



EUROPEISKA
KOMMISSIONEN

Bryssel den 16.12.2020
COM(2020) 823 final

2020/0359 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV

**om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om
upphävande av direktiv (EU) 2016/1148**

(Text av betydelse för EES)

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

MOTIVERING

1. BAKGRUND TILL FÖRSLAGET

• Motiv och syfte med förslaget

Detta förslag ingår i ett åtgärds paket som ytterligare ska förbättra motståndskraften och incidenthanteringskapaciteten hos offentliga och privata entiteter, behöriga myndigheter och unionen som helhet på området cybersäkerhet och skydd av kritisk infrastruktur. Det ligger i linje med kommissionens prioriteringar att rusta Europa för den digitala tidsåldern och att bygga upp en framtidssäkrad ekonomi för människor. Cybersäkerhet är en prioritering i kommissionens hantering av covid-19-krisen. Paketet innehåller en ny strategi för cybersäkerhet som ska stärka unionens strategiska oberoende med målet att förbättra dess motståndskraft och gemensamma reaktionsförmåga och bygga upp ett öppet och globalt internet. Slutligen innehåller paketet ett förslag till direktiv om motståndskraften hos kritiska leverantörer av samhällsviktiga tjänster som syftar till att minska de fysiska hoten mot dessa leverantörer.

Detta förslag bygger på och upphäver direktiv (EU) 2016/1148 om säkerhet i nätverks- och informationssystem (*NIS-direktivet*), som är den första rättsakten i en EU-omfattande lagstiftning om cybersäkerhet som tillhandahåller rättsliga åtgärder för att höja den övergripande cybersäkerhetsnivån i unionen. NIS-direktivet har bidragit till att 1) förbättra cybersäkerhetskapaciteten på nationell nivå genom att kräva att medlemsstaterna antar nationella strategier för cybersäkerhet och utser behöriga nationella myndigheter för cybersäkerhet, 2) öka samarbetet mellan medlemsstaterna på unionsnivå genom att inrätta en rad forum för att underlätta utbytet av strategisk och operativ information, och 3) förbättra cyberresiliensen hos offentliga och privata entiteter inom sju specifika sektorer (energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt digital infrastruktur) och inom tre digitala tjänster (internetbaserade marknadsplatser, internetbaserade sökmotorer och molntjänster) genom att kräva att medlemsstaterna säkerställer att leverantörer av samhällsviktiga och digitala tjänster inför cybersäkerhetskrav och rapporterar incidenter.

Förslaget moderniserar den befintliga rättsliga ramen med beaktande av de senaste årens ökade digitalisering av den inre marknaden och den snabbt föränderliga hotbilden mot cybersäkerheten. Båda dessa utvecklingstendenser har förstärkts ytterligare till följd av covid-19-krisen. Förslaget åtgärdar också flera brister som hindrade NIS-direktivet från att utnyttjas till sin fulla potential.

Trots de betydande framstegen har NIS-direktivet, som banade väg för en betydande attitydförändring vad gäller den institutionella och lagstiftningsmässiga strategin för cybersäkerhet i många medlemsstater, också visat sina begränsningar. Den digitala omvandlingen av samhället (som trappats upp på grund av covid-19-krisen) har expanderat hotbilden och medför nya utmaningar som kräver anpassade och innovativa svarsåtgärder. Antalet cyberattacker fortsätter att öka, och de alltmer sofistikerade attackerna kommer från ett brett spektrum av källor i och utanför EU.

Vid utvärderingen av NIS-direktivets funktion som genomfördes med avseende på konsekvensbedömningen identifierades följande problem: 1) Den låga nivån av cyberresiliens hos företag som är verksamma i EU. 2) Skillnaderna i resiliens mellan medlemsstater och olika sektorer. 3) Den låga graden av gemensam situationsmedvetenhet och avsaknaden av gemensam krishantering. Som exempel kan nämnas att vissa större sjukhus i en medlemsstat inte omfattas av NIS-direktivets tillämpningsområde och därför inte är skyldiga att genomföra

direktivets säkerhetsåtgärder, medan det i en annan medlemsstat är så att nästan varenda vårdgivare i landet omfattas av NIS-direktivets säkerhetskrav.

Förslaget är ett initiativ inom programmet om lagstiftningens ändamålsenlighet och resultat (*Refit-programmet*) och det syftar till att minska regelbördan för behöriga myndigheter och fullgörandekostnaderna för offentliga och privata entiteter. Detta uppnås framför allt genom att avskaffa de behöriga myndigheternas skyldighet att identifiera leverantörer av samhällsviktiga tjänster samt öka harmoniseringen av säkerhets- och rapporteringskraven för att underlätta efterlevnaden av regelverket för entiteter som tillhandahåller gränsöverskridande tjänster. Samtidigt kommer de behöriga myndigheterna att få en rad nya uppgifter, däribland tillsynen av entiteter i sektorer som hittills inte omfattats av NIS-direktivet.

- **Förenlighet med befintliga bestämmelser inom området**

Detta förslag ingår i en bredare uppsättning befintliga rättsliga instrument och kommande initiativ på unionsnivå som syftar till att öka offentliga och privata entiteters motståndskraft mot hot.

På cybersäkerhetsområdet är dessa bland annat direktiv (EU) 2018/1772 om inrättande av en europeisk kodex för elektronisk kommunikation (vars cybersäkerhetsrelaterade bestämmelser kommer att ersättas av bestämmelserna i det föreliggande förslaget) och förslaget till en förordning om digital operativ motståndskraft för finanssektorn (COM(2020) 595 final), som kommer att betraktas som *lex specialis* i förhållande till det föreliggande förslaget när båda väl har trätt i kraft.

Förslaget kompletterar, på området fysisk säkerhet, förslaget till ett direktiv om kritiska entiteters motståndskraft, som är en revidering av direktiv 2008/144/EG om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna (ECI-direktivet), som inrättar ett unionsförfarande för att identifiera och utse europeisk kritisk infrastruktur, och fastställer ett angreppssätt för att förbättra skyddet av denna. I juli 2020 antog kommissionen EU:s strategi för en säkerhetsunion¹, vilken erkände en ökande sammanlänkning och ett ökande ömsesidigt beroende mellan fysisk och digital infrastruktur. Den underströk behovet av en mer sammanhållen och konsekvent strategi mellan ECI-direktivet och direktiv (EU) 2016/1148 när det gäller åtgärder för en hög gemensam nivå på säkerheten i nätverks- och informationssystem i hela unionen.

Förslaget är därför nära anpassat till förslaget till ett direktiv om kritiska entiteters motståndskraft, vilket syftar till att öka kritiska entiteters motståndskraft mot fysiska hot i ett stort antal sektorer. Förslaget syftar till att säkerställa att behöriga myndigheter vidtar komplementära åtgärder enligt bägge direktiven och vid behov utbyter information rörande cyber- och icke-cyberresiliens, samt att i synnerhet kritiska aktörer inom de sektorer som anses vara *väsentliga* enligt det föreliggande förslaget också omfattas av en mer allmän resilienshöjande skyldighet med tonvikt på andra risker än cyberrisker.

¹ COM(2020) 605 final.

- **Förenlighet med unionens politik inom andra områden**

Såsom anges i meddelandet *Att forma EU:s digitala framtid*² är det av avgörande betydelse för Europa att ta till vara alla möjligheter som den digitala tidsåldern erbjuder för att inom säkra och etiska gränser stärka sin industri och innovationsförmåga. I EU-strategin för data fastställs fyra pelare – dataskydd, grundläggande rättigheter, säkerhet och cybersäkerhet – var och en av dem en nödvändig förutsättning för att ett samhälle ska kunna stärkas genom användning av data.

