkelige foranstaltninger til at forebygge eller afhjælpe eventuelle cybertrusler og genoprette tjenestens normale sikkerhedsniveau. Sådanne oplysninger om sikkerhedstrusler bør stilles gratis til rådighed for modtagerne.

(53) Det gælder navnlig, at udbydere af offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester bør informere modtagerne af tjenesten om særlige og væsentlige trusler og om, hvordan de kan sikre deres kommunikation, f.eks. ved at anvende bestemte typer software eller krypteringsteknologier.

(54) For at beskytte sikkerheden i elektroniske kommunikationsnet og -tjenester bør brugen af kryptering, navnlig end-to-end-kryptering, fremmes og om nødvendigt være obligatorisk for udbydere af sådanne tjenester og net i overensstemmelse med principperne om sikkerhed og privatlivsbeskyttelse gennem standardindstillinger og indbygget privatlivsbeskyttelse med henblik på artikel 18. Brugen af end-to-end-kryptering bør forenes med medlemsstaternes beføjelser til at sikre beskyttelsen af deres væsentlige sikkerhedsinteresser og den offentlige sikkerhed og til at muliggøre efterforskning, afsløring og retsforfølgning af strafbare handlinger i overensstemmelse med EU-retten. Løsninger for lovlig adgang til oplysninger i end-to-end-krypteret kommunikation bør opretholde krypteringens effektivitet med hensyn til at beskytte privatlivets fred og kommunikationssikkerheden og samtidig sikre en effektiv bekæmpelse af kriminalitet.

(55) I dette direktiv fastlægges en totrinstilgang for underretning om hændelser med henblik på at finde den rette balance mellem på den ene side hurtig indberetning, der

bidrager til at afbøde den potentielle spredning af hændelser og giver enheder mulighed for at søge støtte, og på den anden side grundig indberetning, der udleder værdifulde erfaringer af individuelle hændelser og med tiden forbedrer individuelle virksomheders og hele sektorers modstandsdygtighed over for cybertrusler. Hvis enheder bliver opmærksomme på en hændelse, bør de være forpligtet til at indsende en første underretning inden for 24 timer efterfulgt af en endelig rapport senest en måned efter. Den første underretning bør kun indeholde de oplysninger, der er strengt nødvendige for at gøre de kompetente myndigheder opmærksomme på hændelsen og give enheden mulighed for at søge bistand, hvis det er nødvendigt. En sådan underretning bør, hvor det er relevant, angive, om hændelsen formodes at være forårsaget af ulovlige eller ondsindede handlinger. Medlemsstaterne bør sikre, at kravet om at foretage denne første underretning ikke fjerner den underrettende enheds ressourcer fra aktiviteter vedrørende håndtering af hændelser, der bør prioriteres. For yderligere at forhindre, at forpligtelser til underretning om hændelser enten omdirigerer ressourcer fra håndtering af hændelser eller på anden måde kan bringe enhedernes indsats i den forbindelse i fare, bør medlemsstaterne også fastsætte, at den pågældende enhed i behørigt begrundede tilfælde og efter aftale med de kompetente myndigheder eller CSIRT'en kan afvige fra fristerne på 24 timer for den første underretning og en måned for den endelige rapport.

(56) Væsentlige og vigtige enheder befinder sig ofte i en situation, hvor en bestemt hændelse på grund af dens karakteristika skal indberettes til forskellige myndigheder som følge af underretningspligten i forskellige retsakter. Sådanne tilfælde medfører yderligere byrder og kan også føre til usikkerhed med hensyn til formatet af og procedurerne for sådanne meddelelser. Med henblik herpå og med henblik på at forenkle indberetningen af sikkerhedshændelser bør medlemsstaterne oprette *et fælles kontaktpunkt* for alle meddelelser, der kræves i henhold til dette direktiv og også i henhold til anden EU-lovgivning såsom forordning (EU) 2016/679 og direktiv 2002/58/EF. ENISA bør i samarbejde med samarbejdsgruppen udvikle fælles underretningsmodeller ved hjælp af retningslinjer, der vil forenkle og strømline de underretningsoplysninger, der kræves i henhold til EU-retten, og mindske byrderne for virksomhederne.

(57) Hvis der er mistanke om, at en hændelse har forbindelse til alvorlige kriminelle aktiviteter i henhold til EU-retten eller national ret, bør medlemsstaterne opfordre væsentlige og vigtige enheder til på grundlag af gældende strafferetsplejeregler i overensstemmelse med EU-retten at indberette hændelser af formodet alvorlig kriminel karakter til de relevante retshåndhævende myndigheder. Hvor det er relevant, og uden at det berører de regler om beskyttelse af personoplysninger, der gælder for Europol, er det ønskeligt, at EC3 og ENISA letter koordineringen mellem de kompetente myndigheder og de retshåndhævende myndigheder i forskellige medlemsstater.

(58) Personoplysninger bliver i mange tilfælde kompromitteret som følge af hændelser. I denne forbindelse bør de kompetente myndigheder samarbejde og udveksle oplysninger om alle relevante spørgsmål med databeskyttelsesmyndighederne og tilsynsmyndighederne i henhold til direktiv 2002/58/EF.

(59) Det er afgørende at vedligeholde nøjagtige og fuldstændige databaser over domænenavne og registreringsdata (såkaldte "WHOIS-data") og give lovlig adgang til sådanne data for at sikre DNS'ens sikkerhed, stabilitet og modstandsdygtighed, hvilket igen bidrager til et højt fælles cybersikkerhedsniveau i Unionen. Hvis behandlingen

omfatter personoplysninger, skal denne behandling være i overensstemmelse med EU's databeskyttelseslovgivning.

(60) Offentlige myndigheders, herunder kompetente myndigheder i henhold til EU-retten eller national ret med henblik på forebyggelse, efterforskning eller retsforfølgning af strafbare handlinger, CERT'er, CSIRT'er og for så vidt angår deres kunders data til udbydere af elektroniske kommunikationsnet og -tjenester og udbydere af cybersikkerhedsteknologier og -tjenester, der handler på vegne af disse kunder, mulighed for at tilgå og få rettidig adgang til disse data er afgørende for at forebygge og bekæmpe misbrug af domænenavnesystemet, navnlig for at forebygge, opdage og reagere på cybersikkerhedshændelser. En sådan adgang bør ske i overensstemmelse med EU's databeskyttelseslovgivning, for så vidt som den vedrører personoplysninger.

(61) For at sikre, at der er adgang til nøjagtige og fuldstændige data til registrering af domænenavne, bør topdomæneregistraturer og enheder, der leverer tjenester til registrering af domænenavne (såkaldte registratorer), indsamle og garantere integriteten og tilgængeligheden af registreringsdata for domænenavne. Topdomæneregistraturer og enheder, der leverer domænenavneregistreringstjenester for topdomænet, bør navnlig fastlægge politikker og procedurer for indsamling og vedligeholdelse af nøjagtige og fuldstændige registreringsdata samt for at forhindre og korrigere unøjagtige registreringsdata i overensstemmelse med EU's databeskyttelsesregler.

(62) Topdomæneregistraturer og enheder, der leverer tjenester til registrering af domænenavne for dem, bør offentliggøre oplysninger om registrering af domænenavne, der falder uden for anvendelsesområdet for EU's databeskyttelsesregler, såsom data, der vedrører juridiske personer[25]. Topdomæneregistraturer og enheder, der leverer domænenavneregistreringstjenester for topdomænet, bør også give legitime adgangssøgende lovlig adgang til specifikke domænenavnsregistreringsdata om fysiske personer i overensstemmelse med EU's databeskyttelseslovgivning. Medlemsstaterne bør sikre, at topdomæneregistraturer og enheder, der udbyder tjenester til registrering af domænenavne for dem, uden unødig forsinkelse besvarer anmodninger fra legitime adgangssøgende om videregivelse af oplysninger om registrering af domænenavne. Topdomæneregistraturer og de enheder, der leverer registreringstjenester for domænenavne til dem, bør fastlægge politikker og procedurer for offentliggørelse og fremlæggelse af registreringsdata, herunder serviceleveranceaftaler til behandling af anmodninger om adgang fra legitime adgangssøgende. Adgangsproceduren kan også omfatte brug af en grænseflade, en portal eller et andet teknisk værktøj til at tilvejebringe et effektivt system til anmodning om og adgang til registreringsdata. Med henblik på at fremme en harmoniseret praksis i hele det indre marked kan Kommissionen vedtage retningslinjer for sådanne procedurer, uden at dette berører Det Europæiske Databeskyttelsesråds beføjelser.

(63) Alle væsentlige og vigtige enheder i henhold til dette direktiv bør henhøre under jurisdiktionen i den medlemsstat, hvor de leverer deres tjenester. Hvis enheden leverer tjenester i mere end én medlemsstat, bør den henhøre under hver af disse

[25] Europa-Parlamentets og Rådets forordning (EU) 2016/679, betragtning 14: "Denne forordning finder ikke anvendelse på behandling af personoplysninger, der vedrører juridiske personer, navnlig virksomheder, der er etableret som juridiske personer, herunder den juridiske persons navn, form og kontaktoplysninger".

medlemsstaters særskilte og parallelle jurisdiktion. De kompetente myndigheder i disse medlemsstater bør samarbejde, yde gensidig bistand til hinanden og, hvor det er relevant, gennemføre fælles tilsynsforanstaltninger.

(64) For at tage hensyn til den grænseoverskridende karakter af DNS-tjenesteudbyderes tjenester og operationer, topdomænenavneregistraturer, udbydere af indholdsleveringsnetværk, udbydere af cloud computing-tjenester, datacentertjenesteudbydere og digitale udbydere bør kun én medlemsstat have jurisdiktion over disse enheder. Jurisdiktionen bør tillægges den medlemsstat, hvor den pågældende enhed har sit hovedsæde i Unionen. Etableringskriteriet i dette direktiv indebærer faktisk udøvelse af virksomhed gennem faste ordninger. De pågældende ordningers juridiske form, hvad enten der er tale om en filial eller et datterselskab med status som juridisk person, har ikke afgørende betydning i denne forbindelse. Dette kriterium bør ikke afhænge af, hvorvidt net- og informationssystemerne fysisk befinder sig på et givent sted. Tilstedeværelsen og anvendelsen af sådanne systemer udgør ikke i sig selv et sådant hjemsted og er derfor ikke et kriterium for fastlæggelse af hjemstedet. Hovedvirksomheden bør være det sted, hvor beslutningerne vedrørende foranstaltninger til styring af cybersikkerhedsrisikoen træffes i Unionen. Dette vil typisk svare til placeringen af selskabernes centrale administration i Unionen. Hvis sådanne beslutninger ikke træffes i Unionen, bør hovedvirksomheden anses for at befinde sig i de medlemsstater, hvor enheden har en virksomhed med det største antal ansatte i Unionen. Når tjenesterne udføres af en gruppe af virksomheder, bør den kontrollerende virksomheds hovedvirksomhed anses for at være gruppen af virksomheders hovedvirksomhed.

(65) I tilfælde, hvor en DNS-tjenesteudbyder, et topdomænenavneregistratur, en udbyder af indholdsudsendelsesnetværk, en udbyder af cloud computing-tjenester, en datacentertjenesteudbyder og en digital udbyder, der ikke er etableret i Unionen, udbyder tjenester i Unionen, bør denne udpege en repræsentant. Med henblik på at afgøre, om en sådan udbyder af digitale tjenester tilbyder tjenester i Unionen, bør det fastslås, om det er åbenbart, at udbyderen af digitale tjenester påtænker at tilbyde tjenester til personer i en eller flere medlemsstater. Alene det forhold, at der i Unionen er adgang til udbyderen af digitale tjenesters eller en mellemmands websted eller til en e-mailadresse og andre kontaktoplysninger, eller at der benyttes et sprog, som almindeligvis benyttes i det tredjeland, hvor enheden er etableret, er ikke tilstrækkeligt til at fastslå en sådan hensigt. Imidlertid kan faktorer såsom anvendelse af et sprog eller en valuta, der almindeligvis anvendes i en eller flere medlemsstater med mulighed for at bestille tjenester på det pågældende sprog, eller omtale af kunder eller brugere, der befinder sig i Unionen, gøre det åbenbart, at udbyderen af enhed påtænker at tilbyde tjenester i Unionen. Repræsentanten bør handle på vegne af enheden, og kompetente myndigheder eller CSIRT'er bør kunne kontakte repræsentanten. Repræsentanten bør udtrykkeligt udpeges ved et skriftligt mandat fra udbyderen af digitale tjenester til at handle på sidstnævntes vegne for så vidt angår sidstnævntes forpligtelser i medfør af dette direktiv, herunder underretning om hændelser.

(66) Hvis oplysninger, der betragtes som klassificerede i henhold til national ret eller EU-retten, udveksles, indberettes eller på anden måde deles i henhold til bestemmelserne i dette direktiv, bør de tilsvarende specifikke regler for håndtering af klassificerede oplysninger finde anvendelse.

(67) I takt med at cybertruslerne bliver mere komplekse og sofistikerede, er gode detektions- og forebyggelsesforanstaltninger i høj grad afhængige af regelmæssig udveksling af trussels- og sårbarhedsefterretninger mellem enheder.

Informationsudveksling bidrager til øget bevidsthed om cybertrusler, hvilket igen styrker finansielle enheders evne til at forhindre trusler i at blive til faktiske hændelser og sætter enhederne i stand til bedre at inddæmme virkningerne af hændelser og foretage en mere effektiv genopretning. Da der ikke findes nogen retningslinjer på EU-plan, synes flere faktorer at have hæmmet en sådan udveksling af efterretninger, navnlig usikkerhed om foreneligheden med databeskyttelsesregler, antitrustregler og regler om ansvar.

(68) Enheder bør tilskyndes til i fællesskab at øge deres individuelle viden og praktiske erfaring på strategisk, taktisk og operationelt plan med henblik på at styrke deres kapacitet til i tilstrækkeligt omfang at vurdere, overvåge, forsvare sig mod og reagere på cybertrusler. Det er derfor nødvendigt at gøre det muligt at etablere mekanismer på EU-plan for frivillige ordninger for udveksling af oplysninger. Med henblik herpå bør medlemsstaterne aktivt støtte og tilskynde også relevante enheder, der ikke er omfattet af dette direktivs anvendelsesområde, til at deltage i sådanne informationsudvekslingsmekanismer. Disse mekanismer bør gennemføres i fuld overensstemmelse med Unionens konkurrenceregler og EU-rettens regler om databeskyttelse.

(69) Behandling af personoplysninger, i det omfang det er strengt nødvendigt og står i et rimeligt forhold til målet om at sikre net- og informationssikkerhed hos enheder, offentlige myndigheder, CERT'er, CSIRT'er og udbydere af sikkerhedsteknologier og -tjenester, bør udgøre en legitim interesse for den pågældende dataansvarlige, jf. forordning (EU) 2016/679. Dette bør omfatte foranstaltninger vedrørende forebyggelse, opdagelse, analyse og reaktion på hændelser, foranstaltninger til at øge bevidstheden i forbindelse med specifikke cybertrusler, udveksling af oplysninger i forbindelse med afhjælpning af sårbarheder og koordineret videregivelse samt frivillig udveksling af oplysninger om disse hændelser samt cybertrusler og sårbarheder, kompromitteringsindikatorer, taktikker, teknikker og procedurer, cybersikkerhedsadvarsler og konfigurationsværktøjer. Sådanne foranstaltninger kan kræve behandling af følgende typer personoplysninger: IP-adresser, uniform resources locators (URL'er), domænenavne og e-mailadresser.

(70) For at styrke de tilsynsbeføjelser og -foranstaltninger, der bidrager til at sikre effektiv overholdelse, bør dette direktiv indeholde en minimumsliste over tilsynsforanstaltninger og -midler, hvorigennem de kompetente myndigheder kan føre tilsyn med væsentlige og vigtige enheder. Desuden bør der ved dette direktiv indføres en differentiering af tilsynsordningen mellem væsentlige og vigtige enheder med henblik på at sikre en rimelig balance mellem forpligtelser for både enheder og kompetente myndigheder. Væsentlige enheder bør derfor være underlagt en fuldt udbygget tilsynsordning (forudgående og efterfølgende), mens vigtige enheder bør være underlagt en lempelig tilsynsordning, som kun gælder efterfølgende. For sidstnævnte betyder dette, at vigtige enheder ikke systematisk bør dokumentere overholdelsen af kravene for styring af cybersikkerhedsrisici, mens de kompetente myndigheder bør anvende en reaktiv efterfølgende tilgang til tilsyn og dermed ikke have en generel forpligtelse til at føre tilsyn med disse enheder.

(71) For at gøre håndhævelsen effektiv bør der fastlægges en minimumsliste over administrative sanktioner for brud på forpligtelserne vedrørende styring af cybersikkerhedsrisici og rapportering i dette direktiv, som opstiller en klar og konsekvent ramme for sådanne sanktioner i hele Unionen. Der bør tages behørigt hensyn til overtrædelsens art, grovhed og varighed, den faktiske skade eller de lidte tab eller potentielle skader eller tab, der kunne være blevet udløst, overtrædelsens

forsætlige eller uagtsomme karakter, de foranstaltninger, der er truffet for at forebygge eller begrænse den lidte skade og/eller de lidte tab, graden af ansvar eller eventuelle relevante tidligere overtrædelser, graden af samarbejde med den kompetente myndighed og enhver anden skærpende eller formildende omstændighed. Pålæggelse af sanktioner, herunder administrative bøder, bør være omfattet af fornødne proceduremæssige garantier i overensstemmelse med de generelle principper i EU-retten og Den Europæiske Unions charter om grundlæggende rettigheder, herunder effektiv retsbeskyttelse og en retfærdig rettergang.

(72) For at sikre en effektiv håndhævelse af de forpligtelser, der er fastsat i dette direktiv, bør hver kompetent myndighed have beføjelse til at pålægge eller anmode om pålæggelse af administrative bøder.

(73) Når en virksomhed pålægges administrative bøder, forstås en virksomhed i denne forbindelse som en virksomhed som omhandlet i artikel 101 og 102 i TEUF. Når personer, der ikke er en virksomhed, pålægges administrative bøder, bør tilsynsmyndigheden i forbindelse med fastsættelsen af bødestørrelsen tage hensyn til det generelle indkomstniveau i den pågældende medlemsstat og personens økonomiske situation. Det bør være op til medlemsstaterne at bestemme, om og i hvilket omfang de offentlige myndigheder bør kunne pålægges administrative bøder. Pålæggelse af en administrativ bøde berører ikke de kompetente myndigheders anvendelse af andre beføjelser eller andre sanktioner, der er fastsat i de nationale regler til gennemførelse af dette direktiv.

(74) Medlemsstaterne bør kunne fastsætte regler om strafferetlige sanktioner for overtrædelse af de nationale regler til gennemførelse af dette direktiv. Pålæggelse af strafferetlige sanktioner for overtrædelse af sådanne nationale regler og tilknyttede administrative sanktioner bør dog ikke føre til et brud på ne bis in idem-princippet som fortolket af EU-Domstolen.

(75) Når dette direktiv ikke harmoniserer administrative sanktioner eller om nødvendigt i andre tilfælde, f.eks. i tilfælde af alvorlige overtrædelser af forpligtelser, der er fastsat i dette direktiv, bør medlemsstaterne indføre en ordning, der giver mulighed for at pålægge sanktioner, som er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning. Sanktionernes art, strafferetlige eller administrative, bør fastsættes i medlemsstaternes nationale ret.

(76) For yderligere at styrke effektiviteten og den afskrækkende virkning af de sanktioner, der finder anvendelse på overtrædelser af forpligtelser, der er fastsat i henhold til dette direktiv, bør de kompetente myndigheder have beføjelse til at anvende sanktioner, der består i at suspendere en certificering eller tilladelse vedrørende en væsentlig enheds tjenester eller dele heraf og indføre et midlertidigt forbud mod en fysisk persons udøvelse af ledelsesfunktioner. I betragtning af deres alvor og indvirkning på enhedernes aktiviteter og i sidste ende på deres forbrugere bør sådanne sanktioner kun anvendes proportionalt med overtrædelsens alvor og under hensyntagen til de særlige omstændigheder i den enkelte sag, herunder overtrædelsens forsætlige eller uagtsomme karakter, foranstaltninger, der træffes for at forebygge eller begrænse den lidte skade og/eller de lidte tab. Sådanne sanktioner bør kun anvendes som ultima ratio, dvs. kun efter at de øvrige relevante håndhævelsesforanstaltninger, der er fastsat i dette direktiv, er udtømt, og kun indtil de enheder, de pålægges, træffer de nødvendige foranstaltninger for at afhjælpe manglerne eller opfylde kravene fra den kompetente myndighed, for hvilken sådanne sanktioner er blevet anvendt. Pålæggelse af sådanne sanktioner skal være underlagt fornødne proceduremæssige garantier i

overensstemmelse med de generelle principper i EU-retten og Den Europæiske Unions charter om grundlæggende rettigheder, herunder effektiv retsbeskyttelse, retfærdig rettergang, uskyldsformodning og retten til et forsvar.

(77) Dette direktiv bør fastlægge samarbejdsregler mellem de kompetente myndigheder og tilsynsmyndighederne i overensstemmelse med forordning (EU) 2016/679 om behandling af overtrædelser vedrørende personoplysninger.

(78) Dette direktiv bør sigte mod at sikre et højt ansvarsniveau for risikohåndteringsforanstaltninger og rapporteringsforpligtelser i forbindelse med cybersikkerhed på organisationsniveau. Derfor bør ledelsesorganerne for de enheder, der er omfattet af dette direktiv, godkende foranstaltningerne vedrørende cybersikkerhedsrisici og føre tilsyn med deres gennemførelse.

(79) Der bør indføres en peerevalueringsmekanisme, som gør det muligt for eksperter udpeget af medlemsstaterne at vurdere gennemførelsen af cybersikkerhedspolitikker, herunder niveauet af medlemsstaternes kapaciteter og tilgængelige ressourcer.

(80) For at tage hensyn til nye cybertrusler, den teknologiske udvikling eller sektorspecifikke særtræk bør beføjelsen til at vedtage retsakter delegeres til Kommissionen i overensstemmelse med artikel 290 i TEUF for så vidt angår elementerne i forbindelse med de risikostyringsforanstaltninger, der kræves i henhold til dette direktiv. Kommissionen bør også tillægges beføjelser til at vedtage delegerede retsakter, der fastsætter, hvilke kategorier af væsentlige enheder der skal have en attest, og i henhold til hvilke specifikke europæiske certificeringsordninger vedrørende cybersikkerhed. Det er navnlig vigtigt, at Kommissionen gennemfører relevante høringer under sit forberedende arbejde, herunder på ekspertniveau, og at disse høringer gennemføres i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning[26]. For at sikre lige deltagelse i forberedelsen af delegerede retsakter modtager Europa-Parlamentet og Rådet navnlig alle dokumenter på samme tid som medlemsstaternes eksperter, og deres eksperter har systematisk adgang til møder i Kommissionens ekspertgrupper, der beskæftiger sig med forberedelse af delegerede retsakter.