I en resolution från den 12 mars 2019 uppmanade Europaparlamentet kommissionen ”att bedöma behovet av att ytterligare utvidga räckvidden för direktivet om nät- och informationssäkerhet till andra kritiska sektorer och tjänster som inte täcks av sektorsspecifik lagstiftning”³. I sina slutsatser från den 9 juni 2020 välkomnade rådet ”[...] kommissionens planer på att säkerställa konsekventa regler för marknadsoperatörer och underlätta ett säkert, stabilt och ändamålsenligt informationsutbyte om hot och incidenter, bland annat genom en översyn av nätverks- och informationssäkerhetsdirektivet (NIS-direktivet), för att eftersträva alternativ för förbättrad cyberresiliens och effektivare svar på cyberattacker, särskilt i fråga om väsentlig ekonomisk och samhällelig verksamhet, samtidigt som medlemsstaternas befogenheter respekteras, inbegripet ansvaret för deras nationella säkerhet”⁴. Vidare påverkar den föreslagna rättsakten inte tillämpningen av de konkurrensregler som föreskrivs i fördraget om Europeiska unionens funktionssätt (EUF-fördraget).

Eftersom en betydande del av cybersäkerhetshoten har sitt ursprung utanför EU krävs en enhetlig strategi för internationellt samarbete. Detta direktiv ska utgöra en referensmodell som ska framhållas inom ramen för EU:s samarbete med tredjeländer, särskilt vid tillhandahållande av externt tekniskt bistånd.

2. RÄTTSLIG GRUND, SUBSIDIARITETSPRINCIPEN OCH PROPORTIONALITETSPRINCIPEN

- **Rättslig grund**

Den rättsliga grunden för NIS-direktivet är artikel 114 i fördraget om Europeiska unionens funktionssätt, vars mål är att upprätta den inre marknaden och säkerställa dess funktion genom att förbättra åtgärderna för tillnärmning av nationella regler. Såsom EU-domstolen slår fast i sin dom i mål C-58/08 Vodafone Ltd m.fl., är det motiverat att välja artikel 114 i EUF-fördraget som grund om skillnaderna mellan de nationella bestämmelserna har en direkt inverkan på den inre marknadens funktion. Domstolen slog också fast att om det redan antagits en akt med stöd av artikel 114 i EUF-fördraget som undanröjer samtliga handelshinder på det harmoniserade området, så får unionslagstiftaren inte fräntas möjligheten att anpassa denna rättsakt när förutsättningarna förändras eller ny kunskap uppkommer med avseende på unionslagstiftarens uppgift att skydda de allmänna intressen som erkänns i fördraget. Domstolen förklarade slutligen att avsikten med de åtgärder för tillnärmning som omfattas av artikel 114 i EUF-fördraget är att ge ett utrymme för skönsmässig bedömning – beroende på det övergripande sammanhanget och de särskilda förhållanden som ska harmoniseras – avseende den mest lämpliga tillnärmningstekniken för att uppnå önskat resultat. Den föreslagna rättsakten skulle undanröja hinder för och förbättra den inre

² COM(2020) 67 final.

³ https://www.europarl.europa.eu/doceo/document/TA-8-2019-0156_EN.html

⁴ <https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/en/pdf>

marknadens upprättande och funktion för väsentliga och viktiga entiteter genom att fastställa tydliga och allmänt tillämpliga regler om tillämpningsområdet för NIS-direktivet och harmonisera de tillämpliga reglerna för riskhantering och incidentrapportering på cybersäkerhetsområdet. De nuvarande skillnaderna på detta område, både på lagstiftnings- och tillsynsnivå, såväl som på nationell och EU-nivå, utgör hinder för den inre marknaden eftersom entiteter som bedriver gränsöverskridande verksamhet ställs inför olika, och eventuellt överlappande, regelmässiga krav och/eller olika krav på tillämpning av dessa, på bekostnad av deras utövande av etableringsfriheten och friheten att tillhandahålla tjänster. Skilda regler har också en negativ inverkan på konkurrensvillkoren på den inre marknaden när det gäller entiteter av samma typ i olika medlemsstater.

- **Subsidiaritetsprincipen (för icke-exklusiv befogenhet)**

Cybersäkerhetsresiliensen i unionen kan inte vara effektiv om den hanteras på olika sätt genom nationellt eller regionalt silotänkande. NIS-direktivet hanterade delvis denna brist genom att fastställa en ram för säkerhet i nätverks- och informationssystem på nationell nivå och på unionsnivå. Införlivandet och genomförandet av direktivet visade emellertid också på inneboende brister och begränsningar vad gäller vissa bestämmelser och strategier, såsom den oklara avgränsningen av direktivets tillämpningsområde som ledde till betydande skillnader i omfattning och djup i fråga om EU:s ingripande på medlemsstatsnivå. Sedan covid-19-krisen startade har den europeiska ekonomin dessutom blivit mer beroende av nätverks- och informationssystem än någonsin förr och olika sektorer och tjänster blir alltmer sammankopplade. Ett mer långtgående ingripande från EU:s sida än de nuvarande åtgärderna i NIS-direktivet motiveras främst av följande: i) De NIS-relaterade hoten och utmaningarna blir alltmer gränsöverskridande till sin art. ii) Unionens insatser har hög potential att förbättra och underlätta effektiva och samordnade nationella strategier. iii) Samordnade och samarbetsinriktade strategiska åtgärder bidrar starkt till ett effektivt integritetsskydd och skydd av personuppgifter.

- **Proportionalitetsprincipen**

De regler som föreslås i detta direktiv går inte utöver vad som är nödvändigt för att i tillräckligt hög grad uppnå de särskilda målen. Den planerade anpassningen och rationaliseringen av säkerhetsåtgärder och rapporteringsskyldigheter har samband med medlemsstaternas och företagens önskemål om en förbättring av den nuvarande ramen.

Förslaget tar hänsyn till redan befintlig praxis i medlemsstaterna. En högre skyddsnivå som uppnås genom sådana rationaliserade och samordnade krav står i proportion till de ökande riskerna, däribland de risker som har ett gränsöverskridande inslag. Kraven är rimliga och motsvarar i allmänhet de berörda entiteternas intresse av att säkerställa kontinuitet och kvalitet i sina tjänster. Kostnaderna för att säkerställa systematiskt samarbete mellan medlemsstaterna skulle vara små jämfört med de ekonomiska och samhällsliga förlusterna och skadorna till följd av cyberincidenter. Vidare visar de samråd med berörda parter som hölls i samband med översynen av NIS-direktivet, inbegripet resultaten av det öppna offentliga samrådet och de riktade undersökningarna, stöd för en översyn av NIS-direktivet enligt ovan angivna linjer.

- **Val av instrument**

Förslaget kommer att rationalisera företagens skyldigheter ytterligare och säkerställa en högre grad av harmonisering av dessa. Förslaget syftar samtidigt till att ge medlemsstaterna den flexibilitet som behövs för att ta hänsyn till nationella särdrag (som t.ex. möjligheten att

identifiera ytterligare väsentliga eller viktiga entiteter som ligger utanför det referensvärde som fastställs i rättsakten). Det framtida rättsliga instrumentet bör därför vara ett direktiv, eftersom ett sådant medger förbättrad harmonisering på ett riktat sätt samt en viss grad av flexibilitet för de behöriga myndigheterna.