(81) For at sikre ensartede betingelser for gennemførelsen af de relevante bestemmelser i dette direktiv vedrørende de proceduremæssige ordninger, der er nødvendige for samarbejdsgruppens funktion, de tekniske elementer vedrørende risikostyringsforanstaltninger eller typen af oplysninger, formatet og proceduren for anmeldelser af hændelser bør Kommissionen tillægges gennemførelsesbeføjelser. Disse beføjelser bør udøves i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011[27].

(82) Kommissionen bør regelmæssigt tage dette direktivs bestemmelser op til fornyet overvejelse efter høring af interesserede parter, navnlig med henblik på at afgøre, om der er behov for ændringer i lyset af skiftende samfundsmæssige, politiske eller teknologiske vilkår eller markedsvilkår.

(83) Eftersom målene for dette direktiv, nemlig at opnå et højt, fælles sikkerhedsniveau i net- og informationssystemer i Unionen, ikke i tilstrækkelig grad kan opfyldes af

[26] EUT L 123 af 12.5.2016, s. 1.

[27] Europa-Parlamentets og Rådets forordning (EU) nr. 182/2011 af 16. februar 2011 om de generelle regler og principper for, hvordan medlemsstaterne skal kontrollere Kommissionens udøvelse af gennemførelsesbeføjelser (EUT L 55 af 28.2.2011, s. 13).

medlemsstaterne, men på grund af handlingens virkninger bedre kan nås på EU-plan, kan Unionen derfor vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. artikel 5 i traktaten om Den Europæiske Union. I overensstemmelse med proportionalitetsprincippet, jf. nævnte artikel, går dette direktiv ikke videre, end hvad der er nødvendigt for at nå disse mål.

(84) Dette direktiv overholder de grundlæggende rettigheder og de principper, der anerkendes i Den Europæiske Unions charter om grundlæggende rettigheder, navnlig retten til respekt for privatlivet og kommunikation, beskyttelsen af personoplysninger, frihed til at oprette og drive egen virksomhed, ejendomsretten og retten til effektive retsmidler for en domstol og retten til at blive hørt. Direktivet bør gennemføres i overensstemmelse med disse rettigheder og principper —

VEDTAGET DETTE DIREKTIV:

KAPITEL I

Generelle bestemmelser

Artikel 1

Genstand

1. Dette direktiv fastsætter foranstaltninger med henblik på at sikre et højt fælles cybersikkerhedsniveau i Unionen.

2. Med henblik herpå gælder det for dette direktiv, at:

(a) det fastsætter forpligtelser for medlemsstaterne til at vedtage nationale cybersikkerhedsstrategier, udpege kompetente nationale myndigheder, centrale kontaktpunkter og enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er)

b) det fastsætter forpligtelser til risikostyring og underretning om cybersikkerhedsrisici for enheder af en type, der benævnes væsentlige enheder i bilag I og vigtige enheder i bilag II

(c) det fastsætter forpligtelser vedrørende udveksling af cybersikkerhedsoplysninger.

Artikel 2

Anvendelsesområde

1. Dette direktiv finder anvendelse på offentlige og private enheder af en type, der betegnes som væsentlige enheder i bilag I og som vigtige enheder i bilag II. Dette

direktiv finder ikke anvendelse på enheder, der betragtes som mikrovirksomheder og små virksomheder som omhandlet i Kommissionens henstilling 2003/361/EF[28].

2. Uanset deres størrelse finder dette direktiv dog også anvendelse på enheder, der er omhandlet i bilag I og II, hvis:

(a) tjenesterne leveres af en af følgende enheder:

i) offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester som omhandlet i bilag I, punkt 8

ii) tillidstjenester som omhandlet i bilag I, punkt 8

iii) udbydere af topdomænenavneregistre og domænenavnesystemer (DNS), jf. bilag I, punkt 8

b) enheden er en offentlig forvaltningsenhed som omhandlet i artikel 4, nr. 23)

c) enheden er den eneste tjenesteyder i en medlemsstat

d) en potentiel forstyrrelse af den tjeneste, enheden leverer, kan have indvirkning på den offentlige sikkerhed eller folkesundheden

e) en potentiel forstyrrelse af den tjeneste, der leveres af enheden, kan medføre systemiske risici, navnlig for de sektorer, hvor en sådan forstyrrelse kan have en grænseoverskridende virkning

f) enheden er kritisk på grund af dens specifikke betydning på regionalt eller nationalt plan for den pågældende sektor eller type af tjeneste eller for andre indbyrdes afhængige sektorer i medlemsstaten

g) enheden identificeres som en kritisk enhed i henhold til Europa-Parlamentets og Rådets direktiv (EU) XXXX/XXXX[29] [direktivet om kritiske enheders modstandsdygtighed] eller som en enhed svarende til en kritisk enhed i henhold til artikel 7 i nævnte direktiv.

Medlemsstaterne opstiller en liste over enheder, der er identificeret i henhold til litra b)-f), og forelægger den for Kommissionen senest [6 måneder efter gennemførelsesfristen]. Medlemsstaterne reviderer listen regelmæssigt og derefter mindst hvert andet år og ajourfører den, hvis det er relevant.

3. Dette direktiv berører ikke medlemsstaternes beføjelser til opretholdelse af den offentlige sikkerhed, forsvaret og den nationale sikkerhed i overensstemmelse med EU-retten.

4. Dette direktiv berører ikke Rådets direktiv 2008/114/EF[30] og Europa-Parlamentets og Rådets direktiv 2011/93/EU[31] og 2013/40/EU[32].

---

28 Kommissionens henstilling 2003/361/EF af 6. maj 2003 om definitionen af mikrovirksomheder, små og mellemstore virksomheder (EUT L 124 af 20.5.2003, s. 36).

29 *[insert the full title and OJ publication reference when known (indsæt den fulde titel og EUT-reference, når den kendes)]*.

30 Rådets direktiv 2008/114/EF af 8. december 2008 om indkredsning og udpegning af europæisk kritisk infrastruktur og vurdering af behovet for at beskytte den bedre (EUT L 345 af 23.12.2008, s. 75).

31 Europa-Parlamentets og Rådets direktiv 2011/93/EU af 13. december 2011 om bekæmpelse af seksuelt misbrug og seksuel udnyttelse af børn og børnepornografi og om erstatning af Rådets rammeafgørelse 2004/68/RIA (EUT L 335 af 17.12.2011, s. 1).

5. Oplysninger, der er fortrolige i henhold til EU-regler og nationale regler, som f.eks. regler om forretningshemmeligheder, udveksles med forbehold af artikel 346 i TEUF kun med Kommissionen og andre relevante myndigheder, hvis en sådan udveksling er nødvendig for anvendelsen af dette direktiv. De udvekslede oplysninger begrænses til, hvad der er relevant og forholdsmæssigt under hensyn til formålet med udvekslingen. Udvekslingen af oplysninger skal sikre de nævnte oplysningers fortrolighed og beskytte sikkerheden og de kommercielle interesser hos væsentlige eller vigtige enheder.

6. Hvis bestemmelser i sektorspecifikke EU-retsakter kræver, at væsentlige eller vigtige enheder enten vedtager risikohåndteringsforanstaltninger for cybersikkerhed eller anmelder hændelser eller væsentlige cybertrusler, og hvis disse krav har en virkning, der mindst svarer til de forpligtelser, der er fastsat i dette direktiv, finder de relevante bestemmelser i dette direktiv, herunder bestemmelsen om tilsyn og håndhævelse i kapitel VI, ikke anvendelse.

Artikel 3

Minimumsharmonisering

Uden at det berører deres øvrige forpligtelser i henhold til EU-retten, kan medlemsstaterne i overensstemmelse med dette direktiv vedtage eller opretholde bestemmelser, der sikrer et højere cybersikkerhedsniveau.

Artikel 4

Definitioner

I dette direktiv forstås ved:

1) "net- og informationssystem":

   a) et elektronisk kommunikationsnet som omhandlet i artikel 2, stk. 1, i direktiv (EU) 2018/1972

   b) enhver anordning eller gruppe af forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af digitale data

   c) digitale data, som lagres, behandles, fremfindes eller overføres af elementer i litra a) og b) med henblik på deres drift, brug, beskyttelse og vedligeholdelse

2) "sikkerhed i net- og informationssystemer": net- og informationssystemers evne til, på et givet sikkerhedsniveau, at modstå handlinger, der er til skade for tilgængeligheden, autenticiteten, integriteten eller fortroligheden i forbindelse med lagrede eller overførte eller behandlede data eller de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via disse net- og informationssystemer

---

[32] Europa-Parlamentets og Rådets direktiv 2013/40/EU af 12. august 2013 om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA (EUT L 218 af 14.8.2013, s. 8).

3) "cybersikkerhed": cybersikkerhed som omhandlet i artikel 2, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) 2019/881[33]

4) "national strategi for cybersikkerhed ": en sammenhængende ramme i en medlemsstat med strategiske mål og prioriteter for sikkerheden af net- og informationssystemer i den pågældende medlemsstat

5) "hændelse": enhver begivenhed, der bringer tilgængeligheden, autenticiteten, integriteten eller fortroligheden af lagrede, overførte eller behandlede data eller de relaterede tjenester, der tilbydes af eller er tilgængelige via net- og informationssystemer, i fare

6) "håndtering af hændelser": alle handlinger og procedurer, der tager sigte på opdagelse, analyse og inddæmning af og reaktion på en hændelse

7) "cybertrussel": en cybertrussel som omhandlet i artikel 2, stk. 8, i forordning (EU) 2019/881

8) "sårbarhed": en svaghed, følsomhed eller fejl i forbindelse med et aktiv, et system, en proces eller en kontrolfunktion, som kan udnyttes af en cybertrussel

9) "repræsentant": enhver fysisk eller juridisk person, der er etableret i Unionen, og som udtrykkeligt er udpeget til at handle på vegne af i) en DNS-tjenesteudbyder, en topdomænenavneregistratur (TLD), en udbyder af cloud computing-tjenester, en datacentertjenesteudbyder, en udbyder af indholdsudsendelsesnetværk som omhandlet i bilag I, punkt 8, eller ii) enheder som omhandlet i bilag II, punkt 6, der ikke er etableret i Unionen, og som kan kontaktes af en national kompetent myndighed eller en CSIRT i stedet for enheden i forbindelse med forpligtelserne i henhold til dette direktiv

10) "standard": en standard som omhandlet i artikel 2, stk. 1, i Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012[34]

11) "teknisk specifikation": en teknisk specifikation som omhandlet i artikel 2, stk. 4, i forordning (EU) nr. 1025/2012

12) "internetudvekslingspunkt (IXP)": en netfacilitet, der muliggør sammenkobling af mere end to uafhængige net (autonome systemer), primært med henblik på at lette udvekslingen af internettrafik Et IXP leverer kun sammenkobling for autonome systemer. Et IXP forudsætter ikke, at internettrafik, som bevæger sig mellem et givet par af deltagende autonome systemer, bevæger sig gennem et tredje autonomt system, og det hverken ændrer eller forstyrrer en sådan trafik.

13) "domænenavnesystem (DNS)": et hierarkisk distribueret navngivningssystem, der gør det muligt for slutbrugere at nå frem til tjenester og ressourcer på internettet

---

[33] Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed, om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed) (EUT L 151 af 7.6.2019, s. 15).

[34] Europa-Parlamentets og Rådets forordning (EU) nr. 1025/2012 af 25. oktober 2012 om europæisk standardisering, om ændring af Rådets direktiv 89/686/EØF og 93/15/EØF og Europa-Parlamentets og Rådets direktiv 94/9/EF, 94/25/EF, 95/16/EF, 97/23/EF, 98/34/EF, 2004/22/EF, 2007/23/EF, 2009/23/EF og 2009/105/EF og om ophævelse af Rådets beslutning 87/95/EØF og Europa-Parlamentets og Rådets afgørelse nr. 1673/2006/EF (EUT L 316 af 14.11.2012, s. 12).

14) "DNS-tjenesteudbyder": en enhed, der leverer rekreative eller autoritative domænenavnsoversættelsestjenester til internetslutbrugere og andre udbydere af DNS-tjenester

15) "topdomænenavneregistratur": en enhed, der har fået uddelegeret et specifikt topdomæne, og som er ansvarlig for at administrere topdomænet, herunder registrering af domænenavne under topdomænet og den tekniske drift af topdomænet, herunder drift af dets navneservere, vedligeholdelse af dets databaser og distribution af topdomænezonefiler på navneservere

16) "digital tjeneste": en tjeneste som omhandlet i artikel 1, stk. 1, litra b), i Europa-Parlamentets og Rådets direktiv (EU) 2015/1535[35]

17) "onlinemarkedsplads": en digital tjeneste som omhandlet i artikel 2, litra n), i Europa-Parlamentets og Rådets direktiv 2005/29/EF[36]

18) "onlinesøgemaskine": en digital tjeneste som omhandlet i artikel 2, stk. 5, i Europa-Parlamentets og Rådets forordning (EU) 2019/1150[37]

19) "cloud computing-tjeneste": en digital tjeneste, som muliggør on demand-administration og giver bred fjernadgang til en skalerbar og elastisk pulje af delbare og distribuerede databehandlingsressourcer

20) "datacentertjeneste": en tjeneste, der omfatter strukturer eller grupper af strukturer, der er dedikeret til central indkvartering, sammenkobling og drift af informationsteknologi og netværksudstyr, der leverer datalagrings-, behandlings- og transporttjenester samt alle faciliteter og infrastrukturer til strømdistribution og miljøkontrol

21) "indholdsleveringsnetværk": et net af geografisk distribuerede servere med henblik på at sikre høj tilgængelighed, adgang til eller hurtig levering af digitalt indhold og digitale tjenester til internetbrugere på vegne af indholds- og tjenesteudbydere

22) "platform for sociale netværkstjenester": en platform, der sætter slutbrugerne i stand til at forbinde, dele, opdage og kommunikere med hinanden på tværs af flere enheder, navnlig via chats, indlæg, videoer og anbefalinger

23) "offentlig forvaltningsinstans": en enhed i en medlemsstat, der opfylder følgende kriterier:

(a) den er oprettet med henblik på at opfylde almennyttige formål og har ikke industriel eller kommerciel karakter

(b) den har status som juridisk person

---

35 Europa-Parlamentets og Rådets direktiv (EU) 2015/1535 af 9. september 2015 om en informationsprocedure med hensyn til tekniske forskrifter samt forskrifter for informationssamfundets tjenester (EUT L 241 af 17.9.2015, s. 1).

36 Europa-Parlamentets og Rådets direktiv 2005/29/EF af 11. maj 2005 om virksomheders urimelige handelspraksis over for forbrugerne på det indre marked og om ændring af Rådets direktiv 84/450/EØF og Europa-Parlamentets og Rådets direktiv 97/7/EF, 98/27/EF og 2002/65/EF og Europa-Parlamentets og Rådets forordning (EF) nr. 2006/2004 (direktivet om urimelig handelspraksis) (EUT L 149 af 11.6.2005, s. 22).

37 Europa-Parlamentets og Rådets forordning (EU) 2019/1150 af 20. juni 2019 om fremme af retfærdighed og gennemsigtighed for brugere af onlineformidlingstjenester (EUT L 186 af 11.7.2019, s. 57).

(c) dens aktivitet finansieres for størstedelens vedkommende af staten, en regional myndighed eller af andre offentligretlige organer, eller den er underlagt ledelsesmæssig kontrol af disse myndigheder eller organer, eller den har et administrations-, ledelses- eller tilsynsorgan, hvor mere end halvdelen af medlemmerne udpeges af staten, regionale myndigheder eller andre offentligretlige organer

(d) den har beføjelse til at rette administrative eller lovgivningsmæssige afgørelser til fysiske eller juridiske personer, der påvirker deres rettigheder i forbindelse med grænseoverskridende bevægelighed for personer, varer, tjenesteydelser eller kapital.

Offentlige forvaltningsenheder, der udfører aktiviteter inden for områderne offentlig sikkerhed, retshåndhævelse, forsvar eller national sikkerhed, er ikke omfattet

24) "enhed": enhver fysisk eller juridisk person, der er oprettet og anerkendt som sådan i henhold til den nationale lovgivning på det sted, hvor den er etableret, og som i eget navn kan udøve rettigheder og være underlagt forpligtelser

25) "væsentlig enhed": enhver enhed af en type, der betegnes som en væsentlig enhed i bilag I

26) "vigtig enhed": enhver enhed af en type, der betegnes som en vigtig enhed i bilag II.

KAPITEL II

Koordinerede lovgivningsmæssige rammer for cybersikkerhed

Artikel 5
National cybersikkerhedsstrategi

1. Hver medlemsstat vedtager en national cybersikkerhedsstrategi, hvori den definerer de strategiske mål og passende politiske og reguleringsmæssige foranstaltninger med henblik på at opnå og opretholde et højt cybersikkerhedsniveau. Den nationale cybersikkerhedsstrategi omfatter navnlig følgende:

(a) en definition af mål og prioriteter i medlemsstaternes strategi for cybersikkerhed

(b) en forvaltningsramme med henblik på at nå disse mål og prioriteter, herunder de politikker, der er omhandlet i stk. 2, og offentlige organers og andre relevante aktørers roller og ansvarsområder

(c) en vurdering med henblik på at identificere relevante aktiver og cybersikkerhedsrisici i den pågældende medlemsstat

(d) identificering af foranstaltninger, der sikrer beredskab, reaktion og genopretning i forbindelse med hændelser, herunder samarbejde mellem den offentlige og den private sektor

(e) en liste over de forskellige myndigheder og aktører, der er involveret i gennemførelsen af den nationale cybersikkerhedsstrategi

(f) en politisk ramme for øget koordinering mellem de kompetente myndigheder i henhold til dette direktiv og Europa-Parlamentets og Rådets direktiv (EU)

XXXX/XXXX[38] [direktivet om kritiske enheders modstandsdygtighed] med henblik på udveksling af oplysninger om hændelser og cybertrusler og udøvelse af tilsynsopgaver.

2. Som led i den nationale cybersikkerhedsstrategi vedtager medlemsstaterne navnlig følgende politikker:

   a) en politik vedrørende cybersikkerhed i forsyningskæden for IKT-produkter og -tjenester, der anvendes af væsentlige og vigtige enheder til levering af deres tjenester

   b) retningslinjer for medtagelse og specificering af cybersikkerhedsrelaterede krav til IKT-produkter og -tjenester i forbindelse med offentlige indkøb

   c) en politik til fremme af koordineret offentliggørelse af sårbarheder som omhandlet i artikel 6

   d) en politik vedrørende opretholdelse af den generelle tilgængelighed og integritet af den offentlige centrale del af det åbne internet

   e) en politik til fremme og udvikling af cybersikkerhedsfærdigheder, bevidstgørelse samt forsknings- og udviklingsinitiativer

   f) en politik for støtte til akademiske institutioner og forskningsinstitutioner med henblik på udvikling af cybersikkerhedsværktøjer og sikker netværksinfrastruktur

   g) en politik, relevante procedurer og passende informationsdelingsværktøjer til støtte for frivillig udveksling af cybersikkerhedsoplysninger mellem virksomheder i overensstemmelse med EU-retten

   h) en politik, der tilgodeser specifikke behov hos SMV'er, navnlig dem, der er udelukket fra dette direktivs anvendelsesområde, i forbindelse med vejledning og støtte til forbedring af deres modstandsdygtighed over for cybersikkerhedstrusler.

3. Medlemsstaterne underretter Kommissionen om deres nationale cybersikkerhedsstrategier senest tre måneder efter deres vedtagelse. Medlemsstaterne kan udelukke specifikke oplysninger fra underretningen, hvis og i det omfang det er strengt nødvendigt af hensyn til den nationale sikkerhed.

4. Medlemsstaterne vurderer deres nationale cybersikkerhedsstrategier mindst hvert fjerde år på grundlag af centrale præstationsindikatorer og ændrer dem om nødvendigt. Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) bistår på anmodning af medlemsstaterne disse med at udvikle en national strategi og nøgleresultatindikatorer til vurdering af strategien.

Artikel 6

Koordineret offentliggørelse af sårbarheder og et europæisk sårbarhedsregister

[38] *[insert the full title and OJ publication reference when known (indsæt den fulde titel og EUT-reference, når den kendes)]*.

1. Hver medlemsstat udpeger en af dens CSIRT'er som omhandlet i artikel 9 som koordinator med henblik på koordineret offentliggørelse af sårbarheder. Den udpegede CSIRT fungerer som betroet formidler og letter om nødvendigt samspillet mellem den underrettende enhed og producenten eller udbyderen af IKT-produkter eller -tjenester. Hvis den indberettede sårbarhed vedrører flere producenter eller udbydere af IKT-produkter eller -tjenester i hele Unionen, samarbejder den udpegede CSIRT for hver berørt medlemsstat med CSIRT-netværket.

2. ENISA udvikler og vedligeholder et europæisk sårbarhedsregister. Med henblik herpå opretter og vedligeholder ENISA passende informationssystemer, -politikker og -procedurer med det formål navnlig at sætte vigtige enheder og deres leverandører af net- og informationssystemer i stand til at afsløre og registrere sårbarheder i IKT-produkter eller -tjenester samt at give alle interesserede parter adgang til oplysningerne om sårbarheder i registret. Registret skal navnlig indeholde oplysninger, der beskriver sårbarheden, det berørte IKT-produkt eller de berørte IKT-tjenester og alvoren af sårbarheden med hensyn til de omstændigheder, hvorunder den kan udnyttes, tilgængeligheden af relaterede patches og, i mangel af tilgængelige patches, vejledning til brugere af sårbare produkter og tjenester om, hvordan risiciene som følge af afslørede sårbarheder kan afbødes.

Artikel 7

Nationale rammer for styring af cybersikkerhedskriser

1. Hver medlemsstat udpeger en eller flere kompetente myndigheder med ansvar for håndtering af væsentlige hændelser og kriser. Medlemsstaterne sikrer, at de kompetente myndigheder har tilstrækkelige ressourcer til på en virkningsfuld og effektiv måde at udføre de opgaver, de pålægges.

2. Hver medlemsstat identificerer kapaciteter, aktiver og procedurer, der kan indsættes i tilfælde af en krise med henblik på dette direktiv.

3. Hver medlemsstat vedtager en national cybersikkerhedshændelses- og kriseberedskabsplan, hvori der er fastsat mål og nærmere bestemmelser for håndteringen af væsentlige cybersikkerhedshændelser og -kriser. Planen skal navnlig indeholde følgende:

   a) målsætninger for nationale beredskabsforanstaltninger og -aktiviteter

   b) de nationale kompetente myndigheders opgaver og ansvarsområder

   c) krisestyringsprocedurer og informationsudvekslingskanaler

   d) beredskabsforanstaltninger, herunder øvelses- og uddannelsesaktiviteter

   e) relevante berørte offentlige og private interesserede parter og infrastruktur

   f) nationale procedurer og ordninger mellem relevante nationale myndigheder og organer for at sikre medlemsstatens effektive deltagelse i og støtte til den koordinerede håndtering af væsentlige cybersikkerhedshændelser og -kriser på EU-plan.

4. Medlemsstaterne underretter Kommissionen om udpegelsen af deres kompetente myndigheder, jf. stk. 1, og forelægger deres nationale cybersikkerhedshændelses- og kriseberedskabsplaner, jf. stk. 3, senest tre måneder efter udpegelsen og vedtagelsen

af disse planer. Medlemsstaterne kan udelukke specifikke oplysninger fra planen, hvis og i det omfang de er strengt nødvendige af hensyn til deres nationale sikkerhed.

Artikel 8

Nationale kompetente myndigheder og centrale kontaktpunkter

1. Hver medlemsstat udpeger en eller flere kompetente myndigheder med ansvar for cybersikkerhed og for de tilsynsopgaver, der er omhandlet i kapitel VI i dette direktiv. Medlemsstaterne kan tildele en eller flere eksisterende myndigheder denne rolle.

2. De i stk. 1 omhandlede kompetente myndigheder fører tilsyn med anvendelsen af dette direktiv på nationalt plan.

3. Hver medlemsstat udpeger et nationalt centralt kontaktpunkt for cybersikkerhed ("centralt kontaktpunkt"). Hvis en medlemsstat kun udpeger én kompetent myndighed, fungerer denne kompetente myndighed ligeledes som det centrale kontaktpunkt for den pågældende medlemsstat.

4. Hvert enkelt kontaktpunkt udøver en forbindelsesfunktion for at sikre grænseoverskridende samarbejde mellem dets medlemsstats myndigheder og de relevante myndigheder i andre medlemsstater samt for at sikre tværsektorielt samarbejde med andre nationale kompetente myndigheder i dets medlemsstat.

5. Medlemsstaterne sikrer, at de i stk. 1 omhandlede kompetente myndigheder og de centrale kontaktpunkter har tilstrækkelige ressourcer til på en effektiv måde at udføre de opgaver, som de pålægges, og dermed opfylde målene i dette direktiv. Medlemsstaterne sikrer et effektivt, virkningsfuldt og sikkert samarbejde mellem de udpegede repræsentanter i den i artikel 12 omhandlede samarbejdsgruppe.

6. Hver medlemsstat underretter uden unødig forsinkelse Kommissionen om udpegelsen af den i stk. 1 omhandlede kompetente myndighed og det i stk. 3 omhandlede centrale kontaktpunkt, deres opgaver og enhver senere ændring heraf. Hver medlemsstat offentliggør udpegelsen af disse. Kommissionen offentliggør listen over udpegede centrale kontaktpunkter.

Artikel 9

Enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er)

1. Hver medlemsstat udpeger en eller flere CSIRT'er, der skal opfylde kravene i artikel 10, stk. 1, og som mindst omfatter de i bilag I og II omhandlede sektorer, delsektorer eller enheder, og som er ansvarlige for at håndtere hændelser og risici i overensstemmelse med en nøje fastlagt proces. En CSIRT kan oprettes inden for en kompetent myndighed, jf. artikel 8.

2. Medlemsstaterne sikrer, at hver CSIRT har tilstrækkelige ressourcer til at udføre sine opgaver som fastsat i artikel 10, stk. 2, effektivt.

3. Medlemsstaterne sikrer, at hver CSIRT råder over en passende, sikker og modstandsdygtig kommunikations- og informationsinfrastruktur til udveksling af oplysninger med væsentlige og vigtige enheder og andre relevante interesserede

parter. Med henblik herpå sikrer medlemsstaterne, at CSIRT'erne bidrager til udbredelsen af sikre informationsudvekslingsværktøjer.

4. CSIRT'er samarbejder og udveksler, hvor det er relevant, relevante oplysninger i overensstemmelse med artikel 26 med pålidelige sektorfællesskaber eller tværsektorielle fællesskaber af væsentlige og vigtige enheder.

5. CSIRT'er deltager i peerevalueringer, der tilrettelægges i overensstemmelse med artikel 16.

6. Medlemsstaterne sikrer et effektivt og sikkert samarbejde mellem deres CSIRT'er i det i artikel 13 omhandlede CSIRT-netværk.

7. Medlemsstaterne underretter uden unødig forsinkelse Kommissionen om de CSIRT'er, der er udpeget i henhold til stk. 1, den CSIRT-koordinator, der er udpeget i henhold til artikel 6, stk. 1, og deres respektive opgaver i relation til de i bilag I og II omhandlede enheder.

8. Medlemsstaterne kan anmode ENISA om bistand til at udvikle nationale CSIRT'er.

Artikel 10

Krav til CSIRT'er og deres opgaver

1. CSIRT'er skal opfylde nedenstående krav:

   a) CSIRT'er skal sikre et højt tilgængelighedsniveau for deres kommunikationstjenester ved at undgå svage punkter ("single points of failure") og ved til enhver tid at have flere muligheder for at blive kontaktet og for at kontakte andre. CSIRT'er skal tydeligt angive kommunikationskanalerne og gøre dem kendt af samarbejdspartnere.

   b) CSIRT'ers lokaler og de underliggende informationssystemer skal være placeret i sikrede områder.

   c) CSIRT'er skal være udstyret med et passende system til administration og videresendelse af anmodninger med henblik på at lette effektive overdragelser.

   d) CSIRT'er skal have tilstrækkeligt personale til at sikre tilgængelighed døgnet rundt.

   e) CSIRT'er skal være udstyret med redundante systemer og backup-arbejdsplads for at sikre kontinuiteten i deres tjenester.

   f) CSIRT'er skal have mulighed for at deltage i internationale samarbejdsnetværk.

2. CSIRT'er har følgende opgaver:

   a) overvågning af cybertrusler, -sårbarheder og -hændelser på nationalt plan

   b) tidlig varsling, alarmer, meddelelser og formidling af oplysninger til væsentlige og vigtige enheder samt til andre relevante interesserede parter om cybertrusler, -sårbarheder og -hændelser

   c) at reagere på hændelser

   d) udarbejdelse af dynamiske risiko- og hændelsesanalyser og situationsbevidsthed vedrørende cybersikkerhed

e) på anmodning af en enhed at foretage en proaktiv scanning af de net- og informationssystemer, der anvendes til levering af deres tjenester

f) deltage i CSIRT-netværket og yde gensidig bistand til andre medlemmer af netværket efter anmodning fra disse.

3. CSIRT'er etablerer samarbejdsrelationer med relevante aktører i den private sektor med henblik på bedre at nå direktivets mål.

4. For at lette samarbejdet fremmer CSIRT'er vedtagelse og anvendelse af fælles eller standardiseret praksis, klassifikationsordninger og taksonomier i forbindelse med følgende:

a) procedurer for håndtering af hændelser

b) krisestyring på cybersikkerhedsområdet

c) koordineret offentliggørelse af sårbarheder.

Artikel 11

Samarbejde på nationalt plan

1. Hvis en medlemsstats kompetente myndigheder som omhandlet i artikel 8, det centrale kontaktpunkt og CSIRT('er) er adskilte enheder, samarbejder de med hensyn til opfyldelsen af de forpligtelser, der er fastlagt i dette direktiv.

2. Medlemsstaterne sikrer, at enten deres kompetente myndigheder eller deres CSIRT'er modtager meddelelser om hændelser og væsentlige cybertrusler og nærvedhændelser, som indgives i henhold til dette direktiv. Hvis en medlemsstat beslutter, at dens CSIRT'er ikke skal modtage disse underretninger, skal CSIRT'erne, i det omfang det er nødvendigt for udførelsen af deres opgaver, have adgang til data om hændelser, som de væsentlige eller vigtige enheder har meddelt i henhold til artikel 20.

3. Hver medlemsstat sikrer, at dens kompetente myndigheder eller CSIRT'er underretter dens centrale kontaktpunkt om underretninger om hændelser, væsentlige cybertrusler og nærvedhændelser, som indgives i henhold til dette direktiv.

4. I det omfang det er nødvendigt for effektivt at udføre de opgaver og forpligtelser, der er fastsat i dette direktiv, sikrer medlemsstaterne et passende samarbejde mellem de kompetente myndigheder og de centrale kontaktpunkter og de retshåndhævende myndigheder, databeskyttelsesmyndigheder og myndigheder med ansvar for kritisk infrastruktur i henhold til direktiv (EU) XXXX/XXXX [direktivet om kritiske enheders modstandsdygtighed] og de nationale finansmyndigheder, der er udpeget i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) XXXX/XXXX[39] [DORA-forordningen] i den pågældende medlemsstat.

5. Medlemsstaterne sikrer, at deres kompetente myndigheder regelmæssigt giver oplysninger til kompetente myndigheder, der er udpeget i henhold til direktiv (EU) XXXX/XXXX [direktivet om kritiske enheders modstandsdygtighed] om cybersikkerhedsrisici, cybertrusler og hændelser, som påvirker væsentlige enheder, der er identificeret som kritiske eller som enheder, der svarer til kritiske enheder, i

[39] *[insert the full title and OJ publication reference when known (indsæt den fulde titel og EUT-reference, når den kendes)]*.

henhold til direktiv (EU) XXXX/XXXX [direktivet om kritiske enheders modstandsdygtighed], samt de foranstaltninger, der træffes af kompetente myndigheder som reaktion på disse risici og hændelser.

KAPITEL III

Samarbejde

Artikel 12
Samarbejdsgruppe

1. For at støtte og lette det strategiske samarbejde og udvekslingen af oplysninger mellem medlemsstaterne inden for direktivets anvendelsesområde nedsættes der en samarbejdsgruppe.

2. Samarbejdsgruppen udfører sine opgaver på grundlag af toårige arbejdsprogrammer som omhandlet i stk. 6.

3. Samarbejdsgruppen består af repræsentanter fra medlemsstaterne, Kommissionen og ENISA. Tjenesten for EU's Optræden Udadtil deltager som observatør i samarbejdsgruppens aktiviteter. De europæiske tilsynsmyndigheder (ESA'er) i henhold til artikel 17, stk. 5, litra c), i forordning (EU) XXXX/XXXX [DORA-forordningen] kan deltage i samarbejdsgruppens aktiviteter.

   Samarbejdsgruppen kan, hvis det er relevant, indbyde repræsentanter fra relevante interessenter til at deltage i arbejdet.

   Sekretariatsopgaverne varetages af Kommissionen.

4. Samarbejdsgruppen har følgende opgaver:

   a) at vejlede de kompetente myndigheder i forbindelse med omsætningen og gennemførelsen af dette direktiv

   b) at udveksle bedste praksis og oplysninger i forbindelse med gennemførelsen af dette direktiv, herunder i forbindelse med cybertrusler, -hændelser og -sårbarheder, nærvedhændelser, bevidstgørelsesinitiativer, uddannelse, øvelser og færdigheder, opbygning af kapacitet samt standarder og tekniske specifikationer

   c) at udveksle rådgivning og samarbejde med Kommissionen om nye politiske initiativer inden for cybersikkerhed

   d) at udveksle rådgivning og samarbejde med Kommissionen om udkast til Kommissionens gennemførelsesretsakter eller delegerede retsakter vedtaget i henhold til dette direktiv

   e) at udveksle bedste praksis og oplysninger med relevante EU-institutioner, -organer, -kontorer og -agenturer

   f) at rådgive om den i artikel 16, stk. 7, omhandlede peerevaluering

   g) at drøfte resultaterne af fælles tilsynsaktiviteter i grænseoverskridende sager, jf. artikel 34

h) at yde strategisk vejledning til CSIRT-netværket om specifikke nye spørgsmål

i) at bidrage til cybersikkerhedskapaciteter i hele Unionen ved at lette udvekslingen af nationale embedsmænd gennem et kapacitetsopbygningsprogram, der omfatter personale fra medlemsstaternes kompetente myndigheder eller CSIRT'er

j) at tilrettelægge regelmæssige fælles møder med relevante private interesserede parter fra hele Unionen for at drøfte gruppens aktiviteter og indsamle input om nye politiske udfordringer

k) at drøfte det arbejde, der er udført i forbindelse med cybersikkerhedsøvelser, herunder ENISA's arbejde.

5. Samarbejdsgruppen kan anmode CSIRT-netværket om en teknisk rapport om udvalgte emner.

6. Senest … [24 måneder efter datoen for dette direktivs ikrafttræden] og derefter hvert andet år udarbejder samarbejdsgruppen et arbejdsprogram for de foranstaltninger, der skal iværksættes for at gennemføre dens mål og opgaver. Tidsrammen for det første program, der vedtages i henhold til dette direktiv, tilpasses tidsrammen for det sidste program, der er vedtaget i henhold til direktiv (EU) 2016/1148.

7. Kommissionen vedtager gennemførelsesretsakter, hvori der fastlægges proceduremæssige ordninger, som er nødvendige for samarbejdsgruppens funktion. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 37, stk. 2.

8. Samarbejdsgruppen mødes regelmæssigt og mindst en gang om året med gruppen for kritiske enheders modstandsdygtighed, der er nedsat i henhold til direktiv (EU) XXXX/XXXX [direktivet om kritiske enheders modstandsdygtighed] for at fremme strategisk samarbejde og udveksling af oplysninger.

Artikel 13
CSIRT-netværket

1. Med henblik på at bidrage til skabelse af tillid mellem medlemsstaterne og fremme et hurtigt og effektivt operationelt samarbejde mellem medlemsstaterne oprettes der et netværk af nationale CSIRT'er.

2. CSIRT-netværket består af repræsentanter fra medlemsstaternes CSIRT'er og CERT-EU. Kommissionen deltager i CSIRT-netværket som observatør. ENISA varetager sekretariatsopgaverne og støtter aktivt samarbejdet mellem CSIRT'erne.

3. CSIRT-netværket har følgende opgaver:

(a) at udveksle oplysninger om CSIRT'ers kapaciteter

(b) at udveksle relevante oplysninger om hændelser, nærvedhændelser, cybertrusler, -risici og -sårbarheder

(c) efter anmodning fra en repræsentant for CSIRT-netværket, der potentielt er berørt af en hændelse, at udveksle og drøfte oplysninger i forbindelse med denne hændelse og tilknyttede cybertrusler, -risici og -sårbarheder

(d) på anmodning af en repræsentant for CSIRT-netværket at drøfte og, når det er muligt, gennemføre en samordnet reaktion på en hændelse, som er identificeret inden for den medlemsstats jurisdiktion

(e) at yde medlemsstaterne støtte til håndtering af grænseoverskridende hændelser i henhold til dette direktiv

(f) at samarbejde og yde bistand til udpegede CSIRT'er, jf. artikel 6, med hensyn til forvaltning af koordineret offentliggørelse af sårbarheder, der berører flere producenter eller udbydere af IKT-produkter, -tjenester og -processer, som er etableret i forskellige medlemsstater

(g) at drøfte og identificere yderligere former for operationelt samarbejde, herunder i forhold til:

i) kategorier af cybertrusler og -hændelser

ii) tidlig varsling

iii) gensidig bistand

iv) principper og retningslinjer for koordination som reaktion på grænseoverskridende risici og hændelser

v) bidrag til den nationale cybersikkerhedshændelses- og kriseberedskabsplan, der er omhandlet i artikel 7, stk. 3

(h) at oplyse samarbejdsgruppen om sine aktiviteter og om yderligere former for operationelt samarbejde, som drøftes i henhold til litra g), og hvis det er nødvendigt, anmode om vejledning i forbindelse hermed

(i) at gøre status over cybersikkerhedsøvelser, herunder fra dem, der tilrettelægges af ENISA

(j) på anmodning af en given CSIRT at drøfte denne CSIRT's kapaciteter og beredskab

(k) at samarbejde og udveksle oplysninger med regionale sikkerhedsoperationscentre og EU-sikkerhedsoperationscentre for at forbedre den fælles situationsbevidsthed om hændelser og trusler i hele Unionen

(l) at drøfte den i artikel 16, stk. 7, omhandlede peerevaluering

(m) at udstede retningslinjer for at lette konvergensen mellem operationel praksis med hensyn til anvendelsen af bestemmelserne i denne artikel vedrørende operationelt samarbejde.

4. Med henblik på den i artikel 35 omhandlede evaluering og senest [24 måneder efter datoen for dette direktivs ikrafttræden] og derefter hvert andet år vurderer CSIRT-netværket de fremskridt, der er gjort med det operationelle samarbejde, og udarbejder en rapport. Rapporten skal navnlig drage konklusioner om resultaterne af de i artikel 16 omhandlede peerevalueringer, som er gennemført vedrørende nationale CSIRT'er, herunder konklusioner og henstillinger, der forfølges i henhold til denne artikel. Rapporten forelægges ligeledes for samarbejdsgruppen.

5. CSIRT-netværket vedtager sin egen forretningsorden.

Artikel 14

Det europæiske netværk af forbindelsesorganisationer for cyberkriser (EU-CyCLONe)

1. For at støtte den koordinerede forvaltning af væsentlige cybersikkerhedshændelser og -kriser på operationelt plan og sikre regelmæssig udveksling af oplysninger mellem medlemsstaterne og Unionens institutioner, organer og agenturer oprettes hermed det europæiske netværk af forbindelsesorganisationer for cyberkriser (EU-CyCLONe).
2. EU-CyCLONe består af repræsentanter for medlemsstaternes krisestyringsmyndigheder, der er udpeget i overensstemmelse med artikel 7, Kommissionen og ENISA. ENISA varetager netværkets sekretariatsfunktion og støtter en sikker udveksling af oplysninger.
3. EU-CyCLONe har til opgave at
   a) øge beredskabet i forbindelse med håndtering af væsentlige hændelser og kriser
   b) udvikle en fælles situationsbevidsthed om relevante cybersikkerhedshændelser
   c) koordinere styringen af væsentlige hændelser og kriser og støtte beslutningstagning på politisk plan i forbindelse med sådanne hændelser og kriser
   d) drøfte nationale planer for cybersikkerhedshændelser og beredskabsplaner, jf. artikel 7, stk. 2.
4. EU-CyCLONe vedtager selv sin forretningsorden.
5. EU-CyCLONe aflægger regelmæssigt rapport til samarbejdsgruppen om cybertrusler, -hændelser og -tendenser med særligt fokus på deres indvirkning på væsentlige og vigtige enheder.
6. EU-CyCLONe samarbejder med CSIRT-netværket på grundlag af aftalte proceduremæssige ordninger.

Artikel 15

Rapport om cybersikkerhedssituationen i Unionen

1. ENISA udarbejder i samarbejde med Kommissionen hvert andet år en rapport om cybersikkerhedssituationen i Unionen. Rapporten skal navnlig indeholde en vurdering af følgende:
   (a) udviklingen af cybersikkerhedskapaciteter i hele Unionen
   (b) de tekniske, finansielle og menneskelige ressourcer, der er til rådighed for kompetente myndigheder og cybersikkerhedspolitikker samt gennemførelsen af tilsynsforanstaltninger og håndhævelsesforanstaltninger i lyset af resultaterne af peerevalueringer, jf. artikel 16
   (c) et cybersikkerhedsindeks, der giver mulighed for en samlet vurdering af cybersikkerhedskapaciteternes modenhedsniveau.
2. Rapporten skal indeholde særlige politiske henstillinger med henblik på at øge cybersikkerhedsniveauet i hele Unionen og et sammendrag af resultaterne for den pågældende periode fra agenturets tekniske EU-cybersikkerhedsrapport, som

udsendes af ENISA i overensstemmelse med artikel 7, stk. 6, i forordning (EU) 2019/881.

Artikel 16

Peerevalueringer

1. Kommissionen fastlægger efter høring af samarbejdsgruppen og ENISA og senest 18 måneder efter dette direktivs ikrafttræden metoden og indholdet af et peerevalueringssystem til vurdering af effektiviteten af medlemsstaternes cybersikkerhedspolitikker. Evalueringerne foretages af tekniske cybersikkerhedseksperter fra andre medlemsstater end den evaluerede og omfatter som minimum følgende:

   i) effektiviteten af gennemførelsen af de krav til styring af cybersikkerhedsrisici og rapporteringsforpligtelser, der er omhandlet i artikel 18 og 20

   ii) kapacitetsniveauet, herunder de finansielle, tekniske og menneskelige ressourcer, der er til rådighed, og effektiviteten af de nationale kompetente myndigheders varetagelse af deres opgaver

   iii) CSIRT'ers operationelle kapacitet og effektivitet

   iv) effektiviteten af gensidig bistand, jf. artikel 34

   v) effektiviteten af den ramme for informationsudveksling, der er omhandlet i artikel 26 i dette direktiv.

2. Metoden skal omfatte objektive, ikkediskriminerende, retfærdige og gennemsigtige kriterier, på grundlag af hvilke medlemsstaterne udpeger eksperter, der kan udføre peerevalueringerne. ENISA og Kommissionen udpeger eksperter, der deltager som observatører i peerevalueringerne. Kommissionen fastsætter med støtte fra ENISA inden for den stk. 1 omhandlede metode et objektivt, ikkediskriminerende, retfærdigt og gennemsigtigt system til udvælgelse og tilfældig tildeling af eksperter til hver peerevaluering.

3. De organisatoriske aspekter af peerevalueringerne fastlægges af Kommissionen med støtte fra ENISA og baseres efter høring af samarbejdsgruppen på kriterier, der er defineret i den i stk. 1 omhandlede metode. Peerevalueringer skal vurdere de i stk. 1 omhandlede aspekter for alle medlemsstater og sektorer, herunder målrettede spørgsmål, der er specifikke for en eller flere medlemsstater eller en eller flere sektorer.

4. Peerevalueringer omfatter faktiske eller virtuelle besøg på stedet og udvekslinger uden for stedet. I henhold til princippet om godt samarbejde giver de medlemsstater, der skal evalueres, de udpegede eksperter de oplysninger, som er nødvendige for vurderingen af de evaluerede aspekter. Alle oplysninger, der indhentes i forbindelse med peerevalueringsprocessen, anvendes kun til dette formål. De eksperter, der deltager i peerevalueringen, må ikke videregive følsomme eller fortrolige oplysninger, som er indhentet i forbindelse med denne gennemgang, til tredjemand.