3. RESULTAT AV EFTERHANDSUTVÄRDERINGAR, SAMRÅD MED BERÖRDA PARTER OCH KONSEKVENSBEDÖMNINGAR

• Efterhandsutvärderingar/kontroller av ändamålsenligheten med befintlig lagstiftning

Kommissionen har gjort en utvärdering av NIS-direktivets funktion⁵. Den har analyserat direktivets relevans, EU-mervärde, samstämmighet, ändamålsenlighet och effektivitet. De viktigaste resultaten av analysen är följande:

- NIS-direktivets tillämpningsområde är för snävt vad gäller de sektorer som omfattas, främst på grund av följande: i) De senaste årens ökade digitalisering och en högre grad av interkonnektivitet, ii) NIS-direktivets tillämpningsområde omfattar inte längre alla digitaliserade sektorer som tillhandahåller centrala tjänster till ekonomin och samhället som en helhet.
- NIS-direktivet är inte tillräckligt tydligt när det gäller tillämpningsområdet för leverantörer av samhällsviktiga tjänster och dess bestämmelser ger inte tillräckligt klarhet om nationell behörighet med avseende på leverantörer av digitala tjänster. Detta har lett till en situation där vissa typer av entiteter inte har identifierats i alla medlemsstater och därför inte är skyldiga att införa säkerhetsåtgärder och rapportera incidenter.
- NIS-direktivet gav medlemsstaterna stort utrymme för skönsmässig bedömning vid fastställandet av säkerhets- och rapporteringskrav för leverantörer av samhällsviktiga tjänster. Utvärderingen visar att medlemsstaterna i vissa fall har genomfört dessa krav på väsentligt olika sätt, vilket har skapat en ytterligare börda för företag som är verksamma i fler än en medlemsstat.
- NIS-direktivets system för tillsyn och kontroll av efterlevnaden är ineffektivt. Medlemsstaterna har till exempel varit mycket tveksamma till att tillämpa sanktioner mot entiteter som inte har infört säkerhetskrav eller rapporterat incidenter. Detta kan få negativa konsekvenser för enskilda entiteters cyberresiliens.
- De ekonomiska och mänskliga resurser som medlemsstaterna avsätter för att utföra sina uppgifter (t.ex. identifiering eller tillsyn av leverantörer av samhällsviktiga tjänster) varierar kraftigt, och därmed även den mognadsnivå som uppnåtts när det gäller att hantera cybersäkerhetsrisker. Detta förstärker ytterligare skillnaderna i cyberresiliens mellan medlemsstaterna.
- Medlemsstaterna delar inte systematiskt information med varandra, vilket särskilt får negativa konsekvenser för cybersäkerhetsåtgärdernas ändamålsenlighet och för graden av gemensam situationsmedvetenhet på EU-nivå. Detta gäller även för informationsutbytet mellan privata entiteter, och för samarbetet mellan samarbetsstrukturer på EU-nivå och privata entiteter.

⁵

[Bilaga 5 till konsekvensbedömningen]

- **Samråd med berörda parter**

Kommissionen har samrått med ett brett spektrum av berörda parter. Medlemsstater och berörda parter uppmanades att delta i det öppna offentliga samrådet och de enkäter och workshoppar som organiserats av Wavestone, Ceps och ICF åt vilka kommissionen uppdrog att genomföra en undersökning till stöd för översynen av NIS-direktivet. Bland de konsulterade parterna ingick behöriga myndigheter, unionsorgan som arbetar med cybersäkerhet, leverantörer av samhällsviktiga tjänster, leverantörer av digitala tjänster, entiteter som tillhandahåller tjänster utanför tillämpningsområdet för det nu gällande NIS-direktivet, branschorganisationer, konsumentorganisationer och medborgare.

Kommissionen har dessutom haft ständig kontakt med de behöriga myndigheter som ansvarar för genomförandet av NIS-direktivet. Samarbetsgruppen har i omfattande utsträckning täckt olika övergripande och sektoriella aspekter av genomförandet. Under sina NIS-besök i medlemsländerna 2019 och 2020, slutligen, intervjuade kommissionen 154 offentliga och privata entiteter, samt 117 behöriga myndigheter.

- **Insamling och användning av sakkunnigutlåtanden**

Kommissionen har anlitat ett konsortium omfattande Wavestone, Ceps och ICF för att bistå den i översynen av NIS-direktivet⁶. Uppdragstagaren har inte bara vänt sig till de aktörer som är direkt berörda av NIS-direktivet med målinriktade enkäter och workshoppar, utan har också samrått med ett brett spektrum av experter på cybersäkerhetsområdet, som till exempel cybersäkerhetsforskare och yrkesverksamma inom cybersäkerhetsindustrin.

- **Konsekvensbedömning**

Detta förslag åtföljs av en konsekvensbedömning⁷ som överlämnades till nämnden för lagstiftningskontroll den 23 oktober 2020 och fick ett positivt utlåtande med kommentarer från nämnden den 20 november 2020. Nämnden rekommenderade förbättringar på vissa områden i syfte att 1) bättre återspegla den roll som gränsöverskridande spridningseffekter spelar i problemanalysen, 2) bättre förklara hur framgång med initiativet skulle se ut, 3) ytterligare motivera förteckningen över policyalternativ, 4) redogöra närmare för kostnaderna för de föreslagna åtgärderna. Konsekvensbedömningen justerades i syfte att behandla dessa aspekter tillsammans med mer detaljerade kommentarer från nämnden. Den innehåller nu mer detaljerade förklaringar av de gränsöverskridande spridningseffekternas inflytande på cybersäkerhetsområdet, en tydligare översikt av hur framgång kan mätas, en mer detaljerad förklaring av utformningen och logiken bakom de olika policyalternativen och de åtgärder som övervägs inom dessa alternativ, en mer detaljerad förklaring av de aspekter som analyserats med avseende NIS-direktivets sektoriella tillämpningsområde och ytterligare förtydliganden vad gäller kostnaderna.

Kommissionen beaktade en rad policyalternativ i syfte att förbättra den rättsliga ramen på området cyberresiliens och hanteringen av cyberincidenter:

⁶ Undersökning till stöd för översynen av direktiv (EU) 2016/1148 när det gäller åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen – nr 2020-665. Wavestone, CEPS och ICF.

⁷ [Länkar till det slutliga dokumentet och till sammanfattningsbladet kommer att läggas till.]

- ”Ingen åtgärd”: NIS-direktivet skulle förbli oförändrat och inga andra åtgärder av icke-rättslig natur skulle vidtas för att hantera de problem som identifierats vid utvärderingen av NIS-direktivet.
- Alternativ 1: Inga ändringar skulle göras på lagstiftningsnivå. I stället skulle kommissionen utfärda rekommendationer och riktlinjer (till exempel om identifiering av leverantörer av samhällsviktiga tjänster, säkerhetskrav, förfarande för incidentrapportering och tillsyn) efter samråd med samarbetsgruppen, EU:s cybersäkerhetsbyrå (Enisa) och, i tillämpliga fall, nätverket av nationella enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter).
- Alternativ 2: Detta alternativ medför riktade ändringar av NIS-direktivet, inbegripet en utvidgning av tillämpningsområdet och flera andra ändringar som skulle syfta till att säkerställa vissa omedelbara lösningar på de problem som identifierats, och därigenom skapa större klarhet och ytterligare harmonisering (till exempel bestämmelser för att harmonisera tröskelvärden i samband med identifiering). Det ändrade NIS-direktivet skulle dock behålla sina viktigaste byggstenar, sin strategi och sitt grundsyfte.
- Alternativ 3: Detta scenario medför systemförändringar och strukturella förändringar av NIS-direktivet (genom ett nytt direktiv) med ett mer grundläggande strategiskifte mot att täcka ett bredare segment av unionens ekonomier, dock med en mer fokuserad tillsyn inriktad på stora och centrala aktörer. Det skulle också innebära en rationalisering av de skyldigheter som åläggs företag och säkerställa en högre nivå av harmonisering av dessa, skapa en effektivare ram för operativa aspekter samt skapa en tydlig grund för ett ökat delat ansvar och ansvarsutkrävande med avseende på olika aktörer i fråga om cybersäkerhetsåtgärder.

Enligt konsekvensbedömningen är alternativ 3 det rekommenderade alternativet (dvs. systemförändringar och strukturella förändringar av NIS-ramen). Vad gäller ändamålsenligheten skulle det rekommenderade alternativet tydligt fastställa NIS-direktivets tillämpningsområde, utvidgat till en mer representativ andel av EU:s ekonomier och samhällen, och anpassningen av kraven till varandra, vid sidan av en bättre definierad ram för tillsyn och efterlevnadskontroll som skulle syfta till att öka fullgörandenivån. Det omfattar också åtgärder i syfte att förbättra de politiska strategierna på medlemsstatsnivå och ett paradigmskifte på detta område, åtgärder för att främja nya ramar för riskhantering i leverantörsrelationer och för samordnad information om sårbarheter. Samtidigt inför det rekommenderade alternativet en tydlig grund för delat ansvar och ansvarsutkrävande och omfattar mekanismer som syftar till att främja ett ökat förtroende mellan medlemsstater, både bland myndigheter och inom branschen, genom att uppmuntra till informationsutbyte och säkerställa en mer operativ strategi, som till exempel mekanismerna för ömsesidigt bistånd och sakkunnigbedömningar. Detta alternativ skulle också tillhandhålla en EU-ram för krishantering som bygger på nyligen inrättade operativa nätverk i EU, och skulle säkerställa en större roll för Enisa, inom ramen för dess nuvarande mandat, när det gäller att hålla en korrekt överblick över cybersäkerhetssituationen i unionen.