5. Når bestemte aspekter er blevet gennemgået i en medlemsstat, må de samme aspekter ikke underkastes yderligere peerevaluering i den pågældende medlemsstat i de to år, der følger efter afslutningen af en peerevaluering, medmindre Kommissionen træffer anden afgørelse efter høring af ENISA og samarbejdsgruppen.

6. Medlemsstaterne sikrer, at enhver risiko for interessekonflikter vedrørende de udpegede eksperter meddeles de øvrige medlemsstater, Kommissionen og ENISA uden unødig forsinkelse.

7. Eksperter, der deltager i peerevalueringer, udarbejder rapporter om resultaterne og konklusionerne af evalueringerne. Rapporterne forelægges for Kommissionen, samarbejdsgruppen, CSIRT-netværket og ENISA. Rapporterne drøftes i samarbejdsgruppen og CSIRT-netværket. Rapporterne kan offentliggøres på samarbejdsgruppens særlige websted.

KAPITEL IV

Forpligtelser vedrørende risikostyring og rapportering i forbindelse med cybersikkerhed

AFDELING I

Styring og rapportering af cybersikkerhedsrisici

Artikel 17

Forvaltning

1. Medlemsstaterne sikrer, at ledelsesorganerne for væsentlige og vigtige enheder godkender de foranstaltninger til styring af cybersikkerhedsrisici, som disse enheder har truffet med henblik på at overholde artikel 18, fører tilsyn med dens gennemførelse og er ansvarlige for enhedernes manglende overholdelse af forpligtelserne i henhold til denne artikel.

2. Medlemsstaterne sikrer, at medlemmerne af ledelsesorganet regelmæssigt følger specifikke kurser for at opnå tilstrækkelig viden og færdigheder til at forstå og vurdere cybersikkerhedsrisici og styringspraksisser samt deres indvirkning på enhedens drift.

Artikel 18

Risikohåndteringsforanstaltninger i forbindelse med cybersikkerhed

1. Medlemsstaterne sikrer, at væsentlige og vigtige enheder træffer passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre risiciene for sikkerheden i net- og informationssystemer, som disse enheder anvender til at levere deres tjenester. Under hensyntagen til det aktuelle stade skal disse foranstaltninger sikre et sikkerhedsniveau for net- og informationssystemer, der står i forhold til risikoen.

2. De i stk. 1 omhandlede foranstaltninger omfatter mindst følgende:

   (a) politikker for risikoanalyse og informationssystemsikkerhed

   (b) håndtering af hændelser (forebyggelse, opdagelse og reaktion på hændelser)

(c) driftskontinuitet og krisestyring

(d) forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forbindelserne mellem den enkelte enhed og dens leverandører eller tjenesteydere såsom leverandører af datalagrings- og databehandlingstjenester eller forvaltede sikkerhedstjenester

(e) sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder

(f) politikker og procedurer (test og revision) til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici

(g) brug af kryptografi og kryptering.

3. Medlemsstaterne sikrer, at enheder, når de overvejer passende foranstaltninger som omhandlet i stk. 2, litra d), tager hensyn til de sårbarheder, der er specifikke for hver leverandør og tjenesteudbyder, og den generelle kvalitet af deres leverandørers og tjenesteudbyderes produkter og cybersikkerhedspraksis, herunder deres sikre udviklingsprocedurer.

4. Medlemsstaterne sikrer, at hvis en enhed finder, at dens tjenester eller opgaver ikke er i overensstemmelse med kravene i stk. 2, træffer den uden unødig forsinkelse alle nødvendige korrigerende foranstaltninger for at bringe den pågældende tjeneste i overensstemmelse med kravene.

5. Kommissionen kan vedtage gennemførelsesretsakter med henblik på at fastlægge de tekniske og metodiske specifikationer for de i stk. 2 omhandlede elementer. Når Kommissionen udarbejder disse retsakter, følger den undersøgelsesproceduren i artikel 37, stk. 2, og følger i videst muligt omfang internationale og europæiske standarder samt relevante tekniske specifikationer.

6. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter i overensstemmelse med artikel 36 med henblik på at supplere de elementer, der er fastsat i stk. 2, for at tage hensyn til nye cybertrusler, den teknologiske udvikling eller sektorspecifikke særtræk.

Artikel 19

Koordinerede EU-risikovurderinger af kritiske forsyningskæder

1. Samarbejdsgruppen kan i samarbejde med Kommissionen og ENISA foretage koordinerede sikkerhedsrisikovurderinger af specifikke kritiske IKT-tjenester, -systemer eller -produktforsyningskæder under hensyntagen til tekniske og, hvor det er relevant, ikketekniske risikofaktorer.

2. Kommissionen identificerer efter høring af samarbejdsgruppen og ENISA de specifikke kritiske IKT-tjenester, -systemer eller -produkter, der kan være genstand for den i stk. 1 omhandlede koordinerede risikovurdering.

Artikel 20

Rapporteringsforpligtelser

1. Medlemsstaterne sikrer, at væsentlige og vigtige enheder uden unødig forsinkelse underretter de kompetente myndigheder eller CSIRT'en i overensstemmelse med stk. 3 og 4 om enhver hændelse, der har en væsentlig indvirkning på leveringen af deres tjenester. Hvor det er relevant, underretter disse enheder uden unødig forsinkelse modtagerne af deres tjenester om hændelser, der kan forventes at påvirke leveringen af den pågældende tjeneste negativt. Medlemsstater sikrer, at disse enheder bl.a. indberetter alle oplysninger, der gør det muligt for den kompetente myndighed eller CSIRT'en at fastslå eventuelle grænseoverskridende konsekvenser af hændelsen.

2. Medlemsstaterne sikrer, at væsentlige og vigtige enheder uden unødig forsinkelse underretter de kompetente myndigheder eller CSIRT'en om enhver væsentlig cybertrussel, som disse enheder identificerer, og som potentielt kunne have resulteret i en væsentlig hændelse.

   Hvor det er relevant, underretter disse enheder uden unødig forsinkelse modtagerne af deres tjenester, som potentielt er berørt af en væsentlig cybertrussel, om eventuelle foranstaltninger eller afhjælpende foranstaltninger, som disse modtagere kan træffe som reaktion på denne trussel. Hvis det er relevant, underretter enhederne også disse modtagere om selve truslen. Underretningen medfører ikke et øget ansvar for den underrettende enhed.

3. En hændelse anses for at være væsentlig, hvis:

   (a) hændelsen har forårsaget eller potentielt kan forårsage væsentlige driftsforstyrrelser eller økonomiske tab for den pågældende enhed

   (b) hændelsen har påvirket eller kan påvirke andre fysiske eller juridiske personer ved at forårsage betydelige materielle eller immaterielle tab.

4. Medlemsstaterne sikrer, at de berørte enheder med henblik på den i stk. 1 omhandlede underretning fremsender følgende til de kompetente myndigheder eller CSIRT'en:

   (a) uden unødig forsinkelse og under alle omstændigheder inden for 24 timer efter at have fået kendskab til hændelsen en indledende underretning, som, hvis det er relevant, skal angive, om hændelsen formodes at være forårsaget af ulovlige eller ondsindede handlinger

   (b) efter anmodning fra en kompetent myndighed eller en CSIRT, en foreløbig rapport om relevante statusopdateringer

   (c) en endelig rapport senest en måned efter forelæggelsen af den i litra a) omhandlede rapport, der som minimum omfatter følgende:

      i) en detaljeret beskrivelse af hændelsen, dens alvorlighed og indvirkning

      ii) den type trussel eller grundlæggende årsag, der sandsynligvis udløste hændelsen

      iii) anvendte og igangværende afbødende foranstaltninger.

   Medlemsstaterne fastsætter bestemmelser om, at den pågældende enhed i behørigt begrundede tilfælde og efter aftale med de kompetente myndigheder eller CSIRT'en kan fravige de frister, der er fastsat i litra a) og c).

5. De kompetente nationale myndigheder eller CSIRT'en skal senest 24 timer efter modtagelsen af den i artikel 4, litra a), omhandlede indledende underretning give den underrettende enhed et svar, herunder indledende tilbagemeldinger om hændelsen og, efter anmodning fra enheden, vejledning om gennemførelsen af mulige afbødende foranstaltninger. Hvis CSIRT'en ikke har modtaget den i stk. 1 omhandlede underretning, gives vejledningen af den kompetente myndighed i samarbejde med CSIRT'en. CSIRT'en yder supplerende teknisk bistand, hvis den berørte enhed anmoder herom. Hvis hændelsen mistænkes for at være af strafferetlig karakter, giver de kompetente nationale myndigheder eller CSIRT'en også vejledning om underretning af retshåndhævende myndigheder om hændelsen.

6. Hvis det er relevant, og navnlig hvor den i stk. 1 omhandlede hændelse berører to eller flere medlemsstater, informerer den kompetente myndighed eller CSIRT'en de øvrige berørte medlemsstater og ENISA om hændelsen. De kompetente myndigheder, CSIRT'erne og de centrale kontaktpunkter sikrer i den forbindelse i overensstemmelse med EU-retten eller national lovgivning, der er i overensstemmelse med EU-retten, den digitale tjenesteudbyders sikkerhed og kommercielle interesser samt fortrolig behandling af de afgivne oplysninger.

7. Hvis offentlighedens kendskab er nødvendig for at forebygge en hændelse eller for at håndtere en igangværende hændelse, eller hvis offentliggørelse af hændelsen på anden vis er i offentlighedens interesse, kan den kompetente myndighed eller CSIRT'en og, hvor det er relevant, myndighederne eller CSIRT'erne i andre berørte medlemsstater efter høring af den berørte enhed informere offentligheden om hændelsen eller kræve, at enheden gør det.

8. På den kompetente myndigheds eller CSIRT'ens anmodning videresender det centrale kontaktpunkt de i stk. 1 og 2 omhandlede underretninger til centrale kontaktpunkter i andre berørte medlemsstater.

9. Det centrale kontaktpunkt forelægger en gang om måneden en sammenfattende rapport for ENISA, herunder anonymiserede og aggregerede data om hændelser, væsentlige cybertrusler og nærvedhændelser, der er indberettet i overensstemmelse med stk. 1 og 2 og i overensstemmelse med artikel 27. For at bidrage til tilvejebringelsen af sammenlignelige oplysninger kan ENISA udstede teknisk vejledning om parametrene for oplysningerne i den sammenfattende rapport.

10. De kompetente myndigheder giver de kompetente myndigheder, der er udpeget i henhold til direktiv (EU) XXXX/XXXX [direktivet om kritiske enheders modstandsdygtighed], oplysninger om hændelser og cybertrusler, som er meddelt i overensstemmelse med stk. 1 og 2 af væsentlige enheder, der er identificeret som kritiske enheder eller som enheder, der svarer til kritiske enheder, i henhold til direktiv (EU) XXXX/XXXX [direktivet om kritiske enheders modstandsdygtighed].

11. Kommissionen kan vedtage gennemførelsesretsakter, der yderligere præciserer typen af oplysninger, formatet og proceduren for en meddelelse indgivet i henhold til stk. 1 og 2. Kommissionen kan også vedtage gennemførelsesretsakter for yderligere at præcisere de tilfælde, hvor en hændelse anses for at være væsentlig, jf. stk. 3. Disse gennemførelsesretsakter vedtages efter undersøgelsesproceduren i artikel 37, stk. 2.

Artikel 21

Brug af europæiske cybersikkerhedscertificeringsordninger

1. For at påvise overensstemmelse med visse krav i artikel 18 kan medlemsstaterne kræve, at væsentlige og vigtige enheder certificerer visse IKT-produkter, -tjenester og -processer i henhold til specifikke europæiske cybersikkerhedscertificeringsordninger, der er vedtaget i henhold til artikel 49 i forordning (EU) 2019/881. De produkter, tjenester og processer, der certificeres, kan være udviklet af en væsentlig eller vigtig enhed eller indkøbes fra tredjeparter.

2. Kommissionen tillægges beføjelser til at vedtage delegerede retsakter, som præciserer, hvilke kategorier af væsentlige enheder der skal indhente en attest, og i henhold til hvilke specifikke europæiske cybersikkerhedscertificeringsordninger, jf. stk. 1. De delegerede retsakter vedtages i overensstemmelse med artikel 36.

3. Kommissionen kan anmode ENISA om at udarbejde et forslag til ordning i henhold til artikel 48, stk. 2, i forordning (EU) 2019/881 i tilfælde, hvor der ikke findes en passende europæisk cybersikkerhedscertificeringsordning, jf. stk. 2.

Artikel 22

Standardisering

1. For at sikre en samordnet gennemførelse af artikel 18, stk. 1 og 2, tilskynder medlemsstaterne til at benytte europæiske eller internationalt anerkendte standarder og specifikationer, der er relevante for sikkerheden i net- og informationssystemer, uden at de påtvinger eller forskelsbehandler til fordel for anvendelse af en bestemt type teknologi.

2. ENISA udarbejder i samarbejde med medlemsstaterne vejledning og retningslinjer om de tekniske områder, der skal overvejes i forbindelse med stk. 1, samt om allerede eksisterende standarder, herunder medlemsstaternes nationale standarder, hvilket vil give mulighed for at dække disse områder.

Artikel 23

Database over domænenavne og registreringsoplysninger

1. Med henblik på at bidrage til DNS' sikkerhed, stabilitet og modstandsdygtighed sikrer medlemsstaterne, at topdomæneregistraturer og enheder, der leverer domænenavnsregistreringstjenester til topdomæner, med rettidig omhu indsamler og vedligeholder nøjagtige og fuldstændige oplysninger om domænenavnsregistrering i en særlig databasefacilitet i henhold til Unionens databeskyttelseslovgivning for så vidt angår personoplysninger.

2. Medlemsstaterne sikrer, at de i stk. 1 omhandlede databaser over domænenavnsregistreringsdata indeholder relevante oplysninger med henblik på at identificere og kontakte indehaverne af domænenavne og de kontaktpunkter, der forvalter domænenavne under topdomæner.

3. Medlemsstaterne sikrer, at topdomæneregistraturerne og de enheder, der leverer domænenavnsregistreringstjenester til topdomænet, har indført politikker og procedurer, der sikrer, at databaserne indeholder nøjagtige og fuldstændige oplysninger. Medlemsstaterne sikrer, at sådanne politikker og procedurer gøres offentligt tilgængelige.

4. Medlemsstaterne sikrer, at topdomæneregistraturerne og de enheder, der leverer domænenavnsregistreringstjenester til topdomænet, uden unødig forsinkelse efter registreringen af et domænenavn offentliggør domæneregistreringsdata, som ikke er personoplysninger.

5. Medlemsstaterne sikrer, at topdomæneregistraturerne og de enheder, der udbyder domænenavnsregistreringstjenester for topdomænet, giver adgang til specifikke oplysninger om domænenavnsregistrering efter lovlige og behørigt begrundede anmodninger fra legitime adgangssøgende i overensstemmelse med EU's databeskyttelseslovgivning. Medlemsstaterne sikrer, at topdomæneregistraturerne og de enheder, der leverer domænenavnsregistreringstjenester til topdomænet, besvarer alle anmodninger om adgang uden unødig forsinkelse. Medlemsstaterne sikrer, at politikker og procedurer for offentliggørelse af sådanne data gøres offentligt tilgængelige.

Afsnit II

Jurisdiktion og registrering

Artikel 24

Jurisdiktion og territorialitet

1. DNS-tjenesteudbydere, topdomænenavneregistraturer, udbydere af cloud computing-tjenester, udbydere af datacentertjenester og udbydere af indholdsudsendelsesnetværk, jf. bilag I, punkt 8, samt digitale udbydere som omhandlet i bilag II, punkt 6, anses for at høre under jurisdiktionen i den medlemsstat, hvor de har deres hovedforretningssted i Unionen.

2. Med henblik på dette direktiv anses enheder som omhandlet i stk. 1 for at have deres hovedvirksomhed i Unionen i den medlemsstat, hvor beslutningerne vedrørende foranstaltningerne til styring af cybersikkerhedsrisici træffes. Hvis sådanne beslutninger ikke træffes i en virksomhed i Unionen, anses hovedvirksomheden for at ligge i den medlemsstat, hvor enhederne har virksomheden med det største antal ansatte i Unionen.

3. Hvis en enhed som omhandlet i stk. 1 ikke er etableret i Unionen, men udbyder tjenester inden for Unionen, udpeger den en repræsentant i Unionen. Repræsentanten skal være etableret i en af de medlemsstater, hvor tjenesterne tilbydes. En sådan enhed anses for at høre under den medlemsstats jurisdiktion, hvor repræsentanten er etableret. Hvis der ikke findes en udpeget repræsentant i Unionen i henhold til denne artikel, kan enhver medlemsstat, hvor enheden leverer tjenester, anlægge sag mod enheden for manglende overholdelse af forpligtelserne i henhold til dette direktiv.

4. En i stk. 1 omhandlet enheds udpegelse af en repræsentant berører ikke eventuelle retlige skridt mod selve udbyderen af digitale tjenester.

Artikel 25

Register over væsentlige og vigtige enheder

1. ENISA opretter og vedligeholder et register for væsentlige og vigtige enheder som omhandlet i artikel 24, stk. 1. Enhederne fremsender følgende oplysninger til ENISA senest [12 måneder efter direktivets ikrafttræden]:

   (a) enhedens navn

   (b) adressen på dens hovedvirksomhed og andre retlige enheder i Unionen eller, hvis den ikke er etableret i Unionen, på den repræsentant, der er udpeget i henhold til artikel 24, stk. 3

   (c) ajourførte kontaktoplysninger, herunder e-mailadresser og telefonnumre på enhederne.

2. De i stk. 1 omhandlede enheder underretter straks og under alle omstændigheder senest tre måneder efter den dato, hvor ændringen trådte i kraft, ENISA om enhver ændring af de oplysninger, de har indsendt i henhold til stk. 1.

3. Efter modtagelse af de i stk. 1 omhandlede oplysninger fremsender ENISA dem til de centrale kontaktpunkter afhængigt af den angivne placering af den enkelte enheds hovedvirksomhed eller, hvis den ikke er etableret i Unionen, dens udpegede repræsentant. Hvis en i stk. 1 omhandlet enhed ud over sin hovedvirksomhed i Unionen har yderligere virksomheder i andre medlemsstater, underretter ENISA også de centrale kontaktpunkter i disse medlemsstater.

4. Hvis en enhed ikke registrerer sine aktiviteter eller fremlægger de relevante oplysninger inden for den i stk. 1 fastsatte frist, er enhver medlemsstat, hvor enheden leverer tjenester, kompetent til at sikre, at enheden overholder forpligtelserne i dette direktiv.

KAPITEL V

Udveksling af oplysninger

Artikel 26

Ordninger for udveksling af cybersikkerhedsoplysninger

1. Uden at det berører forordning (EU) 2016/679, sikrer medlemsstaterne, at væsentlige og vigtige enheder kan udveksle relevante cybersikkerhedsoplysninger indbyrdes, herunder oplysninger om cybertrusler, sårbarheder, kompromitteringsindikatorer, taktikker, teknikker og procedurer, cybersikkerhedsadvarsler og konfigurationsværktøjer, hvis denne informationsudveksling:

   (a) har til formål at forebygge, opdage, reagere på eller afbøde hændelser

   (b) øger cybersikkerhedsniveauet, navnlig ved at øge bevidstheden om cybertrusler, begrænse eller hindre sådanne truslers evne til at sprede sig, støtte en række forsvarskapaciteter, afhjælpe og offentliggøre sårbarheder, teknikker til sporing af trusler, afbødningsstrategier eller indsats- og genopretningsfaser.

2. Medlemsstaterne sikrer, at udvekslingen af oplysninger finder sted inden for betroede fællesskaber af væsentlige og vigtige enheder. En sådan udveksling gennemføres ved hjælp af ordninger for udveksling af oplysninger for så vidt angår den potentielt

følsomme karakter af de udvekslede oplysninger og i overensstemmelse med de i stk. 1 omhandlede EU-retlige bestemmelser.

3. Medlemsstaterne fastsætter regler, der præciserer proceduren, de operationelle elementer (herunder brugen af særlige IKT-platforme), indholdet af og betingelserne for de i stk. 2 omhandlede informationsudvekslingsordninger. Sådanne regler skal også indeholde nærmere bestemmelser om inddragelse af offentlige myndigheder i sådanne ordninger samt operationelle elementer, herunder brug af særlige IT-platforme. Medlemsstaterne yder støtte til anvendelsen af sådanne ordninger i overensstemmelse med deres politikker, jf. artikel 5, stk. 2, litra g).

4. Væsentlige og vigtige enheder underretter de kompetente myndigheder om deres deltagelse i de i stk. 2 omhandlede informationsudvekslingsordninger, når de indtræder i sådanne ordninger, eller, hvis det er relevant, om deres udtræden af sådanne ordninger, når denne udtræden træder i kraft.

5. I overensstemmelse med EU-retten støtter ENISA oprettelsen af ordninger for udveksling af cybersikkerhedsoplysninger som omhandlet i stk. 2 ved at levere bedste praksis og vejledning.

Artikel 27

Frivillig meddelelse af relevante oplysninger

Medlemsstaterne sikrer, at enheder, der falder uden for dette direktivs anvendelsesområde, med forbehold af artikel 3 kan foretage underretninger på frivillig basis om væsentlige hændelser, cybertrusler eller nærvedhændelser. Når medlemsstaterne behandler underretninger, handler de efter proceduren i artikel 20. Medlemsstaterne kan prioritere behandling af obligatoriske underretninger frem for frivillige underretninger. Frivillige underretninger må ikke medføre, at den underrettende enhed pålægges nogen yderligere forpligtelser, som den ikke ville være omfattet af, hvis den ikke havde indgivet denne underretning.

KAPITEL VI

Tilsyn og håndhævelse

Artikel 28

Generelle aspekter vedrørende tilsyn og håndhævelse

1. Medlemsstaterne sikrer, at de kompetente myndigheder effektivt overvåger og træffer de nødvendige foranstaltninger for at sikre, at dette direktiv overholdes, navnlig forpligtelserne i artikel 18 og 20.

2. De kompetente myndigheder indgår i et tæt samarbejde med databeskyttelsesmyndigheder, når de håndterer hændelser, der medfører brud på persondatasikkerheden.

Artikel 29

Tilsyn og håndhævelse for væsentlige enheder

1. Medlemsstaterne sikrer, at de tilsyns- eller håndhævelsesforanstaltninger, der pålægges væsentlige enheder for så vidt angår de forpligtelser, som er fastsat i dette direktiv, er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning under hensyntagen til omstændighederne i den enkelte sag.