Vad gäller effektiviteten skulle det rekommenderade alternativet, samtidigt som det medför extra kostnader med avseende på fullgörande och efterlevnadskontroll både för företag och medlemsstater, även leda till effektiva kompromisser och synergier, med den bästa potentialen av alla analyserade politiska alternativ för att säkerställa en ökad och konsekvent nivå av cyberresiliens hos centrala entiteter i hela unionen som så småningom skulle leda till kostnadsbesparingar för både företag och samhället. Detta policyalternativ skulle leda till vissa ytterligare administrativa bördor och fullgörandekostnader för medlemsstaternas

myndigheter. Detta vägs dock upp av att alternativet på medellång och lång sikt även skulle medföra betydande fördelar genom ökat samarbete mellan medlemsstater, även på operativ nivå, samt genom ömsesidigt bistånd, mekanismer för sakkunnigbedömning och en bättre överblick över och samverkan med centrala företag, och skulle stimulera en allmän ökning av cybersäkerhetskapaciteten på nationell och regional nivå. Det rekommenderade alternativet skulle även i stor utsträckning säkerställa överensstämmelse med annan lagstiftning, andra initiativ eller andra policyåtgärder, inklusive sektorspecifik lex specialis.

Ett åtgärdande av återstående bristande cybersäkerhetsberedskap på medlemsstatsnivå och på företagsnivå och inom andra organisationer skulle kunna leda till effektivitetsvinster och en minskning av extra kostnader till följd av cyberincidenter.

- För väsentliga och viktiga entiteter kan en höjd cybersäkerhetsberedskap leda till att minska potentiella inkomstförluster till följd av störningar – däribland industrispionage – och kan minska de höga kostnaderna för tillfälliga hotbegränsande lösningar. Sådana vinster kommer sannolikt att uppväga de nödvändiga investeringskostnaderna. En minskad fragmentering av den inre marknaden skulle också bidra till mer likvärdiga konkurrensvillkor för aktörerna.
- För medlemsstaterna skulle det kunna ytterligare minska risken för ökande budgetutgifter för tillfälliga hotbegränsande lösningar och extra kostnader i nödsituationer som uppstår i samband med cyberincidenter.
- För medborgarna förväntas hanteringen av cyberincidenter leda till att inkomstförlusterna på grund av ekonomiska störningar minskar.

Höjda cybersäkerhetsnivåer i medlemsstaterna och möjligheter för företag och myndigheter att reagera snabbt på en incident och begränsa dess effekter kommer högst sannolikt att leda till en ökning av medborgarnas allmänna förtroende för den digitala ekonomin, vilket kan få en positiv inverkan på tillväxt och investeringar.

En höjning av den övergripande cybersäkerhetsnivån kommer sannolikt att leda till en ökad allmän säkerhet och smidig oavbruten drift av samhällsviktiga tjänster, som är av kritisk betydelse för samhället. Initiativet kan också bidra till annan samhällspåverkan som minskad cyberbrottslighet och terrorism och ökat civilskydd. En höjd nivå av cyberberedskap för företag och andra organisationer kan leda till att man undviker potentiella ekonomiska förluster till följd av cyberattacker och därmed förhindrar att det uppstår ett behov av att avskeda anställda.

En höjning av den övergripande cybersäkerhetsnivån kan också leda till att miljörisker/miljöskador undviks i händelse av ett angrepp på en samhällsviktig tjänst. Detta kan vara särskilt relevant för energisektorn och för vattenförsörjnings- och vattendistributionssektorn eller transportsektorn. Genom att stärka cybersäkerhetskapaciteten kan initiativet leda till ökad användning av den senaste generationens IKT-infrastruktur och IKT-tjänster, vilka också är mer hållbara i miljöhänseende, och till att ineffektiv och mindre säker befintlig infrastruktur ersätts. Detta väntas även bidra till att minska antalet kostsamma cyberincidenter och frigöra resurser för hållbara investeringar.

• **Lagstiftningens ändamålsenlighet och förenkling**

I förslaget föreskrivs ett allmänt undantag för mikroentiteter och små entiteter från direktivets tillämpningsområde och ett enklare system för efterhandstillsyn som tillämpas på ett stort antal av de nya entiteter som omfattas av det reviderade tillämpningsområdet (så kallade *viktiga entiteter*). Dessa åtgärder har till syfte att minimera och skapa jämvikt i fråga om den

börda som läggs på företag och offentliga förvaltningar. Vidare ersätter förslaget det komplexa systemet för identifiering av leverantörer av samhällsviktiga tjänster med en allmänt tillämplig skyldighet och inför en högre nivå av harmonisering av säkerhets- och rapporteringsskyldigheter, vilket bör minska fullgörandebördan, särskilt för entiteter som tillhandahåller gränsöverskridande tjänster.

Förslaget minimerar fullgörandekostnaderna för små och medelstora företag, eftersom entiteter endast är skyldiga att vidta de åtgärder som krävs för att säkerställa en säkerhetsnivå i nätverks- och informationssystem som är adekvat i förhållande till den reella risken.

- **Grundläggande rättigheter**

EU har åtagit sig att iaktta höga standarder i fråga om skydd av grundläggande rättigheter. Alla frivilliga arrangemang för informationsutbyte mellan entiteter som främjas genom detta direktiv kommer att genomföras i betrodda miljöer med full respekt för unionens dataskyddsregler, särskilt Europaparlamentets och rådets förordning (EU) 2016/679⁸.

4. BUDGETKONSEKVENSER

Se finansieringsöversikten

5. ÖVRIGA INSLAG

- **Genomförandeplaner samt åtgärder för övervakning, utvärdering och rapportering**

Förslaget omfattar en allmän plan för övervakning och utvärdering av effekterna på de särskilda målen, enligt vilken kommissionen är skyldig att göra en översyn minst [54 månader] efter ikraftträdandet, och att rapportera till Europaparlamentet och rådet om de viktigaste resultaten.

Översynen ska genomföras i enlighet med kommissionens riktlinjer för bättre lagstiftning.

- **Ingående redogörelse för de specifika bestämmelserna i förslaget**

Förslaget är uppbyggt kring flera viktiga politikområden som är kopplade till varandra och har till syfte att höja cybersäkerhetsnivån i unionen.

Innehåll och tillämpningsområde (artikel 1 och artikel 2)

I direktivet a) fastställs skyldigheter för medlemsstaterna att anta en nationell strategi för cybersäkerhet och utse behöriga nationella myndigheter, gemensamma kontaktpunkter och CSIRT-enheter, b) föreskrivs att medlemsstaterna ska fastställa riskhanterings- och rapporteringsskyldigheter beträffande cybersäkerhet för entiteter av den typ som betecknas som väsentliga entiteter i bilaga I och viktiga entiteter i bilaga II, och c) föreskrivs att medlemsstaterna ska fastställa skyldigheter avseende informationsutbyte om cybersäkerhet.

Det är tillämpligt på vissa offentliga eller privata väsentliga entiteter som är verksamma inom de sektorer som förtecknas i bilaga I (energi, transporter, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, dricksvatten, avloppsvatten, digital

⁸ Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

infrastruktur, offentlig förvaltning och rymden) och på vissa viktiga entiteter som är verksamma inom de sektorer som förtecknas i bilaga II (post- och budtjänster, avfallshantering, tillverkning, produktion och distribution av kemikalier, produktion, bearbetning och distribution av livsmedel, tillverkning och leverantörer av digitala tjänster). Mikroföretag och små företag i den mening som avses i kommissionens rekommendation 2003/361/EG av den 6 maj 2003 omfattas inte av direktivets tillämpningsområde, med undantag av tillhandahållare av elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster, tillhandahållare av betrodda tjänster, registreringsenheter för toppdomäner och offentlig förvaltning, samt vissa andra entiteter som till exempel den enda leverantören av tjänst i en medlemsstat.

Nationella ramar för cybersäkerhet (artiklarna 5–11)

Medlemsstaterna får skyldighet att anta en nationell strategi för cybersäkerhet som anger strategiska mål och relevanta politiska och reglerande åtgärder, i syfte att uppnå och upprätthålla en hög cybersäkerhetsnivå.

Direktivet fastställer också en ram för samordnad information om sårbarheter och kräver att medlemsstaterna utser CSIRT-enheter som ska fungera som betrodda mellanhänder och underlätta interaktionen mellan rapporterande entiteter och tillverkare eller leverantörer av IKT-produkter eller IKT-tjänster. Enisa får skyldighet att utveckla och upprätthålla ett europeiskt sårbarhetsregister för konstaterade sårbarheter.

Medlemsstaterna får skyldighet att införa nationella ramar för hantering av cyberkriser, bland annat genom att utse nationella behöriga myndigheter med ansvar för hantering av storskaliga cyberincidenter och cyberkriser.

Medlemsstaterna blir skyldiga att utse en eller flera nationella myndigheter med behörighet för cybersäkerhet, med uppgift att utöva tillsyn enligt detta direktiv, och en nationell gemensam kontaktpunkt för cybersäkerhet (*gemensam kontaktpunkt*) med en sambandsfunktion för att säkerställa gränsöverskridande samarbete mellan medlemsstaternas myndigheter. Medlemsstaterna får även skyldighet att utse CSIRT-enheter.

Samarbete (artiklarna 12–16)

Direktivet inrättar en samarbetsgrupp i syfte att stödja och underlätta strategiskt samarbete och utbyte av information mellan medlemsstaterna och att utveckla förtroende och tillit. Det inrättar också ett nätverk av CSIRT-enheter för att bidra till att utveckla förtroende och tillit mellan medlemsstaterna och för att främja snabbt och effektivt operativt samarbete.

Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe) inrättas för att stödja en samordnad hantering av storskaliga cyberincidenter och cyberkriser och för att säkerställa ett regelbundet informationsutbyte mellan medlemsstaterna och EU:s institutioner.

Enisa får skyldighet att, i samarbete med kommissionen, vartannat år utfärda en rapport om cybersäkerhetssituationen i unionen.

Kommissionen får skyldighet att inrätta ett system för regelbundna sakkunnigbedömningar av hur ändamålsenlig medlemsstaternas cybersäkerhetspolitik är.

Riskhanterings- och rapporteringskrav för cybersäkerhet (artiklarna 17–23)

Direktivet kräver att medlemsstaterna föreskriver att alla ledningsorgan inom entiteter som omfattas av detta direktiv godkänner de riskhanteringsåtgärder för cybersäkerhet som respektive entitet vidtar och att de genomgår särskild cybersäkerhetsrelaterad utbildning.

Medlemsstaterna blir skyldiga att säkerställa att entiteter som omfattas av direktivet vidtar ändamålsenliga och proportionella tekniska och organisatoriska åtgärder för att hantera cyberrisker som hotar säkerheten i nätverks- och informationssystem. De blir också skyldiga att säkerställa att entiteter underrättar de nationella behöriga myndigheterna eller CSIRT-enheterna om cyberincidenter som har en betydande inverkan på tillhandahållandet av deras tjänster.

Registreringsenheter för toppdomäner och de enheter som tillhandahåller domännamnsregistreringstjänster för toppdomäner får skyldighet att samla in och upprätthålla korrekta och fullständiga registreringsuppgifter för domännamn. Vidare blir sådana enheter skyldiga att ge legitima åtkomstsökande effektiv åtkomst till domänregistreringsuppgifter.

Jurisdiktion och registrering (artiklarna 24 och 25)

Som regel anses alla väsentliga och viktiga entiteter omfattas av jurisdiktionen i den medlemsstat där de tillhandahåller sina tjänster. Vissa typer av entiteter (leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster och leverantörer av nätverk för innehållsleverans samt digitala leverantörer) anses omfattas av jurisdiktionen i den medlemsstat där de har sitt huvudsakliga etableringsställe i unionen. Syftet är att säkerställa att sådana entiteter inte ställs inför en mängd olika rättsliga krav, då de tillhandahåller tjänster över gränserna i en särskilt stor omfattning. Enisa får skyldighet att skapa och upprätthålla ett register över denna typ av entiteter.

Informationsutbyte (artiklarna 26 och 27)

Medlemsstaterna måste föreskriva regler som möjliggör för entiteter att delta i informationsutbyte om cybersäkerhet inom ramen för särskilda arrangemang för utbyte av information om cybersäkerhet, i enlighet med artikel 101 i EUF-fördraget. Utöver detta måste medlemsstater tillåta entiteter som inte omfattas av tillämpningsområdet för detta direktiv att på frivillig basis rapportera om betydande incidenter, cyberhot eller tillbud.

Tillsyn och efterlevnadskontroll (artiklarna 28–34)

Behöriga myndigheter får skyldighet att utöva tillsyn över entiteter som omfattas av detta direktivs tillämpningsområde, särskilt för att säkerställa att de fullgör säkerhets- och incidentrapporteringskraven. Direktivet skiljer mellan förhandstillsyn för väsentliga entiteter och efterhandstillsyn för viktiga entiteter – den senare kräver att behöriga myndigheter vidtar åtgärder när de har tillgång till bevis eller indikationer på att en viktig entitet inte uppfyller säkerhets- och incidentrapporteringskraven.

Direktivet kräver också att medlemsstaterna ålägger väsentliga och viktiga entiteter administrativa sanktionsavgifter och direktivet fastställer vissa högsta bötesbelopp.

Medlemsstaterna får skyldighet att vid behov samarbeta och bistå varandra när entiteter tillhandahåller tjänster i mer än en medlemsstat eller när en entitet har sitt huvudsakliga etableringsställe eller en företrädare i en medlemsstat medan dess nätverks- och informationssystem är belägna i en eller flera andra medlemsstater.

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV**om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148**

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT
 DETTA DIREKTIV

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 114,
 med beaktande av Europeiska kommissionens förslag,
 efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,
 med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande⁹,
 med beaktande av Regionkommitténs yttrande¹⁰,
 i enlighet med det ordinarie lagstiftningsförfarandet, och
 av följande skäl:

- (1) Syftet med Europaparlamentets och rådets direktiv (EU) 2016/1148¹¹ var att bygga upp cybersäkerhetskapaciteten i hela unionen, minska hoten mot nätverks- och informationssystem som används för att tillhandahålla samhällsviktiga tjänster i centrala sektorer och säkerställa kontinuiteten i sådana tjänster när de utsätts för cyberincidenter, och därigenom bidra till att unionens ekonomi och samhälle kan fungera effektivt.
- (2) Sedan ikraftträdandet av direktiv (EU) 2016/1148 har det gjorts betydande framsteg med att öka unionens nivå av resiliens på cybersäkerhetsområdet. Översynen av det direktivet har visat att det har fungerat som katalysator för den institutionella och lagstiftningsmässiga strategin för cybersäkerhet i unionen och har banat väg för en betydande attitydförändring. Direktivet har säkerställt fullbordandet av nationella ramar genom att fastställa nationella strategier för cybersäkerhet, inrätta nationell kapacitet och genomföra lagstiftningsåtgärder som omfattar viktig infrastruktur och viktiga aktörer som identifierats av varje medlemsstat. Det har också bidragit till samarbete på unionsnivå genom inrättandet av samarbetsgruppen¹² och ett nätverk av nationella it-incidentcentrum (*CSIRT-nätverket*)¹³. Trots dessa framsteg har översynen

⁹ EUT C [...], [...], s. [...].