2. Medlemsstaterne sikrer, at de kompetente myndigheder, når de udfører deres tilsynsopgaver i forbindelse med væsentlige enheder, har beføjelse til at pålægge disse enheder:

   a) kontrol på stedet og tilsyn uden for stedet, herunder stikprøvekontrol

   b) regelmæssig revision

   c) målrettede sikkerhedsrevisioner baseret på risikovurderinger eller risikorelaterede tilgængelige oplysninger

   d) sikkerhedsscanninger baseret på objektive, ikkediskriminerende, retfærdige og gennemsigtige risikovurderingskriterier

   e) anmodninger om oplysninger, der er nødvendige for at vurdere enhedens cybersikkerhedsforanstaltninger, herunder dokumenterede cybersikkerhedspolitikker, samt overholdelse af forpligtelsen til at underrette ENISA i henhold til artikel 25, stk. 1 og 2

   f) anmodninger om adgang til data, dokumenter eller oplysninger, der er nødvendige for udførelsen af deres tilsynsopgaver

   g) anmodninger om dokumentation for gennemførelsen af cybersikkerhedspolitikker såsom resultaterne af sikkerhedsrevisioner udført af en kvalificeret revisor og den respektive underliggende dokumentation.

3. Ved udøvelsen af deres beføjelser i henhold til stk. 2, litra e)-g), angiver de kompetente myndigheder formålet med anmodningen og præciserer, hvilke oplysninger der anmodes om.

4. Medlemsstaterne sikrer, at de kompetente myndigheder, når de udøver deres håndhævelsesbeføjelser over for væsentlige enheder, har beføjelse til at:

   (a) udstede advarsler om enhedernes manglende overholdelse af forpligtelserne i dette direktiv

   (b) udstede bindende instrukser eller pålægge disse enheder at afhjælpe de konstaterede mangler eller overtrædelserne af de forpligtelser, der er fastsat i dette direktiv

   (c) pålægge disse enheder at ophøre med at udvise adfærd, der ikke opfylder de forpligtelser, som er fastsat i dette direktiv, og afstå fra at gentage denne adfærd

   (d) pålægge disse enheder at bringe deres risikostyringsforanstaltninger og/eller rapporteringsforpligtelser i overensstemmelse med forpligtelserne i artikel 18 og 20 på en nærmere bestemt måde og inden for en nærmere angivet frist

   (e) pålægge disse enheder at underrette den eller de fysiske eller juridiske personer, som de leverer tjenester eller aktiviteter til, og som potentielt er berørt af en væsentlig cybertrussel, om eventuelle beskyttelsesforanstaltninger

eller afhjælpende foranstaltninger, som disse fysiske eller juridiske personer kan træffe som reaktion på denne trussel

(f) pålægge disse enheder at gennemføre de anbefalinger, der er fremsat som følge af en sikkerhedsrevision, inden for en rimelig frist

(g) udpege en overvågningsansvarlig med veldefinerede opgaver til gennem en nærmere fastsat periode at føre tilsyn med overholdelsen af deres forpligtelser i henhold til artikel 18 og 20

(h) pålægge disse enheder at offentliggøre aspekter af manglende overholdelse af forpligtelserne i dette direktiv på en nærmere angivet måde

(i) fremsætte en offentlig erklæring, der identificerer den eller de juridiske og fysiske personer, som er ansvarlige for overtrædelsen af en forpligtelse, der er fastsat i dette direktiv, og overtrædelsens art

(j) pålægge eller anmode de relevante organer eller domstole om i henhold til national lovgivning at pålægge en administrativ bøde i henhold til artikel 31 ud over eller i stedet for de foranstaltninger, der er omhandlet i dette stykkes litra a)-i), afhængigt af omstændighederne i den enkelte sag.

5. Hvis håndhævelsesforanstaltninger vedtaget i henhold til stk. 4, litra a)-d) og f), viser sig at være virkningsløse, sikrer medlemsstaterne, at de kompetente myndigheder har beføjelse til at fastsætte en frist, inden for hvilken den væsentlige enhed anmodes om at træffe de nødvendige foranstaltninger for at afhjælpe manglerne eller opfylde disse myndigheders krav. Hvis den ønskede foranstaltning ikke træffes inden for den fastsatte frist, sikrer medlemsstaterne, at de kompetente myndigheder har beføjelse til at:

(a) suspendere eller anmode et certificerings- eller godkendelsesorgan om at suspendere en certificering eller godkendelse vedrørende dele af eller alle de tjenester eller aktiviteter, der leveres af en væsentlig enhed

(b) pålægge eller anmode de relevante organer eller domstole om i henhold til national lovgivning midlertidigt at forbyde enhver person med ledelsesansvar på administrerende eller juridisk niveau i den pågældende væsentlige enhed og enhver anden fysisk person, der anses for at være ansvarlig for overtrædelsen, at udøve ledelsesfunktioner i den pågældende enhed.

Disse sanktioner anvendes kun, indtil enheden træffer de nødvendige foranstaltninger for at afhjælpe manglerne eller opfylde kravene fra den kompetente myndighed, for hvilken sådanne sanktioner blev anvendt.

6. Medlemsstaterne sikrer, at enhver fysisk person, der er ansvarlig for eller optræder som repræsentant for en væsentlig enhed på grundlag af beføjelsen til at repræsentere den, beføjelsen til at træffe afgørelser på dennes vegne eller beføjelsen til at udøve kontrol over den, har beføjelse til at sikre, at enheden overholder forpligtelserne i dette direktiv. Medlemsstaterne sikrer, at disse fysiske personer kan drages til ansvar for tilsidesættelse af deres forpligtelser til at sikre overholdelse af forpligtelserne i dette direktiv.

7. Når de kompetente myndigheder træffer håndhævelsesforanstaltninger eller anvender sanktioner i henhold til stk. 4 og 5, skal de overholde retten til forsvar og tage hensyn til omstændighederne i den enkelte sag og som minimum tage behørigt hensyn til:

(a) overtrædelsens grovhed og betydningen af de tilsidesatte bestemmelser. Blandt de overtrædelser, der bør betragtes som alvorlige: gentagne overtrædelser, manglende underretning om eller afhjælpning af hændelser med en betydelig forstyrrende virkning, manglende afhjælpning af mangler som følge af bindende instrukser fra de kompetente myndigheder, der lægger hindringer i vejen for revisioner eller overvågningsaktiviteter, som den kompetente myndighed har beordret efter konstatering af en overtrædelse, afgivelse af urigtige eller klart unøjagtige oplysninger i forbindelse med risikostyringskravene eller rapporteringsforpligtelserne i artikel 18 og 20

(b) overtrædelsens varighed, herunder elementet af gentagne overtrædelser

(c) de faktiske skader eller lidte tab eller potentielle skader eller tab, der kunne være blevet udløst, for så vidt de kan fastslås. Ved evalueringen af dette aspekt skal der bl.a. tages hensyn til faktiske eller potentielle finansielle eller økonomiske tab, virkninger for andre tjenester, antal brugere, der er berørt eller potentielt berørt

(d) hvorvidt overtrædelsen blev begået forsætligt eller uagtsomt

(e) foranstaltninger, som enheden har truffet for at forebygge eller afbøde skaden og/eller tabet

(f) overholdelse af godkendte adfærdskodekser eller godkendte certificeringsmekanismer

(g) graden af samarbejde mellem den eller de fysiske eller juridiske person(er), der gøres ansvarlig(e), og de kompetente myndigheder.

8. De kompetente myndigheder skal give en detaljeret begrundelse for deres håndhævelsesafgørelser. Inden de kompetente myndigheder træffer sådanne afgørelser, underretter de de berørte enheder om deres foreløbige resultater og giver disse enheder en rimelig frist til at fremsætte bemærkninger.

9. Medlemsstaterne sikrer, at deres kompetente myndigheder underretter de relevante kompetente myndigheder i den berørte medlemsstat, der er udpeget i henhold til direktiv (EU) XXXX/XXXX [direktivet om kritiske enheders modstandsdygtighed], når de udøver deres tilsyns- og håndhævelsesbeføjelser med henblik på at sikre, at en væsentlig enhed, der er identificeret som kritisk eller som en enhed svarende til en kritisk enhed, i henhold til direktiv (EU) XXXX/XXXX [direktivet om kritiske enheders modstandsdygtighed] overholder forpligtelserne i henhold til dette direktiv. Efter anmodning fra kompetente myndigheder i henhold til direktiv (EU) XXXX/XXXX [direktivet om kritiske enheders modstandsdygtighed] kan de kompetente myndigheder udøve deres tilsyns- og håndhævelsesbeføjelser over for en væsentlig enhed, der er identificeret som kritisk eller tilsvarende.

Artikel 30

Tilsyn og håndhævelse for vigtige enheder

1. Hvis der forelægges dokumentation for eller tegn på, at en vigtig enhed ikke overholder forpligtelserne i dette direktiv, særlig artikel 18 og 20, sikrer medlemsstaterne, at de kompetente myndigheder træffer foranstaltninger, hvor det er nødvendigt, gennem efterfølgende tilsynsforanstaltninger.

2. Medlemsstaterne sikrer, at de kompetente myndigheder, når de udfører deres tilsynsopgaver i forbindelse med vigtige enheder, har beføjelse til at pålægge disse enheder:

   (a) kontrol på stedet og efterfølgende tilsyn uden for stedet

   (b) målrettede sikkerhedsrevisioner baseret på risikovurderinger eller risikorelaterede tilgængelige oplysninger

   (c) sikkerhedsscanninger baseret på objektive, retfærdige og gennemsigtige risikovurderingskriterier

   (d) anmodninger om oplysninger, der er nødvendige for efterfølgende at vurdere cybersikkerhedsforanstaltningerne, herunder dokumenterede cybersikkerhedspolitikker, samt overholdelsen af forpligtelsen til at underrette ENISA i henhold til artikel 25, stk. 1 og 2

   (e) anmodninger om adgang til data, dokumenter og/eller oplysninger, der er nødvendige for udførelsen af tilsynsopgaverne.

3. Ved udøvelsen af deres beføjelser i henhold til stk. 2, litra d) eller e), angiver de kompetente myndigheder formålet med anmodningen og præciserer, hvilke oplysninger der anmodes om.

4. Medlemsstaterne sikrer, at de kompetente myndigheder, når de udøver deres håndhævelsesbeføjelser over for vigtige enheder, har beføjelse til at:

   (a) udstede advarsler om enhedernes manglende overholdelse af forpligtelserne i dette direktiv

   (b) udstede bindende instrukser eller pålægge disse enheder at afhjælpe de konstaterede mangler eller overtrædelserne af de forpligtelser, der er fastsat i dette direktiv

   (c) pålægge disse enheder at ophøre med at udvise en adfærd, der ikke opfylder de forpligtelser, som er fastsat i dette direktiv, og afstå fra at gentage denne adfærd

   (d) pålægge disse enheder at bringe deres risikostyringsforanstaltninger eller underretningsforpligtelser i overensstemmelse med de forpligtelser, der er fastsat i artikel 18 og 20, på en nærmere angivet måde og inden for en nærmere angivet frist

   (e) pålægge disse enheder at underrette den eller de fysiske eller juridiske personer, som de leverer tjenester eller aktiviteter til, og som potentielt er berørt af en væsentlig cybertrussel, om eventuelle beskyttelsesforanstaltninger eller afhjælpende foranstaltninger, som disse fysiske eller juridiske personer kan træffe som reaktion på denne trussel

   (f) pålægge disse enheder at gennemføre de anbefalinger, der er fremsat som følge af en sikkerhedsrevision, inden for en rimelig frist

   (g) pålægge disse enheder at offentliggøre aspekter af manglende overholdelse af deres forpligtelser i henhold til dette direktiv på en nærmere angivet måde

   (h) fremsætte en offentlig erklæring, der identificerer den eller de juridiske og fysiske personer, som er ansvarlige for overtrædelsen af en forpligtelse, der er fastsat i dette direktiv, og overtrædelsens art

(i) pålægge eller anmode de relevante organer eller domstole om i henhold til national lovgivning at pålægge en administrativ bøde i henhold til artikel 31 ud over eller i stedet for de foranstaltninger, der er omhandlet i dette stykkes litra a)-h), afhængigt af omstændighederne i den enkelte sag.

5. Artikel 29, stk. 6-8, finder også anvendelse på tilsyns- og håndhævelsesforanstaltningerne i denne artikel for de vigtige enheder, der er opført i bilag II.

Artikel 31

Generelle betingelser for pålæggelse af administrative bøder

1. Medlemsstaterne sikrer, at administrative bøder, der pålægges væsentlige og vigtige enheder i henhold til denne artikel for overtrædelse af de forpligtelser, som er fastsat i dette direktiv, i hvert enkelt tilfælde er effektive, står i rimeligt forhold til overtrædelsen og har afskrækkende virkning.

2. Administrative bøder pålægges afhængigt af omstændighederne i hver enkelt sag i tillæg til eller i stedet for foranstaltninger som omhandlet i artikel 29, stk. 4, litra a)-i), artikel 29, stk. 5 og artikel 30, stk. 4, litra a)-h).

3. Når det skal besluttes, om der skal pålægges en administrativ bøde, og der træffes afgørelse om dens størrelse i hvert enkelt tilfælde, tages der som minimum behørigt hensyn til de i artikel 29, stk. 7, omhandlede elementer.

4. Medlemsstaterne sikrer, at overtrædelser af forpligtelserne i artikel 18 eller artikel 20 i overensstemmelse med nærværende artikels stk. 2 og 3 straffes med administrative bøder på maksimalt mindst 10 000 000 EUR eller op til 2 % af den samlede globale årsomsætning i den virksomhed, som den væsentlige eller vigtige enhed tilhører i det foregående regnskabsår, alt efter hvad der er højest.

5. Medlemsstaterne kan fastsætte beføjelser til at pålægge tvangsbøder for at tvinge en væsentlig eller vigtig enhed til at bringe en overtrædelse til ophør i overensstemmelse med en forudgående afgørelse truffet af den kompetente myndighed.

6. Uden at det berører tilsynsmyndighedernes korrigerende beføjelser i henhold til artikel 29 og 30, kan hver medlemsstat fastsætte regler om, hvorvidt og i hvilket omfang administrative bøder må pålægges offentlige forvaltningsorganer, jf. artikel 4, nr. 23, i henhold til bestemmelserne i nærværende direktiv.

Artikel 32

Overtrædelser, der medfører brud på persondatasikkerheden

1. Hvis de kompetente myndigheder konstaterer tegn på, at en væsentlig eller vigtig enheds overtrædelse af de forpligtelser, der er fastsat i artikel 18 og 20, medfører et brud på persondatasikkerheden som omhandlet i artikel 4, stk. 12, i forordning (EU) 2016/679, som skal anmeldes i henhold til nævnte forordnings artikel 33, underretter de inden for en rimelig frist de tilsynsmyndigheder, der er kompetente i henhold til nævnte forordnings artikel 55 og 56.

2. Hvis de tilsynsmyndigheder, der er kompetente i henhold til artikel 55 og 56 i forordning (EU) 2016/679, beslutter at udøve deres beføjelser i henhold til artikel 58, litra i), i nævnte forordning og pålægger en administrativ bøde, pålægger de kompetente myndigheder ikke en administrativ bøde for den samme overtrædelse i henhold til dette direktivs artikel 31. De kompetente myndigheder kan dog anvende de håndhævelsesforanstaltninger eller udøve de sanktionsbeføjelser, der er omhandlet i dette direktivs artikel 29, stk. 4, litra a)-i), artikel 29, stk. 5, og artikel 30, stk. 4, litra a)-h).

3. Hvis den tilsynsmyndighed, der er kompetent i henhold til forordning (EU) 2016/679, er etableret i en anden medlemsstat end den kompetente myndighed, kan den kompetente myndighed underrette tilsynsmyndigheden, der er etableret i samme medlemsstat.

Artikel 33

Sanktioner

1. Medlemsstaterne fastsætter regler om sanktioner, der skal anvendes i tilfælde af overtrædelser af de nationale regler, der er vedtaget i medfør af dette direktiv, og træffer alle nødvendige foranstaltninger til at sikre, at de gennemføres. Sanktionerne skal være effektive, stå i et rimeligt forhold til overtrædelsen og have afskrækkende virkning.

2. Medlemsstaterne giver senest [to] år efter dette direktivs ikrafttræden Kommissionen meddelelse om disse regler og foranstaltninger og underretter den uden unødig forsinkelse om alle senere ændringer, der berører dem.

Artikel 34

Gensidig bistand

1. Hvis en væsentlig eller vigtig enhed leverer tjenester i mere end én medlemsstat eller har sit hjemsted eller en repræsentant i én medlemsstat, men dets net- og informationssystemer er beliggende i en eller flere andre medlemsstater, samarbejder den kompetente myndighed i den medlemsstat, hvor hjemstedet eller en anden virksomhed eller repræsentanten befinder sig, og de kompetente myndigheder i de pågældende andre medlemsstater og bistår hinanden efter behov. Dette samarbejde indebærer som minimum, at:

   (a) de kompetente myndigheder, der anvender tilsyns- eller håndhævelsesforanstaltninger i en medlemsstat, via det fælles kontaktpunkt underretter og hører de kompetente myndigheder i de øvrige berørte medlemsstater om de tilsyns- og håndhævelsesforanstaltninger, der er truffet, og opfølgningen heraf i overensstemmelse med artikel 29 og 30

   (b) en kompetent myndighed kan anmode en anden kompetent myndighed om at træffe de tilsyns- eller håndhævelsesforanstaltninger, der er omhandlet i artikel 29 og 30

   (c) en kompetent myndighed yder efter modtagelse af en begrundet anmodning fra en anden kompetent myndighed bistand til den anden kompetente myndighed,

således at de tilsyns- eller håndhævelsesforanstaltninger, der er omhandlet i artikel 29 og 30, kan gennemføres på en effektiv, virkningsfuld og konsekvent måde. En sådan gensidig bistand kan omfatte anmodninger om oplysninger og tilsynsforanstaltninger, herunder anmodninger om at foretage inspektioner på stedet eller tilsyn uden for stedet eller målrettede sikkerhedskontroller. En kompetent myndighed, som en anmodning om bistand er rettet til, kan ikke afvise anmodningen, medmindre det efter en udveksling med de øvrige berørte myndigheder, ENISA og Kommissionen fastslås, enten at myndigheden ikke er kompetent til at yde den ønskede bistand, eller at den bistand, der anmodes om, ikke står i et rimeligt forhold til den kompetente myndigheds tilsynsopgaver, der udføres i overensstemmelse med artikel 29 eller artikel 30.

2. Når det er hensigtsmæssigt og efter fælles overenskomst, kan kompetente myndigheder fra forskellige medlemsstater gennemføre de i artikel 29 og 30 omhandlede fælles tilsynsforanstaltninger.

KAPITEL VII

Overgangsbestemmelser og afsluttende bestemmelser

Artikel 35

Evaluering

Kommissionen tager regelmæssigt dette direktivs funktion op til evaluering og forelægger en rapport for Europa-Parlamentet og Rådet. Rapporten skal navnlig vurdere relevansen af de i bilag I og II omhandlede sektorer, delsektorer, størrelser og typer af enheder for økonomien og samfundet i forbindelse med cybersikkerhed. Til dette formål og med henblik på yderligere at fremme det strategiske og operationelle samarbejde tager Kommissionen højde for rapporterne fra samarbejdsgruppen og CSIRT-netværket om de erfaringer, der er gjort på strategisk og operationelt plan. Den første rapport forelægges senest … [54 måneder efter datoen for dette direktivs ikrafttræden].

Artikel 36

Udøvelse af de delegerede beføjelser

1. Beføjelsen til at vedtage delegerede retsakter tillægges Kommissionen på de i denne artikel fastlagte betingelser.

2. Beføjelsen til at vedtage delegerede retsakter, jf. artikel 18, stk. 6, og artikel 21, stk. 2, tillægges Kommissionen for en periode på fem år fra den […].

3. Den i artikel 18, stk. 6, og artikel 21, stk. 2, omhandlede delegation af beføjelser kan til enhver tid tilbagekaldes af Europa-Parlamentet eller Rådet. En afgørelse om tilbagekaldelse bringer delegationen af de beføjelser, der er angivet i den pågældende afgørelse, til ophør. Den får virkning dagen efter offentliggørelsen af afgørelsen i Den Europæiske Unions Tidende eller på et senere tidspunkt, der angives i afgørelsen. Den berører ikke gyldigheden af delegerede retsakter, der allerede er i kraft.

4. Inden vedtagelsen af en delegeret retsakt hører Kommissionen eksperter, som er udpeget af hver enkelt medlemsstat, i overensstemmelse med principperne i den interinstitutionelle aftale af 13. april 2016 om bedre lovgivning.

5. Så snart Kommissionen vedtager en delegeret retsakt, giver den samtidigt Europa-Parlamentet og Rådet meddelelse herom.

6. En delegeret retsakt vedtaget i henhold til artikel 18, stk. 6, og artikel 21, stk. 2, træder kun i kraft, hvis hverken Europa-Parlamentet eller Rådet har gjort indsigelse inden for en frist på to måneder fra meddelelsen af den pågældende retsakt til Europa-Parlamentet og Rådet, eller hvis Europa-Parlamentet og Rådet inden udløbet af denne frist begge har underrettet Kommissionen om, at de ikke agter at gøre indsigelse. Fristen forlænges med to måneder på Europa-Parlamentets eller Rådets initiativ.

Artikel 37

Udvalgsprocedure

1. Kommissionen bistås af et udvalg. Dette udvalg er et udvalg som omhandlet i forordning (EU) nr. 182/2011.

2. Når der henvises til dette stykke, finder artikel 5 i forordning (EU) nr. 182/2011 anvendelse.

3. Når udvalgets udtalelse indhentes efter en skriftlig procedure, afsluttes proceduren uden noget resultat, hvis formanden for udvalget træffer beslutning herom, eller hvis et medlem af udvalget anmoder herom inden for tidsfristen for afgivelse af udtalelsen.

Artikel 38

Gennemførelse

1. Medlemsstaterne vedtager og offentliggør senest … [18 måneder efter direktivets ikrafttrædelsesdato] de love og administrative bestemmelser, der er nødvendige for at efterkomme dette direktiv. De underretter straks Kommissionen herom. De anvender disse love og bestemmelser fra den ... [én dag efter den dato, der er nævnt i første afsnit].

2. Lovene og bestemmelserne skal ved vedtagelsen indeholde en henvisning til dette direktiv eller skal ved offentliggørelsen ledsages af en sådan henvisning. De nærmere regler for henvisningen fastsættes af medlemsstaterne.

Artikel 39

Ændring af forordning (EU) nr. 910/2014

Artikel 19 i forordning (EU) nr. 910/2014 udgår.

Artikel 40

Ændring af direktiv (EU) 2018/1972

Artikel 40 og 41 i direktiv (EU) 2018/1972 udgår.

Artikel 41

Ophævelse

Direktiv (EU) 2016/1148 ophæves med virkning fra den [dato for direktivets gennemførelsesfrist].

Henvisninger til direktiv (EU) 2016/1148 betragtes som henvisninger til nærværende direktiv, jf. sammenligningstabellen i bilag III.

Artikel 42

Ikrafttræden

Dette direktiv træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Artikel 43

Adressater

Dette direktiv er rettet til medlemsstaterne.

Udfærdiget i Bruxelles, den […].

På Europa-Parlamentets vegne	*På Rådets vegne*
Formand	*Formand*

FINANSIERINGSOVERSIGT

Indholdsfortegnelse

1. FORSLAGETS/INITIATIVETS RAMME

1.1. Forslagets/initiativets betegnelse

Forslag til direktiv om foranstaltninger, der skal sikre et højt fælles cybersikkerhedsniveau i hele Unionen, og om ophævelse af direktiv (EU) 2016/1148

1.2. Berørte(e) politikområder *(programklynge)*

Kommunikationsnet, indhold og teknologi

1.3. Forslaget/initiativet vedrører:

☐ **en ny foranstaltning**

☐ **en ny foranstaltning som opfølgning på et pilotprojekt/en forberedende foranstaltning**[40]

☒ **en forlængelse af en eksisterende foranstaltning**

☐ **en sammenlægning eller omlægning af en eller flere foranstaltninger til en ny/anden foranstaltning**

1.4. Forslagets/initiativets begrundelse

1.4.1. Behov, der skal opfyldes på kort eller lang sigt, herunder en detaljeret tidsplan for iværksættelsen af initiativet

Formålet med revisionen er at øge cyberrobustheden i et omfattende sæt af virksomheder, der opererer i Den Europæiske Union, på tværs af alle relevante sektorer, at mindske uoverensstemmelser i modstandsdygtigheden på tværs af det indre marked i de sektorer, der allerede er omfattet af direktivet, og at forbedre niveauet af fælles situationsbevidsthed og den kollektive kapacitet til at forberede sig og reagere.

1.4.2. Merværdi ved en indsats fra EU's side (f.eks. koordineringsfordele, retssikkerhed, større effektivitet eller komplementaritet). Ved "merværdien ved en indsats fra EU's side" forstås her merværdien af EU's intervention i forhold til den værdi, som medlemsstaterne ville have skabt enkeltvis.

Modstandsdygtigheden over for cybertrusler i hele Unionen kan ikke være effektiv, hvis der gribes ind på en uensartet måde gennem nationale eller regionale siloer. NIS-direktivet har til formål at afhjælpe denne mangel ved at fastlægge en ramme for net- og informationssystemernes sikkerhed på nationalt plan og EU-plan. Den første regelmæssige evaluering af NIS-direktivet pegede imidlertid på en række iboende mangler, som i sidste ende har ført til betydelige forskelle mellem medlemsstaterne med hensyn til kapacitet, planlægning og beskyttelsesniveau, hvilket samtidig påvirker de lige vilkår for lignende virksomheder på det indre marked. En EU-indsats, der går videre end de nuværende foranstaltninger i NIS-direktivet, er primært begrundet i: i) problemets grænseoverskridende karakter, ii) EU-indsatsens potentiale til at forbedre og fremme effektive nationale politikker og iii) bidrag fra samordnede og samarbejdsbaserede politiske foranstaltninger vedrørende NIS til effektiv sikring af databeskyttelse og beskyttelse af privatlivets fred.

[40] Jf. finansforordningens artikel 58, stk. 2, litra a) hhv. b).

Målene kan derfor bedre opfyldes gennem en indsats på EU-plan, snarere end af medlemsstaterne alene.

1.4.3. Erfaringer fra lignende foranstaltninger

NIS-direktivet er det første horisontale instrument for det indre marked, der har til formål at forbedre nettenes og systemernes modstandsdygtighed over for cybersikkerhedsrisici i Unionen. Det har allerede i høj grad bidraget til at øge det fælles cybersikkerhedsniveau i medlemsstaterne. Evalueringen af, hvordan direktivet fungerer og gennemføres, har imidlertid peget på en række mangler, som ud over den stigende digitalisering og behovet for en mere tidssvarende reaktion skal afhjælpes i en revideret retsakt.

1.4.4. Sammenhæng med andre relevante instrumenter og eventuel synergivirkning

Det nye forslag er fuldt ud i overensstemmelse med og konsekvent i forhold til andre relaterede initiativer såsom forslaget til forordning om digital operationel modstandsdygtighed i den finansielle sektor ("DORA") og forslaget til direktiv om modstandsdygtigheden hos kritiske operatører af væsentlige tjenester. Det er også i overensstemmelse med den europæiske kodeks for elektronisk kommunikation, den generelle forordning om databeskyttelse og eIDAS-forordningen.

Forslaget er en væsentlig del af strategien for EU's sikkerhedsunion.

1.5. Varighed og finansielle virkninger

☐ **begrænset varighed**

– ☐ gældende fra [DD/MM]YYYY til [DD/MM]YYYY

– ☐ Finansielle virkninger fra YYYY til YYYY for forpligtelsesbevillinger og fra YYYY til YYYY for betalingsbevillinger.

☒ **ubegrænset varighed**

– Iværksættelse med en indkøringsperiode fra 2022 til 2025

– derefter gennemførelse i fuldt omfang.

1.6. Påtænkt(e) forvaltningsmetode(r)[41]

Direkte forvaltning ved Kommissionen

– ☒ i dens tjenestegrene, herunder ved dens personale i EU's delegationer

– ☐ i gennemførelsesorganer

☐ **Delt forvaltning** i samarbejde med medlemsstaterne

☐ **Indirekte forvaltning** ved at overlade budgetgennemførelsesopgaver til:

– ☐ tredjelande eller organer, som tredjelande har udpeget

– ☐ internationale organisationer og deres organer (angives nærmere)

– ☐ Den Europæiske Investeringsbank og Den Europæiske Investeringsfond

– X☐ organer, der er omhandlet i finansforordningens artikel 70 og 71

– ☐ offentligretlige organer

– ☐ privatretlige organer, der har fået overdraget samfundsopgaver, forudsat at de stiller tilstrækkelige finansielle garantier

– ☐ privatretlige organer, undergivet lovgivningen i en medlemsstat, som har fået overdraget gennemførelsen af et offentlig-privat partnerskab, og som stiller tilstrækkelige finansielle garantier

– ☐ personer, der har fået overdraget gennemførelsen af specifikke aktioner i den fælles udenrigs- og sikkerhedspolitik i henhold til afsnit V i traktaten om Den Europæiske Union, og som er udpeget i den relevante basisretsakt

– *Hvis der angives flere forvaltningsmetoder, gives der en nærmere forklaring i afsnittet "Bemærkninger".*

Bemærkninger

Den Europæiske Unions Agentur for Cybersikkerhed, ENISA, som ved forordningen om cybersikkerhed har fået tildelt et nyt permanent mandat, vil bistå medlemsstaterne og Kommissionen med gennemførelsen af det reviderede NIS-direktiv.

Som følge af det reviderede NIS-direktiv vil ENISA fra og med 2022/23 få yderligere indsatsområder. Selv om disse indsatsområder vil være omfattet af ENISA's generelle opgaver i henhold til dets mandat, vil de medføre en yderligere arbejdsbyrde for agenturet. ENISA skal nærmere bestemt ud over sine nuværende indsatsområder i henhold til Kommissionens

[41] Forklaringer vedrørende forvaltningsmetoder og henvisninger til finansforordningen findes på webstedet BudgWeb: https://myintracomm.ec.europa.eu/budgweb/DA/man/budgmanag/Pages/budgmanag.aspx.

forslag til et revideret NIS-direktiv også specifikt indarbejde følgende foranstaltninger i sit arbejdsprogram: i) udvikle og vedligeholde et europæisk sårbarhedsregister (artikel 6, stk. 2, i forslaget), ii) varetage sekretariatsfunktionen for det europæiske netværk af forbindelsesorganisationer for cyberkriser (EU-CyCLONe) (artikel 14 i forslaget) og udarbejde en årlig rapport om cybersikkerhedssituationen i EU (artikel 15 i forslaget), iii) støtte tilrettelæggelsen af peerevalueringer mellem medlemsstaterne (artikel 16 i forslaget), iv) indsamle aggregerede hændelsesdata fra medlemsstaterne og udarbejde teknisk vejledning (artikel 20, stk. 9, i forslaget), v) etablere og vedligeholde et register over enheder, der leverer grænseoverskridende tjenester (artikel 25 i forslaget).

Derfor vil der blive anmodet om 5 ekstra årsværk fra 2022 med et tilhørende budget på ca. 0,61 mio. EUR om året til dækning af disse nye stillinger (se særskilt finansieringsoversigt for agenturer).

2. FORVALTNINGSFORANSTALTNINGER

2.1. Bestemmelser om kontrol og rapportering

Angiv hyppighed og betingelser.

Kommissionen vil regelmæssigt evaluere, hvordan direktivet fungerer, og aflægge rapport til Europa-Parlamentet og Rådet, første gang tre år efter ikrafttrædelsen. Kommissionen vil også vurdere, om medlemsstaterne gennemfører direktivet korrekt.

2.2. Forvaltnings- og kontrolsystem(er)

2.2.1. Begrundelse for den/de påtænkte forvaltningsmetode(r), finansieringsmekanisme(r), betalingsvilkår og kontrolstrategi

Det kontor i GD CNECT, der har ansvaret for det politiske område, vil stå for gennemførelsen af direktivet.

2.2.2. Oplysninger om de konstaterede risici og det/de interne kontrolsystem(er), der etableres for at afbøde dem

Meget lav risiko, da NIS-direktivets økosystem allerede er på plads.

2.2.3. Vurdering af og begrundelse for kontrolforanstaltningernes omkostningseffektivitet (forholdet mellem kontrolforanstaltningerne og værdien af de forvaltede midler) samt vurdering af den forventede risiko for fejl (ved betaling og ved afslutning)

Ikke relevant. Kun anvendelse af administrationsbudgettet ("den samlede bevillingsramme").

2.3. Foranstaltninger til forebyggelse af svig og uregelmæssigheder

Angiv eksisterende eller påtænkte forebyggelses- og beskyttelsesforanstaltninger, f.eks. fra strategien til bekæmpelse af svig.

Ikke relevant. Kun anvendelse af administrationsbudgettet ("den samlede bevillingsramme").

3. FORSLAGETS/INITIATIVETS ANSLÅEDE FINANSIELLE VIRKNINGER

3.1. Udgiftsområde(r) i den flerårige finansielle ramme og foreslået(ede) ny(e) udgiftspost(er) på budgettet

Udgiftsområde i den flerårige finansielle ramme	Budgetpost	Udgiftens art	Bidrag			
	Nummer [Udgiftsområde…7……...……]	OB/IOB[42]	fra EFTA-lande[43]	fra kandidatlande[44]	fra tredjelande	iht. finansforordningens artikel [21, stk. 2, litra b)]
	20 02 06 administrationsudgifter 20 02 06	IOB	NEJ	NEJ	NEJ	NEJ

[42] OB = opdelte bevillinger/IOB = ikke-opdelte bevillinger.

[43] EFTA: Den Europæiske Frihandelssammenslutning.

[44] Kandidatlande og, efter omstændighederne, potentielle kandidatlande på Vestbalkan.

3.2. Anslåede virkninger for udgifterne

3.2.1. Sammenfatning af de anslåede virkninger for udgifterne

i mio. EUR (tre decimaler)

Udgiftsområde i den flerårige finansielle ramme	**<…>**	[Udgiftsområde……...…… …]

			2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Efter 2027***	**I ALT**
Aktionsbevillinger (opdelt efter de under afsnit 3.1 anførte budgetposter)	Forpligtelser	(1)									
	Betalinger	(2)									
Administrationsbevillinger finansieret over bevillingsrammen for programmer[45]	Forpligtelser = Betalinger	(3)									
Bevillinger finansieret over bevillingsrammen for programmet I ALT	Forpligtelser	=1+3									
	Betalinger	=2+3									

Udgiftsområde i den flerårige finansielle ramme	7	"Administration" Møder: Der afholdes normalt plenarmøder i NIS-samarbejdsgruppen fire gange om året. Kommissionen dækker udgifter til forplejning og rejser for repræsentanter fra 27 medlemsstater (en repræsentant pr. medlemsstat). Udgifterne til et møde kan beløbe sig til op til 15 000 EUR. Tjenesterejser: Tjenesterejser vedrører overvågning af gennemførelsen af NIS-direktivet. Eksempel: Inden for et år (maj 2019-juli 2020) skulle vi arrangere såkaldte "NIS-landebesøg" og besøge alle 27 medlemsstater for at drøfte gennemførelsen af

[45] Teknisk og/eller administrativ bistand og udgifter til støtte for gennemførelsen af EU's programmer og/eller aktioner (tidligere BA-poster), indirekte forskning, direkte forskning.

		NIS-direktivet i hele EU.

Dette afsnit skal udfyldes ved hjælp af arket vedrørende de administrative budgetoplysninger, der først skal indføres i Bilag til finansieringsoversigten, som uploades til DECIDE med henblik på høring af andre tjenestegrene.

i mio. EUR (tre decimaler)

		2021	2022	2023	2024	2025	2026	2027	*Efter 2027*	I ALT
Menneskelige ressourcer		1,14	1,14	1,14	1,14	1,14	1,14	**1,14**		**7,98**
Andre administrationsudgifter		**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**	**0,09**		**0,63**
Bevillinger I ALT under UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme	(Forpligtelser i alt = betalinger i alt)	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**		**8,61**

i mio. EUR (tre decimaler)

		2021	2022	2023	2024	2025	2026	2027	*Efter 2027*	I ALT
Bevillinger I ALT under samtlige UDGIFTSOMRÅDER i den flerårige finansielle ramme	Forpligtelser									
	Betalinger									

3.2.2. Sammenfatning af de anslåede virkninger for administrationsbevillingerne

– ☐ Forslaget/initiativet medfører ikke anvendelse af administrationsbevillinger

– ☐X Forslaget/initiativet medfører anvendelse af administrationsbevillinger som anført herunder:

i mio. EUR (tre decimaler)

Regnskabsår	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**I ALT**
UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme								
Menneskelige ressourcer	1,14	1,14	1,14	1,14	1,14	1,14	**1,14**	**7,98**
Andre administrationsudgifter	0,09	0,09	0,09	0,09	0,09	0,09	**0,09**	**0,63**
Subtotal UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme	1,23	1,23	1,23	1,23	1,23	1,23	**1,23**	**8,61**

Uden for UDGIFTSOMRÅDE 7[46] of the multiannual financial framework								
Menneskelige ressourcer								
Andre udgifter af administrativ art								
Subtotal uden for UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme								

I ALT	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**1,23**	**8,61**

Bevillingerne til menneskelige ressourcer og andre administrationsudgifter vil blive dækket ved hjælp af de bevillinger, der i forvejen er afsat til generaldirektoratets forvaltning af aktionen, og/eller ved intern omfordeling i generaldirektoratet, eventuelt suppleret med yderligere bevillinger, som tildeles det ansvarlige generaldirektorat i forbindelse med den årlige tildelingsprocedure under hensyntagen til de budgetmæssige begrænsninger.

[46] Teknisk og/eller administrativ bistand og udgifter til støtte for gennemførelsen af EU's programmer og/eller aktioner (tidligere BA-poster), indirekte forskning, direkte forskning.

3.2.2.1. Anslået behov for menneskelige ressourcer

– ☐ Forslaget/initiativet medfører ikke anvendelse af menneskelige ressourcer

– X☐ Forslaget/initiativet medfører anvendelse af menneskelige ressourcer som anført herunder:

Overslag angives i årsværk

Regnskabsår		**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
• **Stillinger i stillingsfortegnelsen (tjenestemænd og midlertidigt ansatte)**								
Hovedsædet og Kommissionens repræsentationskontorer		6	6	6	6	6	6	6
Delegationer								
Forskning								
• **Eksternt personale (i årsværk): årsværk) — KA, LA, UNE, V og JED** [47] Udgiftsområde 7								
Finansieret over UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme	— i hovedsædet	3	3	3	3	3	3	3
	— i delegationer							
Finansieret over bevillingsrammen for programmet [48]	— i hovedsædet							
	— i delegationer							
Forskning								
Andet (skal angives)								
I ALT		**9**	**9**	**9**	**9**	**9**	**9**	**9**

Personalebehovet vil blive dækket ved hjælp af det personale, som generaldirektoratet allerede har afsat til aktionen, og/eller interne rokader i generaldirektoratet, eventuelt suppleret med yderligere bevillinger, som tildeles det ansvarlige generaldirektorat i forbindelse med den årlige tildelingsprocedure under hensyntagen til de budgetmæssige begrænsninger.

Opgavebeskrivelse:

Tjenestemænd og midlertidigt ansatte	• Udarbejdelse af delegerede retsakter i henhold til artikel 18, stk. 6, artikel 21, stk. 2, og artikel 36 • Udarbejdelse af gennemførelsesretsakter i henhold til artikel 12, stk. 8, artikel 18, stk. 5, og artikel 20, stk. 11 • Oprettelse af et sekretariat for NIS-samarbejdsgruppen • Tilrettelæggelse af NIS-samarbejdsgruppens plenarmøder og arbejdsmøder • Koordinering af medlemsstaternes arbejde med forskellige dokumenter (retningslinjer, værktøjskasser osv.) • Kontakt til andre af Kommissionens tjenestegrene, ENISA og nationale myndigheder med henblik på gennemførelse af NIS-direktivet • Analyse af nationale metoder og bedste praksis i forbindelse med gennemførelsen af NIS-direktivet.
Eksternt personale	Støtte til ovenstående opgaver efter behov

[47] KA = kontraktansatte, LA: lokalt ansatte, UNE: udstationerede nationale eksperter, V: vikarer, JED: junioreksperter ved delegationerne.

[48] Delloft for eksternt personale under aktionsbevillingerne (tidligere BA-poster).

3.2.3. Tredjemands bidrag til finansieringen

Forslaget/initiativet:

– X☐ indeholder ikke bestemmelser om samfinansiering med tredjemand

– ☐ indeholder bestemmelser om samfinansiering, jf. følgende overslag:

Bevillinger i mio. EUR (tre decimaler)

Regnskabsår	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**I ALT**
Angiv organ, som deltager i samfinansieringen								
Samfinansierede bevillinger I ALT								

3.3. Anslåede virkninger for indtægterne

– ☐X Forslaget/initiativet har ingen finansielle virkninger for indtægterne

– ☐ Forslaget/initiativet har følgende finansielle virkninger:

☐ for egne indtægter

☐ for andre indtægter

Angiv, om indtægterne er formålsbestemte ☐

i mio. EUR (tre decimaler)

Indtægtspost på budgettet	Forslagets/initiativets virkninger[49]						
	2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
Artikel …….							

For indtægter, der er formålsbestemte, angives det, hvilke af budgettets udgiftsposter der påvirkes.

Andre bemærkninger (f.eks. om hvilken metode, der er benyttet til at beregne virkningerne for indtægterne).

[49] Med hensyn til EU's traditionelle egne indtægter (told og sukkerafgifter) opgives beløbene netto, dvs. bruttobeløb, hvorfra der er trukket opkrævningsomkostninger på 20 %.

BILAG
til FINANSIERINGSOVERSIGT

Forslagets/initiativets navn

Forslag til direktiv om ændring af Europa-Parlamentets og Rådets direktiv (EU) 2016/1148 af 6. juli 2016 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen

……
……

1. PERSONALEBEHOV OG PERSONALEOMKOSTNINGER

2. ANDRE ADMINISTRATIONSUDGIFTER

3. ANVENDTE METODER TIL BEREGNING AF OMKOSTNINGSOVERSLAG

3.1 Menneskelige ressourcer

3.2 Andre administrationsudgifter

*Dette bilag, **som skal udfyldes af hvert GD/hver tjenestegren, der deltager i forslaget/initiativet**, skal ledsage finansieringsoversigten ved høring på tværs af tjenestegrenene.*

Datatabellerne er brugt som kilde til tabellerne i finansieringsoversigten. De er udelukkende til internt brug i Kommissionen.

1. Personalebehov og personaleomkostninger

☐ Forslaget/initiativet medfører ikke anvendelse af menneskelige ressourcer

X☐ Forslaget/initiativet medfører anvendelse af menneskelige ressourcer som anført herunder:

i mio. EUR (tre decimaler)

UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme		**2021**		**2022**		**2023**		**2024**		**2025**		**2026**		**2027**		**I ALT**	
		årsværk	Bevillinger	årsværk	Bevillinger	årsværk	Bevillinger	årsværk	Bevillinger	årsværk	Bevillinger	årsværk	Bevillinger	årsværk	Bevillinger	årsværk	Bevillinger
• Stillinger i stillingsfortegnelsen (tjenestemænd og midlertidigt ansatte)																	
Hovedsædet og Kommissionens repræsentationskontorer	AD	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	42	6,3
	AST																
i EU-delegationer	AD																
	AST																
• Eksternt personale[50] 0,24																	
Samlet bevillingsramme	KA	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	21	1,68
	UNE																
	V																
i EU-delegationer	KA																
	LA																
	UNE																

[50] KA = kontraktansatte, LA: lokalt ansatte, UNE: udstationerede nationale eksperter, V: vikarer, JED: junioreksperter ved delegationerne.

	V																
	JED																
Andre budgetposter (*skal angives*)																	
Subtotal — UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme		9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	63	7,98

Personalebehovet vil blive dækket ved hjælp af det personale, som generaldirektoratet allerede har afsat til aktionen, og/eller interne rokader i generaldirektoratet, eventuelt suppleret med yderligere bevillinger, som tildeles det ansvarlige generaldirektorat i forbindelse med den årlige tildelingsprocedure under hensyntagen til de budgetmæssige begrænsninger.