¹⁰ EUT C [...], [...], s. [...].

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

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

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

av direktiv (EU) 2016/1148 avslöjat inneboende brister som hindrar det från att effektivt hantera samtida och framväxande utmaningar på cybersäkerhetsområdet.

- (3) Nätverks- och informationssystem har utvecklats till att vara ett centralt inslag i vardagslivet i och med den snabba digitala omställningen och sammankopplingen av samhället, vilket även gäller vid gränsöverskridande utbyten. Denna utveckling har lett till en expansion av hotbilden mot cybersäkerheten, vilket medfört nya utmaningar som kräver anpassade, samordnade och innovativa svarsåtgärder i alla medlemsstater. Cyberincidenter, som blir allt fler och mer omfattande, sofistikerade och vanliga och får allt större inverkan, utgör ett allvarligt hot mot nätverks- och informationssystemens funktion. Därför kan sådana cyberincidenter hindra utövandet av ekonomisk verksamhet på den inre marknaden, generera ekonomiska förluster, undergräva användarnas förtroende och orsaka allvarlig skada för unionens ekonomi och samhälle. Beredskap och ändamålsenlighet på cybersäkerhetsområdet är därför nu viktigare än någonsin för att den inre marknaden ska kunna fungera väl.
- (4) Den rättsliga grunden för direktiv (EU) 2016/1148 var artikel 114 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget), vars mål är att upprätta den inre marknaden och säkerställa dess funktion genom att förbättra åtgärderna för tillnärmning av nationella regler. De cybersäkerhetskrav som åläggs entiteter som tillhandahåller tjänster eller ekonomiskt relevant verksamhet varierar avsevärt mellan medlemsstaterna vad gäller typen av krav, kravens utförlighet och tillsynsmetoden. Dessa skillnader medför extra kostnader och gör det svårt för företagen att erbjuda varor och tjänster över gränserna. Krav som ställs av en medlemsstat och som skiljer sig från eller rentav står i strid med krav som ställs av en annan medlemsstat, kan väsentligt påverka dessa gränsöverskridande verksamheter. Det är dessutom sannolikt att illa utformade eller otillräckligt genomförda standarder för cybersäkerhet i en medlemsstat kommer att få återverkningar för cybersäkerhetsnivån i andra medlemsstater, särskilt med tanke på det intensiva utbytet över gränserna. Översynen av direktiv (EU) 2016/1148 har visat på stora skillnader i genomförandet från en medlemsstat till en annan, även vad gäller dess tillämpningsområde, då avgränsningen av detta i stor utsträckning har överlåtits på medlemsstaterna. Direktiv (EU) 2016/1148 gav också medlemsstaterna mycket stort utrymme för skönsmässig bedömning vad gäller genomförandet av de incidentrapporteringskyldigheter som anges i det. Dessa skyldigheter genomfördes därför på väsentligt skilda sätt på nationell nivå. Liknande skillnader i genomförandet uppstod i fråga om direktivets bestämmelser om tillsyn och efterlevnadskontroll.
- (5) Alla dessa skillnader medför en fragmentering av den inre marknaden och kan ha en potentiellt skadlig inverkan på dess funktion, vilket påverkar i synnerhet tillhandahållandet av tjänster över gränserna och nivån av cybersäkerhetsresiliens till följd av tillämpningen av olika standarder. Direktivets mål är att undanröja dessa stora skillnader mellan medlemsstater, särskilt genom att föreskriva minimiregler för ett fungerande samordnat regelverk genom fastställande av mekanismer för effektivt samarbete mellan de ansvariga myndigheterna i varje medlemsstat, genom uppdatering av förteckningen över sektorer och verksamheter som omfattas av skyldigheter vad gäller cybersäkerhet och genom föreskrivande av effektiva rättsmedel och sanktioner, vilket är avgörande för att upprätthålla en effektiv kontroll av att dessa skyldigheter efterlevs. Därför bör direktiv (EU) 2016/1148 upphävas och ersättas av det här direktivet.
- (6) Detta direktiv påverkar inte medlemsstaternas förmåga att vidta de åtgärder som är nödvändiga för att skydda deras väsentliga säkerhetsintressen, upprätthålla allmän

ordning och säkerhet och möjliggöra utredning, upptäckt och lagföring av brott, i överensstämmelse med unionsrätten. Enligt artikel 346 i EUF-fördraget ska ingen medlemsstat vara förpliktad att lämna information vars avslöjande den anser strida mot sina väsentliga säkerhetsintressen. Nationella regler och unionsregler till skydd för säkerhetsklassificerade uppgifter, sekretessavtal, eller informella sekretessavtal såsom *Traffic Light Protocol*¹⁴, är relevanta i detta sammanhang.

- (7) Med upphävandet av direktiv (EU) 2016/1148 bör tillämpningsområdet med avseende på olika sektorer utvidgas till en större del av ekonomin mot bakgrund av beaktandena i skälen 4–6. Täckningen av sektorer enligt direktiv (EU) 2016/1148 bör därför utvidgas så att den ger en omfattande täckning av sektorer och tjänster som är av avgörande betydelse för viktiga samhällseliga och ekonomiska verksamheter på den inre marknaden. Reglerna bör inte vara olika beroende på om entiteterna är leverantörer av samhällsviktiga tjänster eller leverantörer av digitala tjänster. En sådan differentiering har visat sig vara inaktuell eftersom den inte återspeglar den faktiska betydelse som dessa sektorer och tjänster har för samhällseliga och ekonomiska verksamheter på den inre marknaden.
- (8) I enlighet med direktiv (EU) 2016/1148 hade medlemsstaterna ansvaret för att fastställa vilka entiteter som uppfyllde kriterierna för att klassificeras som leverantörer av samhällsviktiga tjänster (*identifieringsförfarande*). För att begränsa de stora skillnaderna mellan medlemsstater i detta avseende och säkerställa rättslig säkerhet vad gäller riskhanteringskraven och rapporteringsskyldigheterna för alla relevanta entiteter, bör det fastställas ett enhetligt kriterium för vilka entiteter som ska omfattas av tillämpningsområdet för detta direktiv. Kriteriet bör bestå i tillämpningen av en storleksbaserad regel genom vilken alla medelstora och stora företag, enligt definitionen i kommissionens rekommendation 2003/361/EG¹⁵, som är verksamma i de sektorer eller tillhandahåller den typ av tjänster som omfattas av direktivet också omfattas av direktivets tillämpningsområde. Medlemsstaterna bör inte vara skyldiga att upprätta en förteckning över entiteter som uppfyller detta allmänt tillämpliga storleksbaserade kriterium.
- (9) Små entiteter och mikroentiteter som uppfyller vissa kriterier som visar att de spelar en nyckelroll i medlemsstaternas ekonomier eller samhällen eller för särskilda sektorer eller typer av tjänster, bör emellertid också omfattas av detta direktiv. Medlemsstaterna bör ha ansvaret för att upprätta en förteckning över sådana entiteter och lämna in den till kommissionen.
- (10) Kommissionen kan, i samarbete med samarbetsgruppen, utfärda riktlinjer om genomförandet av de kriterier som ska tillämpas på mikroföretag och små företag.
- (11) Beroende på inom vilken sektor de bedriver sin verksamhet eller vilken typ av tjänst de tillhandahåller bör de entiteter som omfattas av tillämpningsområdet för detta direktiv indelas i två kategorier: väsentliga och viktiga. Denna kategoriindelning bör ta hänsyn till hur kritisk sektorn eller typen av tjänst är, såväl som beroendegraden hos andra sektorer eller typer av tjänster. Väsentliga och viktiga entiteter bör omfattas av samma riskhanteringskrav och rapporteringsskyldigheter. Tillsyns- och

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

¹⁵ Kommissionens rekommendation 2003/361/EG av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (EUT L 124, 20.5.2003, s. 36).

sanktionssystemen bör dock differentieras mellan dessa två kategorier i syfte att säkerställa en rättvis balans mellan krav och skyldigheter å ena sidan och den administrativa börda som följer av tillsynen av fullgörandet å den andra.