Uden for UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme			2021		2022		2023		2024		2025		2025		2025		I ALT	
			årsværk	Bevillinger	årsværk	Bevillinger	årsværk	Bevillinger	årsværk	Bevillinger	årsværk	Bevillinger	årsværk	Bevillinger	årsværk	Bevillinger	årsværk	Bevillinger
• Stillinger i stillingsfortegnelsen (tjenestemænd og midlertidigt ansatte)																		
Forskning		AD																
		AST																
• Eksternt personale[51]																		
Eksternt personale finansieret over aktionsbevillinger (tidligere BA-poster).	— i hovedsædet	KA																
		UNE																
		V																
	— i EU-delegationer	KA																
		LA																
		UNE																
		V																
		JED																
Forskning		KA																
		UNE																
		V																
Andre budgetposter (*skal*																		

[51] KA = kontraktansatte, LA: lokalt ansatte, UNE: udstationerede nationale eksperter, V: vikarer, JED: junioreksperter ved delegationerne.

angives)																	
Subtotal -– uden for UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme																	

Personalebehovet vil blive dækket ved hjælp af det personale, som generaldirektoratet allerede har afsat til aktionen, og/eller interne rokader i generaldirektoratet, eventuelt suppleret med yderligere bevillinger, som tildeles det ansvarlige generaldirektorat i forbindelse med den årlige tildelingsprocedure under hensyntagen til de budgetmæssige begrænsninger.

Anslåede virkninger for ENISA's menneskelige ressourcer

Den Europæiske Unions Agentur for Cybersikkerhed, ENISA, som ved forordningen om cybersikkerhed har fået tildelt et nyt permanent mandat, vil bistå medlemsstaterne og Kommissionen med gennemførelsen af det reviderede NIS-direktiv.

Som følge af det reviderede NIS-direktiv vil ENISA fra og med 2022/23 få yderligere indsatsområder. Selv om disse indsatsområder vil være omfattet af ENISA's generelle opgaver i henhold til dets mandat, vil de medføre en yderligere arbejdsbyrde for agenturet. ENISA skal nærmere bestemt ud over sine nuværende indsatsområder i henhold til Kommissionens forslag til et revideret NIS-direktiv også specifikt indarbejde følgende foranstaltninger i sit arbejdsprogram: i) udvikle og vedligeholde et europæisk sårbarhedsregister (artikel 6, stk. 2, i forslaget), ii) varetage sekretariatsfunktionen for det europæiske netværk af forbindelsesorganisationer for cyberkriser (EU-CyCLONe) (artikel 14 i forslaget) og udarbejde en årlig rapport om cybersikkerhedssituationen i EU (artikel 15 i forslaget), iii) støtte tilrettelæggelsen af peerevalueringer mellem medlemsstaterne (artikel 16 i forslaget), iv) indsamle aggregerede hændelsesdata fra medlemsstaterne og udarbejde teknisk vejledning (artikel 20, stk. 9, i forslaget), v) etablere og vedligeholde et register over enheder, der leverer grænseoverskridende tjenester (artikel 25 i forslaget).

Derfor vil der blive anmodet om 5 ekstra årsværk fra 2022 med et tilhørende budget på ca. 0,61 mio. EUR om året til dækning af disse nye stillinger (se særskilt finansieringsoversigt for agenturer).

Derfor vil der blive anmodet om 5 ekstra årsværk fra 2022 med et tilsvarende budget til dækning af disse nye stillinger.

☐ Forslaget/initiativet medfører ikke anvendelse af administrationsbevillinger

☐X Forslaget/initiativet medfører anvendelse af administrationsbevillinger som anført herunder:

i mio. EUR (tre decimaler)

	År **N** [52] **2022**	År **n+1** **2023**	År **n+2** **2024**	År **n+3** **2025**	Der indsættes flere år, hvis virkningerne varer længere (jf. punkt 1.6)			**I ALT**
Midlertidigt ansatte (AD)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**

[52] År n er det år, hvor gennemførelsen af forslaget/initiativet begynder. I stedet for "n" indsættes det forventede første gennemførelsesår (f.eks.: 2021). Dette gælder også for de følgende år.

Midlertidigt ansatte (AST)								
Kontraktansatte	0,160	0,160	0,160	0,160	0,160	0,160		
Udstationerede nationale eksperter								**0,96**

I ALT	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

Personalebehov (i årsværk):

	År **N** [53] **2022**	År **n+1** **2023**	År **n+2** **2024**	År **n+3** **2025**	Der indsættes flere år, hvis virkningerne varer længere (jf. punkt 1.6)			**I ALT**
Midlertidigt ansatte (AD)	3	3	3	3	3	3		**18**
Midlertidigt ansatte (AST)								
Kontraktansatte	2	2	2	2	2	2		**12**
Udstationerede nationale eksperter								

[53] År n er det år, hvor gennemførelsen af forslaget/initiativet begynder. I stedet for "n" indsættes det forventede første gennemførelsesår (f.eks.: 2021). Dette gælder også for de følgende år.

I ALT	**5**	**5**	**5**	**5**	**5**	**5**		**30**

2. Andre administrationsudgifter

☐ Forslaget/initiativet medfører ikke anvendelse af administrationsbevillinger

X☐ Forslaget/initiativet medfører anvendelse af administrationsbevillinger som anført herunder:

i mio. EUR (tre decimaler)

UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**I alt**
I hovedsædet								
Udgifter til tjenesterejser og repræsentation	0,03	0,03	0,03	0,03	0,03	0,03	0,03	**0,21**
Udgifter til konferencer og møder	0,06	0,06	0,06	0,06	0,06	0,06	0,06	**0,42**
Udvalg[54]								
Undersøgelser og konsultationer								
Informations- og forvaltningssystemer								
IKT-udstyr og -tjenester[55]								

[54] Oplys, hvilken type udvalg det drejer sig om, og hvilken gruppe det tilhører.

[55] IKT: Informations- og kommunikationsteknologi: DIGIT skal høres.

Andre budgetposter (*angiv, hvis relevant*)								
I EU-delegationer								
Udgifter til tjenesterejser, konferencer og repræsentation								
Faglig videreuddannelse								
Udgifter til køb og leje m.m.								
Udstyr, møbler, forsyninger og tjenesteydelser								
Subtotal UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme	0,09	0,09	0,09	0,09	0,09	0,09	0,09	**0,63**

i mio. EUR (tre decimaler)

Uden for UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme	**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	**I alt**
Udgifter til teknisk og administrativ bistand (omfatter ikke eksternt personale) finansieret over aktionsbevillinger (tidligere BA-poster)								
— i hovedsædet								
— i EU-delegationer								
Andre forskningsrelaterede administrationsudgifter								
Andre budgetposter (*angiv, hvis relevant*)								
Subtotal – Uden for UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme								

I ALT **UDGIFTSOMRÅDE 7 og Uden for UDGIFTSOMRÅDE 7** i den flerårige finansielle ramme	1,23	1,23	1,23	1,23	1,23	1,23	1,23	**8,61**

Administrationsbevillingerne vil blive dækket ved hjælp af de bevillinger, som GD'et allerede har afsat til forvaltningen af aktionen, og/eller ved omfordeling, hvortil kommer de eventuelle yderligere bevillinger, som tildeles det ansvarlige GD i forbindelse med den årlige tildelingsprocedure under hensyntagen til de budgetmæssige begrænsninger.

3. Anvendte metoder til beregning af omkostningsoverslag

3.1 Menneskelige ressourcer

Denne del beskriver beregningsmetoden til vurdering af de menneskelige ressourcer, der anses for at være nødvendige (forventet arbejdsbyrde, herunder særlige job (Sysper 2 work profiles), personalekategorier og de tilsvarende gennemsnitlige omkostninger)

UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme
NB: Gennemsnitlige omkostninger for hver personalekategori i hovedsædet kan ses på BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx
• Tjenestemænd og midlertidigt ansatte 6 årsværk, tjenestemænd (gennemsnitlige udgifter 0,150) = 0,9 pr. år - Udarbejdelse af delegerede retsakter i henhold til artikel 18, stk. 6, artikel 21, stk. 2, og artikel 36 - Udarbejdelse af gennemførelsesretsakter i henhold til artikel 12, stk. 8, artikel 18, stk. 5, og artikel 20, stk. 11 - Oprettelse af et sekretariat for NIS-samarbejdsgruppen - Tilrettelæggelse af NIS-samarbejdsgruppens plenarmøder og arbejdsmøder - Koordinering af medlemsstaternes arbejde med forskellige dokumenter (retningslinjer, værktøjskasser osv.) - Kontakt til andre af Kommissionens tjenestegrene, ENISA og nationale myndigheder med henblik på gennemførelse af NIS-direktivet - Analyse af nationale metoder og bedste praksis i forbindelse med gennemførelsen af NIS-direktivet.
• Eksternt personale 3 KA (gennemsnitlig udgift 0,08) = 0,24 pr. år - Støtte til ovenstående opgaver efter behov

Uden for UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme
• Kun stillinger finansieret over forskningsbudgettet
• Eksternt personale

3.2 Andre administrationsudgifter

Oplys nærmere om den beregningsmetode, der anvendes for hver budgetpost,

herunder de underliggende antagelser (f.eks. antal møder om året, gennemsnitlige omkostninger m.v.)

UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme
Møder: Der afholdes normalt plenarmøder i NIS-samarbejdsgruppen fire gange om året. Kommissionen dækker udgifter til forplejning og rejser for repræsentanter fra 27 medlemsstater (en repræsentant pr. medlemsstat). Udgifterne til et møde kan beløbe sig til op til 15 000 EUR, hvilket giver 60 000 EUR om året. Tjenesterejser: Tjenesterejser vedrører overvågning af gennemførelsen af NIS-direktivet. Eksempel: Inden for et år (maj 2019-juli 2020) skulle vi arrangere såkaldte "NIS-landebesøg" og besøge alle 27 medlemsstater for at drøfte gennemførelsen af NIS-direktivet i hele EU.

Uden for UDGIFTSOMRÅDE 7 i den flerårige finansielle ramme

BILAG 7

til

KOMMISSIONENS AFGØRELSE

om de interne regler for gennemførelse af Den Europæiske Unions almindelige budget (sektionen for Europa-Kommissionen) rettet til Kommissionens tjenestegrene

FINANSIERINGSOVERSIGT (AGENTURER)

Denne finansieringsoversigt dækker anmodningen om at øge ENISA's personale med 5 årsværk fra 2022 for at udføre supplerende aktiviteter i forbindelse med gennemførelsen af NIS-direktivet. Disse aktiviteter er allerede omfattet af ENISA's mandat.

Indholdsfortegnelse

1. FORSLAGETS/INITIATIVETS RAMME

1.1. Forslagets/initiativets betegnelse

Forslag til direktiv om foranstaltninger, der skal sikre et højt fælles cybersikkerhedsniveau i hele Unionen, og om ophævelse af direktiv (EU) 2016/1148

1.2. Berørt(e) politikområde(r)

Kommunikationsnet, indhold og teknologi

1.3. Forslaget vedrører

☐ **en ny foranstaltning**

☐ **en ny foranstaltning som opfølgning på et pilotprojekt/en forberedende foranstaltning**[56]

☒ **en forlængelse af en eksisterende foranstaltning**

☐ **en sammenlægning af en eller flere foranstaltninger til en anden/en ny foranstaltning**

1.4. Mål

1.4.1. Generelle mål

Formålet med revisionen er at øge cyberrobustheden i et omfattende sæt af virksomheder, der opererer på tværs af alle relevante sektorer i Den Europæiske Union, at mindske uoverensstemmelser i modstandsdygtigheden på tværs af det indre marked i de sektorer, der allerede er omfattet af direktivet, og at forbedre niveauet af fælles situationsbevidsthed og den kollektive kapacitet til at forberede sig og reagere.

1.4.2. Specifikke mål

For at løse problemet med lav cyberrobusthed hos virksomheder, der opererer i Den Europæiske Union, er det specifikke mål at sikre, at enheder i alle sektorer, der er afhængige af net- og informationssystemer, og som leverer vigtige tjenester til økonomien og samfundet som helhed, er forpligtet til at træffe cybersikkerhedsforanstaltninger og foretage underretninger om hændelser med henblik på at øge den generelle cyberrobusthed i hele det indre marked.

For at løse problemet med inkonsekvent modstandsdygtighed på tværs af medlemsstater og sektorer er det specifikke mål at sikre, at alle enheder, som er aktive i sektorer, der er omfattet af de retlige rammer for net- og informationssikkerhed, og som er af samme størrelse og har en sammenlignelig rolle, er underlagt den samme reguleringsordning (enten inden for eller uden for anvendelsesområdet), uanset hvilken jurisdiktion de hører under i EU.

For at sikre, at alle enheder, der er aktive i sektorer, som er omfattet af de retlige rammer for net- og informationssikkerhed, skal følge de samme forpligtelser baseret på begrebet risikostyring, når det drejer sig om sikkerhedsforanstaltninger, og skal foretage underretninger om alle hændelser på grundlag af et ensartet sæt kriterier, er de specifikke mål at sikre, at de kompetente myndigheder håndhæver de regler, der er fastsat i retsakten, mere effektivt

[56] Jf. finansforordningens artikel 58, stk. 2, litra a) hhv. b).

gennem tilpassede tilsyns- og håndhævelsesforanstaltninger og at sikre et sammenligneligt niveau af ressourcer på tværs af medlemsstaterne, som tildeles de kompetente myndigheder, så de kan udføre de centrale opgaver, der er fastlagt i NIS-rammen.

For at løse problemet med fælles situationsbevidsthed og mangel på fælles kriserespons er det specifikke mål at sikre, at vigtige oplysninger udveksles mellem medlemsstaterne ved at indføre klare forpligtelser for de kompetente myndigheder til at udveksle oplysninger og samarbejde i forbindelse med cybertrusler og -hændelser samt ved at udvikle en fælles operationel kriseberedskabskapacitet på EU-plan.

1.4.3. Forventede resultater og virkninger

Angiv, hvilke virkninger forslaget/initiativet forventes at få for modtagerne/målgruppen.

Forslaget forventes at medføre betydelige fordele: Skøn viser, at det kan føre til en reduktion af omkostningerne ved cybersikkerhedshændelser med 11,3 mia. EUR. Det sektorspecifikke anvendelsesområde vil blive udvidet betydeligt inden for NIS-rammen, men ud over ovennævnte fordele vil den byrde, der kan opstå som følge af NIS-kravene, navnlig ud fra et tilsynsperspektiv, også være afbalanceret for såvel de nye enheder, der skal dækkes, som de kompetente myndigheder. Dette skyldes, at den nye NIS-ramme vil etablere en tostrenget tilgang med fokus på store og centrale enheder og en differentiering af tilsynsordningen, der kun tillader efterfølgende tilsyn for et stort antal enheder, navnlig dem, der anses for at være "vigtige", men endnu ikke "væsentlige".

Overordnet set vil forslaget føre til effektive afvejninger og synergier med det bedste potentiale blandt alle de analyserede politiske løsningsmodeller og sikre en øget og konsekvent grad af cyberrobusthed hos centrale enheder i hele Unionen, hvilket i sidste ende vil føre til omkostningsbesparelser for både virksomheder og samfundet.

Forslaget vil også medføre visse overholdelses- og håndhævelsesomkostninger for de relevante myndigheder i medlemsstaterne (det blev anslået, at ressourcerne skulle øges med i alt ca. 20-30 %). Den nye ramme vil imidlertid også medføre betydelige fordele takket være et bedre overblik over og interaktion med centrale virksomheder, øget operationelt samarbejde henover grænserne samt gensidig bistand og peerevalueringsmekanismer. Dette vil føre til en generel forøgelse af cybersikkerhedskapaciteterne på tværs af medlemsstaterne.

For de virksomheder, der vil være omfattet af NIS-rammen, anslås det, at deres nuværende udgifter til IKT-sikkerhed vil skulle øges med 22 % i de første år efter indførelsen af den nye NIS-ramme (dette tal vil være 12 % for virksomheder, der allerede er omfattet af det nuværende NIS-direktiv). Denne gennemsnitlige stigning i udgifterne til IKT-sikkerhed vil imidlertid medføre en forholdsmæssig fordel ved sådanne investeringer, navnlig på grund af en betydelig reduktion af omkostningerne ved cybersikkerhedshændelser (anslået til 118 mia. EUR over ti år).

Små virksomheder og mikrovirksomheder vil blive undtaget fra NIS-rammens anvendelsesområde. For mellemstore virksomheder kan det forventes, at der vil ske en stigning i udgifterne til IKT-sikkerhed i de første år efter indførelsen af den nye NIS-ramme. Samtidig vil en styrkelse af sikkerhedsniveauet for disse enheder også kunne tilskynde dem til at styrke deres cybersikkerhedskapaciteter og bidrage til en forbedring af deres IKT-risikostyring.

Den foretrukne løsning vil have virkninger for de nationale budgetter og myndigheder: Der forventes en stigning på omkring 20-30 % i ressourcerne på kort og mellemlang sigt.

Der forventes ingen andre væsentlige eller negative virkninger. Forslaget forventes at føre til mere robuste cybersikkerhedskapaciteter og vil derfor have en mere betydelig dæmpende virkning på antallet og alvoren af hændelser, herunder brud på datasikkerheden. Det vil sandsynligvis også have en positiv indvirkning med hensyn til at sikre lige vilkår på tværs af medlemsstaterne for alle enheder, der er omfattet af anvendelsesområdet for net- og informationssikkerhed, og mindske asymmetrier i cybersikkerhedsoplysninger.

1.4.4. Resultatindikatorer

Angiv indikatorerne til overvågning af fremskridt og resultater.

Vurderingen af indikatorerne vil blive foretaget af Kommissionen med støtte fra ENISA og samarbejdsgruppen, første gang tre år efter ikrafttrædelsen af den nye NIS-retsakt. Følgende overvågningsindikatorer vil bl.a. danne grundlag for vurderingen af NIS-undersøgelsens succes:

- Bedre håndtering af hændelser: Ved at træffe cybersikkerhedsforanstaltninger forbedrer virksomhederne ikke blot deres evne til at undgå visse hændelser fuldt ud, men også deres kapacitet til at reagere på hændelser. Succeskriterier er derfor i) reduktion af den gennemsnitlige tid, det tager at opdage en hændelse, ii) den tid, det gennemsnitligt tager organisationer at blive genoprettet efter en hændelse, og iii) de gennemsnitlige omkostninger ved en skade forårsaget af en hændelse.

- Øget bevidsthed om cybersikkerhedsrisici i virksomhedernes øverste ledelse: Ved at kræve, at virksomheder træffer foranstaltninger, vil et revideret NIS-direktiv bidrage til at øge bevidstheden om cybersikkerhedsrelaterede risici hos den øverste ledelse. Dette kan måles ved at undersøge, i hvilket omfang virksomheder under anvendelsesområdet for NIS prioriterer cybersikkerhed i interne virksomhedspolitikker og -processer, hvilket fremgår af intern dokumentation, relevante uddannelsesprogrammer og oplysningsaktiviteter for medarbejderne samt prioritering af sikkerhedsrelaterede IKT-investeringer. Ledelsen af alle væsentlige og vigtige enheder bør også være opmærksom på de regler, der er fastsat i NIS-direktivet.

- Tilpasning af sektorspecifikke udgifter: Udgifterne til IKT-sikkerhed varierer betydeligt fra sektor til sektor i EU. Ved at kræve, at virksomheder i flere sektorer træffer foranstaltninger, bør afvigelser fra de gennemsnitlige sektorspecifikke udgifter til IKT-sikkerhed som en procentdel af de samlede IKT-udgifter mindskes mellem sektorerne og på tværs af medlemsstaterne.

- Stærkere kompetente myndigheder og øget samarbejde: Et revideret NIS-direktiv vil potentielt give de kompetente myndigheder yderligere opgaver. Dette vil have en målbar indvirkning på de finansielle og menneskelige ressourcer, der afsættes til cybersikkerhedsagenturer på nationalt plan, og bør også have en positiv indvirkning på de kompetente myndigheders evne til proaktivt at samarbejde og dermed øge antallet af tilfælde, hvor kompetente myndigheder samarbejder med hinanden med henblik på at håndtere grænseoverskridende hændelser eller udføre fælles tilsynsaktiviteter.

- Øget informationsudveksling: Det reviderede NIS-direktiv vil også forbedre informationsudvekslingen mellem virksomhederne og med de kompetente myndigheder. Et af målene for revisionen kunne være at øge antallet af enheder, der deltager i de forskellige former for informationsudveksling.

1.5. Forslagets/initiativets begrundelse

1.5.1. Behov, der skal opfyldes på kort eller lang sigt, herunder en detaljeret tidsplan for iværksættelsen af initiativet

Formålet med forslaget er at øge cyberrobustheden i et omfattende sæt af virksomheder, der opererer på tværs af alle relevante sektorer i Den Europæiske Union, at mindske uoverensstemmelser i modstandsdygtigheden på tværs af det indre marked i de sektorer, der allerede er omfattet af direktivet, og at forbedre niveauet af fælles situationsbevidsthed og den kollektive kapacitet til at forberede sig og reagere. Det vil bygge videre på de resultater, der er opnået med gennemførelsen af direktiv (EU) 2016/1148 i de seneste 4 år.

1.5.2. Merværdi ved en indsats fra EU's side (f.eks. koordineringsfordele, retssikkerhed, større effektivitet eller komplementaritet). Ved "merværdien ved en indsats fra EU's side" forstås her merværdien af EU's intervention i forhold til den værdi, som medlemsstaterne ville have skabt enkeltvis.

Modstandsdygtigheden over for cybertrusler i hele Unionen kan ikke være effektiv, hvis der gribes ind på en uensartet måde gennem nationale eller regionale siloer. NIS-direktivet har til formål at afhjælpe denne mangel ved at fastlægge en ramme for net- og informationssystemernes sikkerhed på nationalt plan og EU-plan. Den første regelmæssige evaluering af NIS-direktivet pegede imidlertid på en række iboende mangler, som i sidste ende har ført til betydelige forskelle mellem medlemsstaterne med hensyn til kapacitet, planlægning og beskyttelsesniveau, hvilket samtidig påvirker de lige vilkår for lignende virksomheder på det indre marked.

En EU-indsats, der går videre end de nuværende foranstaltninger i NIS-direktivet, er primært begrundet i: i) problemets grænseoverskridende karakter, ii) EU-indsatsens potentiale til at forbedre og fremme effektive nationale politikker og iii) bidrag fra samordnede og samarbejdsbaserede politiske foranstaltninger vedrørende NIS til effektiv sikring af databeskyttelse og beskyttelse af privatlivets fred.

Målene kan derfor bedre opfyldes gennem en indsats på EU-plan, snarere end af medlemsstaterne alene.

1.5.3. Erfaringer fra lignende foranstaltninger

NIS-direktivet er det første horisontale instrument for det indre marked, der har til formål at forbedre nettenes og systemernes modstandsdygtighed over for cybersikkerhedsrisici i Unionen. Siden det trådte i kraft i 2016, har det allerede i høj grad bidraget til at øge det fælles cybersikkerhedsniveau i medlemsstaterne. Evalueringen af, hvordan direktivet fungerer og gennemføres, har imidlertid peget på en række mangler, som ud over den stigende digitalisering og behovet for en mere tidssvarende reaktion skal afhjælpes i en revideret retsakt.

1.5.4. Sammenhæng med den flerårige finansielle ramme og eventuelle synergivirkninger med andre relevante instrumenter

Det nye forslag er fuldt ud i overensstemmelse med og konsekvent i forhold til andre relaterede initiativer såsom forslaget til forordning om digital operationel modstandsdygtighed i den finansielle sektor ("DORA") og forslaget til direktiv om modstandsdygtigheden hos kritiske operatører af væsentlige tjenester. Det er også i overensstemmelse med den europæiske kodeks for elektronisk kommunikation, den generelle forordning om databeskyttelse og eIDAS-forordningen.

Forslaget er en væsentlig del af strategien for EU's sikkerhedsunion.

1.5.5. Vurdering af de forskellige tilgængelige finansieringsmuligheder, herunder muligheden for omfordeling

ENISA's forvaltning af disse opgaver kræver særlige profiler og en ekstra arbejdsbyrde, som ikke kan absorberes uden en forøgelse af de menneskelige ressourcer.

1.6. Forslagets/initiativets varighed og finansielle virkninger

☐ **begrænset varighed**

– ☐ Forslag/initiativ gældende fra [DD/MM]YYYY til [DD/MM]YYYY

– ☐ Finansielle virkninger fra YYYY til YYYY

☒ **ubegrænset varighed**

– Iværksættelse med en indkøringsperiode fra 2022 til 2025

– derefter gennemførelse i fuldt omfang.

1.7. Påtænkt(e) forvaltningsmetode(r)[57]

☒ **Direkte forvaltning** ved Kommissionen

gennem

– ☐ forvaltningsorganer

☐ **Delt forvaltning** i samarbejde med medlemsstaterne

☐X **Indirekte forvaltning** ved at overlade budgetgennemførelsesopgaver til:

☐ internationale organisationer og deres organer (angives nærmere)

☐ Den Europæiske Investeringsbank og Den Europæiske Investeringsfond

☒ de organer, der er omhandlet i finansforordningens artikel 70 og 71

☐ offentligretlige organer

☐ privatretlige organer, der har fået overdraget samfundsopgaver, forudsat at de stiller tilstrækkelige finansielle garantier

☐ privatretlige organer, undergivet lovgivningen i en medlemsstat, som har fået overdraget gennemførelsen af et offentlig-privat partnerskab, og som stiller tilstrækkelige finansielle garantier

☐ personer, der har fået overdraget gennemførelsen af specifikke aktioner i den fælles udenrigs- og sikkerhedspolitik i henhold til afsnit V i traktaten om Den Europæiske Union, og som er udpeget i den relevante basisretsakt

Bemærkninger

Den Europæiske Unions Agentur for Cybersikkerhed, ENISA, som ved forordningen om cybersikkerhed har fået tildelt et nyt permanent mandat, vil bistå medlemsstaterne og Kommissionen med gennemførelsen af det reviderede NIS-direktiv.

Som følge af det reviderede NIS-direktiv vil ENISA fra og med 2022/23 få yderligere indsatsområder. Selv om disse indsatsområder vil være omfattet af ENISA's generelle opgaver i henhold til dets mandat, vil de medføre en yderligere arbejdsbyrde for agenturet. ENISA skal nærmere bestemt ud over sine nuværende indsatsområder i henhold til Kommissionens forslag til et revideret NIS-direktiv også specifikt indarbejde følgende foranstaltninger i sit arbejdsprogram: i) udvikle og vedligeholde et europæisk sårbarhedsregister (artikel 6, stk. 2, i forslaget), ii) varetage sekretariatsfunktionen for det

[57] Forklaringer vedrørende forvaltningsmetoder og henvisninger til finansforordningen findes på webstedet BudgWeb: https://myintracomm.ec.europa.eu/budgweb/DA/man/budgmanag/Pages/budgmanag.aspx.

europæiske netværk af forbindelsesorganisationer for cyberkriser (EU-CyCLONe) (artikel 14 i forslaget) og udarbejde en årlig rapport om cybersikkerhedssituationen i EU (artikel 15 i forslaget), iii) støtte tilrettelæggelsen af peerevalueringer mellem medlemsstaterne (artikel 16 i forslaget), iv) indsamle aggregerede hændelsesdata fra medlemsstaterne og udarbejde teknisk vejledning (artikel 20, stk. 9, i forslaget), v) etablere og vedligeholde et register over enheder, der leverer grænseoverskridende tjenester (artikel 25 i forslaget).

Derfor vil der blive anmodet om 5 ekstra årsværk fra 2022 med et tilsvarende budget på ca. 0,61 mio. EUR om året til dækning af disse nye stillinger.

2. FORVALTNINGSFORANSTALTNINGER

2.1. Bestemmelser om kontrol og rapportering

Angiv hyppighed og betingelser.

Kommissionen vil regelmæssigt evaluere, hvordan direktivet fungerer, og aflægge rapport til Europa-Parlamentet og Rådet, første gang tre år efter ikrafttrædelsen.

Kommissionen vil også vurdere, om medlemsstaterne gennemfører direktivet korrekt.

Overvågningen og rapporteringen af forslaget vil følge principperne i ENISA's permanente mandat i henhold til forordning (EU) 2019/881 (forordningen om cybersikkerhed).

De datakilder, der anvendes til den planlagte overvågning, vil hovedsagelig komme fra ENISA, samarbejdsgruppen, CSIRT-netværket og medlemsstaternes myndigheder. Ud over de data, der indsamles fra rapporterne (herunder de årlige aktivitetsrapporter) fra ENISA, samarbejdsgruppen og CSIRT-netværket, vil der blive anvendt særlige dataindsamlingsværktøjer efter behov (f.eks. rundspørger over for nationale myndigheder, Eurobarometer og rapporter fra kampagnen "Cybersecurity Month" og de fælleseuropæiske øvelser).

2.2. Forvaltnings- og kontrolsystem(er)

2.2.1. Begrundelse for den/de påtænkte forvaltningsmetode(r), finansieringsmekanisme(r), betalingsvilkår og kontrolstrategi

Det kontor i GD CNECT, der har ansvaret for det politiske område, vil stå for gennemførelsen af direktivet.

Med hensyn til ENISA's forvaltning indeholder artikel 15 i forordningen om cybersikkerhed en detaljeret liste over ENISA's bestyrelses kontrolfunktioner.

I henhold til artikel 31 i forordningen om cybersikkerhed er ENISA's administrerende direktør ansvarlig for gennemførelsen af ENISA's budget, og Kommissionens interne revisor har samme beføjelser over for ENISA som over for Kommissionens tjenestegrene. ENISA's bestyrelse afgiver en udtalelse om ENISA's endelige årsregnskab.

2.2.2. Oplysninger om de konstaterede risici og det/de interne kontrolsystem(er), der etableres for at afbøde dem

Meget lav risiko, da NIS-direktivets økosystem allerede er på plads og allerede dækker ENISA, som har et permanent mandat efter ikrafttrædelsen af forordningen om cybersikkerhed i 2019.

2.2.3. Vurdering af og begrundelse for kontrolforanstaltningernes omkostningseffektivitet (forholdet mellem kontrolforanstaltningerne og værdien af de forvaltede midler) samt vurdering af den forventede risiko for fejl (ved betaling og ved afslutning)

Den ønskede budgetforhøjelse finder anvendelse på budgetafsnit 1 og har til formål at finansiere lønninger. Det betyder, at risikoen for fejl på betalingsniveau er meget lav.

2.3. Foranstaltninger til forebyggelse af svig og uregelmæssigheder

Angiv eksisterende eller påtænkte forebyggelses- og beskyttelsesforanstaltninger, f.eks. fra strategien til bekæmpelse af svig.

ENISA's forebyggelses- og beskyttelsesforanstaltninger finder anvendelse, herunder:

— Udbetalinger til tjenester eller bestilte undersøgelser forhåndskontrolleres af Agenturets tjenestegrene under hensyntagen til eventuelle kontraktlige forpligtelser, økonomiske principper og god finansiel og forvaltningsmæssig praksis. Alle aftaler og kontrakter mellem Agenturet og modtagere af udbetalinger vil indeholde bestemmelser om forholdsregler mod svig (tilsyn, rapporteringskrav m.v.).

— Bestemmelserne i Europa-Parlamentets og Rådets forordning (EU, Euratom) nr. 883/2013 af 25. maj 1999 om undersøgelser, der foretages af Det Europæiske Kontor for Bekæmpelse af Svig (OLAF), finder ubegrænset anvendelse i forbindelse med bekæmpelsen af svig, korruption og andre retsstridige handlinger.

— I henhold til artikel 33 i den generelle kontrolaftale tiltrådte ENISA den 28. december 2019 den interinstitutionelle aftale af 25. maj 1999 mellem Europa-Parlamentet, Rådet for Den Europæiske Union og Kommissionen for De Europæiske Fællesskaber om de interne undersøgelser, der foretages af Det Europæiske Kontor for Bekæmpelse af Svig (OLAF). ENISA udsteder straks passende bestemmelser, der finder anvendelse på alle agenturets ansatte.

3. FORSLAGETS/INITIATIVETS ANSLÅEDE FINANSIELLE VIRKNINGER

3.1. Berørt(e) udgiftspost(er) på budgettet og udgiftsområde(r) i den flerårige finansielle ramme

- Eksisterende udgiftsposter på budgettet

I samme rækkefølge som udgiftsområderne i den flerårige finansielle ramme og budgetposterne.

Udgiftsområde i den flerårige finansielle ramme	Budgetpost	Udgiftens art	Bidrag			
	Nummer	OB/IOB[58]	fra EFTA-lande[59]	fra kandidatlande[60]	fra tredjelande	iht. finansforordningens artikel 21, stk. 2, litra b)
2	02 10 04	/IOB	JA	NEJ	NEJ	/NEJ

- Nye budgetposter, som der er søgt om.

I samme rækkefølge som udgiftsområderne i den flerårige finansielle ramme og budgetposterne.

[58] OB = opdelte bevillinger/IOB = ikke-opdelte bevillinger.
[59] EFTA: Den Europæiske Frihandelssammenslutning.
[60] Kandidatlande og, efter omstændighederne, potentielle kandidatlande på Vestbalkan.

Udgiftsområde i den flerårige finansielle ramme	Budgetpost	Udgiftens art	Bidrag			
	Nummer	OB/IOB	fra EFTA-lande	fra kandidatlande	fra tredjelande	iht. finansforordningens artikel 21, stk. 2, litra b)
	[XX.YY.YY.YY]		JA/NEJ	JA/NEJ	JA/NEJ	JA/NEJ

3.2. Anslåede virkninger for udgifterne

3.2.1. Sammenfatning af de anslåede virkninger for udgifterne

i mio. EUR (tre decimaler)

Udgiftsområde i den flerårige finansielle ramme	Nummer	[Udgiftsområde....2 Det indre marked, innovation og det digitale område……..……]

[Organ]: <…ENISA….>			År **N**[61] **2022**	År **n+1** **2023**	År **n+2** **2024**	År **n+3** **2025**	Der indsættes flere år, hvis virkningerne varer længere (jf. punkt 1.6) **2026**	**2027**		**I ALT**
Afsnit 1:	Forpligtelser	(1)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Betalinger	(2)	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
Afsnit 2:	Forpligtelser	(1a)								
	Betalinger	(2a)								
Afsnit 3:	Forpligtelser	(3a)								
	Betalinger	(3b)								
Bevillinger I ALT for [organ] <ENISA…….>	Forpligtelser	=1+1a +3a	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Betalinger	=2+2a +3b	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

[61] År n er det år, hvor gennemførelsen af forslaget/initiativet begynder. I stedet for "n" indsættes det forventede første gennemførelsesår (f.eks.: 2021). Dette gælder også for de følgende år.

Udgiftsområde i den flerårige finansielle ramme	**5**	"Administrationsudgifter"

i mio. EUR (tre decimaler)

		År **n**	År **n+1**	År **n+2**	År **n+3**	Der indsættes flere år, hvis virkningerne varer længere (jf. punkt 1.6)			**I ALT**
GD: <…….>									
• Menneskelige ressourcer									
• Andre administrationsudgifter									
I ALT GD <…….>	Bevillinger								

Bevillinger I ALT under UDGIFTSOMRÅDE 5 i den flerårige finansielle ramme	(Forpligtelser i alt = Betalinger i alt)								

i mio. EUR (tre decimaler)

		År **N**[62] **2022**	År **n+1** **2023**	År **n+2** **2024**	År **n+3** **2025**	Der indsættes flere år, hvis virkningerne varer længere (jf. punkt 1.6) **2026**	**2027**		**I ALT**
Bevillinger I ALT under UDGIFTSOMRÅDE 1-5 i den flerårige finansielle ramme	Forpligtelser	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**
	Betalinger	0,61	0,61	0,61	0,61	0,61	0,61		**3,66**

[62] År n er det år, hvor gennemførelsen af forslaget/initiativet begynder. I stedet for "n" indsættes det forventede første gennemførelsesår (f.eks.: 2021). Dette gælder også for de følgende år.

3.2.2. Anslåede virkninger for [organets] bevillinger

– ☐x Forslaget/initiativet medfører ikke anvendelse af aktionsbevillinger

– ☐ Forslaget/initiativet medfører anvendelse af aktionsbevillinger som anført herunder:

Forpligtelsesbevillinger i mio. EUR (tre decimaler)

Der angives mål og resultater ⇩			År **n**		År **n+1**		År **n+2**		År **n+3**		Der indsættes flere år, hvis virkningerne varer længere (jf. punkt 1.6)						**I ALT**	
	RESULTATER																	
	Type[63]	Resultaternes gnsntl. omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal	Omkostninger	Antal resultater i alt	Omkostninger i alt
SPECIFIKT MÅL NR. 1[64]...																		
— Resultat																		
— Resultat																		
— Resultat																		
Subtotal for specifikt mål nr. 1																		
SPECIFIKT MÅL NR. 2																		
— Resultat																		
Subtotal for specifikt mål nr. 2																		
OMKOSTNINGER I ALT																		

63 Resultater er de produkter og tjenesteydelser, der skal leveres (f.eks. antal finansierede studenterudvekslinger, antal km bygget vej osv.).

64 Som beskrevet i punkt 1.4.2. "Specifikke mål ...".

3.2.3. Anslåede virkninger for ENISA's menneskelige ressourcer

3.2.3.1. Resumé

Som følge af det reviderede NIS-direktiv vil ENISA fra og med 2022/23 få yderligere opgaver. Selv om disse opgaver vil være omfattet af ENISA's mandat, vil de medføre en yderligere arbejdsbyrde for agenturet. Nærmere bestemt vil ENISA ud over sine nuværende opgaver i henhold til Kommissionens forslag til et revideret NIS-direktiv bl.a. få til opgave i) at udvikle og vedligeholde et europæisk sårbarhedsregister (artikel 6, stk. 2), ii) at varetage sekretariatsfunktionen for det europæiske netværk af forbindelsesorganisationer for cyberkriser (EU-CyCLONe) (artikel 14) og udarbejde en årlig rapport om cybersikkerhedssituationen i EU (artikel 15), iii) at støtte tilrettelæggelsen af peerevalueringer mellem medlemsstaterne (artikel 16), iv) at indsamle aggregerede hændelsesdata fra medlemsstaterne og udarbejde teknisk vejledning (artikel 20, stk. 9), v) at etablere og vedligeholde et register over enheder, der leverer grænseoverskridende tjenester (artikel 25).

Derfor vil der blive anmodet om 5 ekstra årsværk fra 2022 med et tilsvarende budget til dækning af disse nye stillinger.

– ☐ Forslaget/initiativet medfører ikke anvendelse af administrationsbevillinger

– ☐X Forslaget/initiativet medfører anvendelse af administrationsbevillinger som anført herunder:

i mio. EUR (tre decimaler)

	År **n**[65] **2022**	År **n+1** **2023**	År **n+2** **2024**	År **n+3** **2025**	Der indsættes flere år, hvis virkningerne varer længere (jf. punkt 1.6) **2026** **2027**			**I ALT**
Midlertidigt ansatte (AD)	0,450	0,450	0,450	0,450	0,450	0,450		**2,7**
Midlertidigt ansatte (AST)								
Kontraktansatte	0,160	0,160	0,160	0,160	0,160	0,160		**0,96**
Udstationerede nationale eksperter								
I ALT	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**	**0,61**		**3,66**

[65] År n er det år, hvor gennemførelsen af forslaget/initiativet begynder. I stedet for "n" indsættes det forventede første gennemførelsesår (f.eks.: 2021). Dette gælder også for de følgende år.

Personalebehov (i årsværk):

	År **n**[66] **2022**	År **n+1** **2023**	År **n+2** **2024**	År **n+3** **2025**	Der indsættes flere år, hvis virkningerne varer længere (jf. punkt 1.6) **2026** **2027**			**I ALT**
Midlertidigt ansatte (AD)	3	3	3	3	3	3		**18**
Midlertidigt ansatte (AST)								
Kontraktansatte	2	2	2	2	2	2		**12**
Udstationerede nationale eksperter								
I ALT	**5**	**5**	**5**	**5**	**5**	**5**		**30**

3.2.3.2. Anslået behov for menneskelige ressourcer i det overordnede generaldirektorat

– ☐ Forslaget/initiativet medfører ikke anvendelse af menneskelige ressourcer

– ☐ Forslaget/initiativet medfører anvendelse af menneskelige ressourcer som anført herunder:

Overslag angives i hele tal (eller med højst én decimal)

	År **n**	År **n+1**	År **n+2**	År **n+3**	Der indsættes flere år, hvis virkningerne varer længere (jf. punkt 1.6)		
• **Stillinger i stillingsfortegnelsen (tjenestemænd og midlertidigt ansatte)**							
XX 01 01 01 (i hovedsædet og i Kommissionens repræsentationskontorer)							
XX 01 01 02 (i delegationer)							
XX 01 05 01 (indirekte forskning)							
10 01 05 01 (direkte forskning)							
• **Eksternt personale (i årsværk) årsværk**[67]							

66 År n er det år, hvor gennemførelsen af forslaget/initiativet begynder. I stedet for "n" indsættes det forventede første gennemførelsesår (f.eks.: 2021). Dette gælder også for de følgende år.

XX 01 02 01 (KA, UNE, V under den samlede bevillingsramme)								
XX 01 02 02 (KA, LA, UNE, V og JED i delegationerne)								
XX 01 04 ***yy***[68]	— i hovedsædet[69]							
	— i delegationer							
XX 01 05 02 (KA, UNE, V — Indirekte forskning)								
10 01 05 02 (KA, UNE, V — Direkte forskning)								
Andre budgetposter (skal angives)								
I ALT								

XX angiver det berørte politikområde eller budgetafsnit.

Personalebehovet vil blive dækket ved hjælp af det personale, som generaldirektoratet allerede har afsat til aktionen, og/eller interne rokader i generaldirektoratet, eventuelt suppleret med yderligere bevillinger, som tildeles det ansvarlige generaldirektorat i forbindelse med den årlige tildelingsprocedure under hensyntagen til de budgetmæssige begrænsninger.

Opgavebeskrivelse:

Tjenestemænd og midlertidigt ansatte	
Eksternt personale	

Beskrivelsen af, hvordan udgifterne til fuldtidsækvivalenterne er beregnet, bør medtages i afsnit 3 i bilag V.

67 KA = kontraktansatte, LA: lokalt ansatte, UNE: udstationerede nationale eksperter, V: vikarer, JED = junioreksperter ved delegationerne.

68 Delloft for eksternt personale under aktionsbevillingerne (tidligere BA-poster).

69 Angår især strukturfondene, Den Europæiske Landbrugsfond for Udvikling af Landdistrikterne (ELFUL) og Den Europæiske Fiskerifond (EFF).

3.2.4. Forenelighed med indeværende flerårige finansielle ramme

– ☐X Forslaget/initiativet er foreneligt med indeværende flerårige finansielle ramme

– ☐ Forslaget/initiativet kræver omlægning af det relevante udgiftsområde i den flerårige finansielle ramme

Der redegøres for omlægningen med angivelse af de berørte budgetposter og beløbenes størrelse Forslaget/initiativet er foreneligt med den flerårige finansielle ramme 21-27. Udligningen af det budget, der anmodes om til dækning af forøgelsen af personaleressourcerne i ENISA, vil ske ved at reducere budgettet for programmet for et digitalt Europa med samme beløb under samme udgiftsområde.

– ☐ Forslaget/initiativet kræver, at fleksibilitetsinstrumentet anvendes, eller at den flerårige finansielle ramme revideres[70].

Der redegøres for behovet med angivelse af de berørte udgiftsområder og budgetposter og beløbenes størrelse

3.2.5. Tredjemands bidrag til finansieringen

– Forslaget/initiativet indeholder ikke bestemmelser om samfinansiering med tredjemand.

– Forslaget/initiativet indeholder bestemmelser om samfinansiering, jf. følgende overslag:

i mio. EUR (tre decimaler)

	År **n**	År **n+1**	År **n+2**	År **n+3**	Der indsættes flere år, hvis virkningerne varer længere (jf. punkt 1.6)			I alt
Angiv organ, som deltager i samfinansieringen								
Samfinansierede bevillinger I ALT								

[70] Jf. artikel 11 og 17 i Rådets forordning (EU, Euratom) nr. 1311/2013 om fastlæggelse af den flerårige finansielle ramme for årene 2014-2020.

3.3. Anslåede virkninger for indtægterne

– ☐ Forslaget/initiativet har ingen finansielle virkninger for indtægterne

– ☐ Forslaget/initiativet har følgende finansielle virkninger:

☐ for egne indtægter

☐ for andre indtægter

☐ angiv, om indtægterne er formålsbestemte

i mio. EUR (tre decimaler)

Indtægtspost på budgettet	Bevillinger til rådighed i indeværende regnskabsår	Forslagets/initiativets virkninger[71]						
		År **n**	År **n+1**	År **n+2**	År **n+3**	Der indsættes flere år, hvis virkningerne varer længere (jf. punkt 1.6)		
Artikel …….								

For diverse indtægter, der er formålsbestemte, angives det, hvilke af budgettets udgiftsposter der påvirkes.

Det oplyses, hvilken metode der er benyttet til at beregne virkningerne for indtægterne.

[71] Med hensyn til EU's traditionelle egne indtægter (told og sukkerafgifter) opgives beløbene netto, dvs. bruttobeløb, hvorfra der er trukket opkrævningsomkostninger på 20 %.