- (12) Lagstiftning och instrument som är sektorsspecifika kan bidra till att säkerställa höga nivåer av cybersäkerhet, samtidigt som de fullt ut beaktar de enskilda sektorernas särdrag och komplexitet. När det i sektorsspecifika unionsrättsakter föreskrivs att väsentliga eller viktiga entiteter ska anta åtgärder för att hantera cybersäkerhetsrisker eller rapportera incidenter eller betydande cyberhot och dessa bestämmelser har minst samma verkan som de skyldigheter som fastställs i detta direktiv, bör dessa relevanta sektorsspecifika bestämmelser, inbegripet om tillsyn och efterlevnadskontroll, tillämpas. Kommissionen kan utfärda riktlinjer avseende genomförandet av *lex specialis*. Detta direktiv hindrar inte antagandet av kompletterande sektorsspecifika unionsrättsakter innehållande riskhanteringsåtgärder för cybersäkerhet eller åtgärder för incidentrapportering. Detta direktiv påverkar inte de befintliga genomförandebefogenheter som har tilldelats kommissionen med avseende på ett antal sektorer, däribland transport och energi.
- (13) Europaparlamentets och rådets förordning XXXX/XXXX¹⁶ bör betraktas som en sektorsspecifik unionsrättsakt vid tillämpning av detta direktiv med avseende på entiteter i den finansiella sektorn. Bestämmelserna i förordning XXXX/XXXX rörande riskhanteringsåtgärder för informations- och kommunikationsteknik (IKT), hantering av IKT-relaterade incidenter, särskilt incidentrapportering, samt om rapportering om testning av digital operativ motståndskraft, arrangemang för informationsutbyte och IKT-tredjepartsrisk bör tillämpas i stället för dem som fastställs i detta direktiv. Medlemsstaterna bör därför inte tillämpa detta direktivs bestämmelser om riskhanterings- och rapporteringsskyldigheter beträffande cybersäkerhet, om informationsutbyte eller om tillsyn och efterlevnadskontroll på finansiella entiteter som omfattas av förordning XXXX/XXXX. Det är samtidigt viktigt att upprätthålla starka förbindelser och informationsutbyte med finanssektorn inom ramen för detta direktiv. Därför gör förordning XXXX/XXXX det möjligt för alla finansiella tillsynsmyndigheter, de europeiska tillsynsmyndigheterna för finanssektorn och de nationella behöriga myndigheterna enligt förordning XXXX/XXXX att delta i de strategiska politiska diskussionerna och det tekniska arbetet inom ramen för samarbetsgruppen, och att utbyta information och samarbeta med de gemensamma kontaktpunkter som utsetts enligt detta direktiv och med de nationella CSIRT-enheterna. De behöriga myndigheterna enligt förordning XXXX/XXXX bör även översända uppgifter om större IKT-relaterade incidenter till de gemensamma kontaktpunkter som utsetts enligt detta direktiv. Vidare bör medlemsstaterna fortsätta att inkludera finanssektorn i sina strategier för cybersäkerhet och de nationella CSIRT-enheterna kan inbegripa finanssektorn i sin verksamhet.
- (14) Med beaktande av kopplingarna mellan cybersäkerhet och entiteters fysiska säkerhet bör man säkerställa samstämmighet mellan Europaparlamentet och rådets direktiv (EU) XXX/XXX¹⁷ och detta direktiv. För att uppnå detta bör medlemsstaterna säkerställa att kritiska entiteter och med dessa likvärdiga entiteter enligt direktiv (EU) XXX/XXX anses vara väsentliga entiteter enligt detta direktiv. Medlemsstaterna bör även säkerställa att deras strategier för cybersäkerhet tillhandahåller en politisk ram för ökat samarbete mellan den behöriga myndigheten enligt detta direktiv och den

¹⁶

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

¹⁷

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

behöriga myndigheten enligt direktiv (EU) XXX/XXX när det gäller informationsutbyte om incidenter och cyberhot och utövandet av tillsynsuppgifter. Myndigheter enligt båda direktiven bör samarbeta och utbyta information, särskilt när det gäller identifiering av kritiska entiteter, cyberhot, cybersäkerhetsrisker, incidenter som påverkar kritiska entiteter samt när det gäller cybersäkerhetsåtgärder som vidtas av kritiska entiteter. På begäran av behöriga myndigheter enligt direktiv (EU) XXXX/XXXX bör behöriga myndigheter enligt det här direktivet få utöva sina tillsyns- och efterlevnadskontrollbefogenheter avseende en väsentlig entitet som identifierats som kritisk. Bägge myndigheter bör samarbeta och utbyta information i detta syfte.

- (15) Att upprätthålla och bevara ett tillförlitligt, resilient och säkert domännamnssystem (DNS) är en viktig faktor för att upprätthålla internets integritet och är avgörande för en kontinuerlig och stabil drift, vilket den digitala ekonomin och samhället är beroende av. Därför bör detta direktiv tillämpas på alla leverantörer av DNS-tjänster längs hela DNS-uppslagningskedjan, inbegripet operatörer av rotnamnsservrar, toppdomänsservrar, auktoritativa namnservrar för domännamn och rekursiva resolvrar.
- (16) Molntjänster bör omfatta tjänster som möjliggör administration av beställtjänster och bred fjärråtkomst till en skalbar och elastisk pool av delbara och distribuerade dataresurser. Sådana dataresurser omfattar resurser såsom nätverk, servrar eller annan infrastruktur, operativsystem, programvara, lagring, applikationer och tjänster. Distribueringsmodellerna för molntjänster bör omfatta privat moln, gemensamt moln, offentligt moln och hybridmoln. De ovannämnda tjänste- och distribueringsmodellerna har samma innebörd som termerna tjänste- och distribueringsmodeller som definieras i standarden ISO/IEC 17788:2014. Molnanvändarens kapacitet att ensidigt självständigt tillhandahålla datorkapacitet, såsom servertid eller nätlagring, utan någon mänsklig medverkan från leverantören av molntjänster kan beskrivas som beställtjänster. Termen *bred fjärråtkomst* används för att beskriva att molnkapaciteten tillhandahålls över nätet och nås genom mekanismer som främjar användning av heterogena tunna eller tjocka klientplattformar (däribland mobiltelefoner, surfplattor, bärbara datorer och arbetsstationer). Termen *skalbar* avser dataresurser som leverantören av molntjänster fördelar på ett flexibelt sätt, oberoende av resursernas geografiska läge, för att hantera fluktuationer i efterfrågan. Termen *elastisk pool* används för att beskriva dataresurser som avsätts och utnyttjas beroende på efterfrågan för att tillgängliga resurser snabbt ska kunna utökas och minskas i takt med arbetsbördan. Termen *delbar* används för att beskriva dataresurser som tillhandahålls flera användare som delar en gemensam åtkomst till tjänsten där behandlingen genomförs separat för varje användare, även om tjänsten tillhandahålls från samma elektroniska utrustning. Termen *distribuerad* används för att beskriva de dataresurser som finns på olika nätverksanslutna datorer eller enheter och som kommunicerar och samordnar sig sinsemellan genom meddelandepassning.
- (17) Med tanke på framväxten av innovativ teknik och nya affärsmodeller, förväntas nya molntjänster och nya servicemodeller att uppstå på marknaden som svar på kundernas föränderliga behov. I detta sammanhang kan molntjänster levereras i en mycket distribuerad form, ännu närmare den plats där data genereras eller samlas in, och därmed övergå från den traditionella modellen till en mycket distribuerad modell (*edge computing*).
- (18) Tjänster som erbjuds av leverantörer av datacentraltjänster tillhandahålls inte alltid i form av molntjänster. Därför ingår inte datacentraler alltid i en molninfrastruktur. För att hantera alla risker för säkerheten i nätverks- och informationssystem bör detta

direktiv även omfatta leverantörer av datacentraltjänster som inte är molnbaserade. Vid tillämpningen av detta direktiv bör *datacentraltjänst* omfatta strukturer, eller grupper av strukturer, avsedda för centraliserad inkvartering, sammankoppling och drift av it- och nätutrustning som tillhandahåller datalagrings-, databehandlings- och datatransporttjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll. Termen *datacentraltjänst* är inte tillämplig på interna datacentraler som ägs och drivs för egen räkning av den berörda entiteten.

- (19) Tillhandahållare av posttjänster i den mening som avses i Europaparlamentets och rådets direktiv 97/67/EG¹⁸, och tillhandahållare av budtjänster, bör omfattas av detta direktiv om de tillhandahåller minst ett led i postleveranskedjan, särskilt insamling, sortering och distribution, inklusive upphämtning. Transporttjänster som inte utförs i samband med något av dessa steg bör inte omfattas av tillämpningsområdet för posttjänster.
- (20) Dessa växande ömsesidiga beroendeförhållanden är resultatet av ett allt mer gränsöverskridande nätverk av tillhandahållande av tjänster, med ett inbördes beroende, som använder central infrastruktur över hela unionen inom sektorerna energi, transport, digital infrastruktur, dricks- och avloppsvatten, hälso- och sjukvård, vissa aspekter av offentlig förvaltning, samt rymden i den mån tillhandahållandet av vissa tjänster som är beroende av markbaserad infrastruktur som ägs, förvaltas och drivs av medlemsstater eller privata parter berörs; därför omfattas inte infrastruktur som ägs, förvaltas eller drivs av unionen eller på unionens vägnar som en del av dess rymdprogram. Dessa beroendeförhållanden innebär att alla störningar, även sådana som inledningsvis är begränsade till en entitet eller sektor, kan få dominoeffekter i vidare bemärkelse, vilket kan leda till långtgående och långvariga effekter på tillhandahållandet av tjänster på hela den inre marknaden. Covid-19-pandemin har visat hur sårbara våra alltmer av varandra beroende samhällen är för risker med låg sannolikhet.
- (21) Mot bakgrund av skillnaderna i nationella förvaltningsstrukturer och för att skydda befintliga sektorsspecifika arrangemang eller unionens tillsyns- och regleringsorgan, bör medlemsstaterna kunna utse mer än en nationell behörig myndighet med ansvar för att utföra uppgifter som rör säkerheten i de nätverks- och informationssystem som används av väsentliga och viktiga entiteter enligt detta direktiv. Medlemsstaterna bör kunna tilldela en befintlig myndighet denna roll.
- (22) För att underlätta gränsöverskridande samarbete och kommunikation mellan myndigheter och för att göra det möjligt att genomföra detta direktiv på ett effektivt sätt måste varje medlemsstat utse en nationell gemensam kontaktpunkt med ansvar för samordningen av frågor angående säkerhet i nätverks- och informationssystem och gränsöverskridande samarbete på unionsnivå.
- (23) Behöriga myndigheter eller CSIRT-enheter bör motta underrättelser om incidenter från entiteter på ett ändamålsenligt och effektivt sätt. Den gemensamma kontaktpunkten bör ges i uppgift att vidarebefordra incidentrapporter till de gemensamma kontaktpunkterna i andra berörda medlemsstater. I syfte att säkerställa en gemensam kontaktpunkt i varje medlemsstat bör, på myndighetsnivå i medlemsstaterna, den gemensamma kontaktpunkten också vara mottagare av relevant information om

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

incidenter rörande entiteter i den finansiella sektorn från de behöriga myndigheterna enligt förordning XXXX/XXXX; mottagarna bör kunna vidarebefordra denna information till de relevanta nationella behöriga myndigheterna eller till CSIRT-enheterna enligt detta direktiv, beroende på vad som är lämpligt.

- (24) Medlemsstaterna bör ha både den tekniska och organisatoriska kapacitet som krävs för att förebygga, upptäcka, vidta åtgärder mot och begränsa effekterna av incidenter och risker vad gäller nätverks- och informationssystem. Medlemsstater bör därför säkerställa att de har väl fungerande CSIRT-enheter, även kallade incidenthanteringsorganisationer (Computer Emergency Response Teams, Cert), som uppfyller grundläggande krav i syfte att garantera effektiv och kompatibel kapacitet att hantera incidenter och risker och säkerställa ett effektivt samarbete på unionsnivå. För att stärka förtroendeförhållandet mellan entiteterna och CSIRT-enheterna, i fall där en CSIRT-enhet är en del av den behöriga myndigheten, bör medlemsstaterna överväga funktionell åtskillnad mellan de operativa uppgifter som utförs av CSIRT-enheten, särskilt när det gäller informationsutbyte och stöd till entiteterna, och de behöriga myndigheternas tillsynsverksamhet.
- (25) Vad gäller personuppgifter bör CSIRT-enheterna, i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679¹⁹, på en entitets vägnar och begäran inom ramen för detta direktiv tillhandahålla en proaktiv skanning av de nätverks- och informationssystem som används för att tillhandahålla deras tjänster. Medlemsstaterna bör sträva efter att säkerställa en lika hög nivå av teknisk kapacitet hos alla sektoriella CSIRT-enheter. Medlemsstaterna får begära bistånd från Europeiska unionens cybersäkerhetsbyrå (Enisa) vid inrättandet av nationella CSIRT-enheter.
- (26) Med tanke på vikten av internationellt samarbete på området cybersäkerhet, bör CSIRT-enheterna kunna delta i internationella samarbetsnätverk utöver det CSIRT-nätverk som inrättas genom detta direktiv.
- (27) I enlighet med bilagan till kommissionens rekommendation (EU) 2017/1548 om samordnade insatser vid storskaliga cyberincidenter och cyberkriser på alla relevanta nivåer²⁰, bör en storskalig cyberincident anses vara en incident som påverkar två eller flera medlemsstater eller som leder till störningar som är så omfattande att den berörda medlemsstaten inte kan hantera dem på egen hand. Beroende på orsak och verkan kan storskaliga incidenter eskalera och förvandlas till fullt utvecklade kriser som hindrar den inre marknaden från att fungera korrekt. Med beaktande av sådana incidenters stora omfattning och, i de flesta fall, gränsöverskridande karaktär, bör medlemsstater och relevanta EU-institutioner, -organ och -byråer samarbeta på teknisk, operativ och politisk nivå i syfte att på lämpligt sätt samordna insatserna i hela unionen.
- (28) Eftersom utnyttjandet av sårbarheter i nätverks- och informationssystem kan orsaka betydande störningar och skada, är snabb identifiering och snabbt åtgärdande av dessa sårbarheter en viktig faktor för att minska cybersäkerhetsrisken. Entiteter som utvecklar sådana system bör därför inrätta lämpliga förfaranden för att hantera sårbarheter när de upptäcks. Eftersom sårbarheter ofta upptäcks och rapporteras (meddelas) av tredjeparter (rapporterande entiteter) bör tillverkaren eller leverantören

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

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

av IKT-produkter eller IKT-tjänster även införa nödvändiga förfaranden för att motta sårbarhetsinformation från tredjeparter. I detta avseende ger standarderna ISO/IEC 30111 och ISO/IEC 29417 vägledning om sårbarhetshantering respektive meddelande av information om sårbarheter. När det gäller meddelande av information om sårbarheter är samordning mellan rapporterande entiteter och tillverkare eller leverantörer av IKT-produkter eller IKT-tjänster särskilt viktig. Samordnad information om sårbarheter specificerar en strukturerad process genom vilken sårbarheter rapporteras till organisationer på ett sätt som gör det möjligt för organisationen att diagnostisera och åtgärda sårbarheter innan detaljerad information om sårbarheten meddelas tredjeparter eller allmänheten. Samordnad information om sårbarheter bör även omfatta samordning mellan den rapporterande entiteten och organisationen vad gäller tidpunkten för åtgärdandet och offentliggörandet av sårbarheter.

- (29) Medlemsstaterna bör därför vidta åtgärder för att underlätta samordnad information om sårbarheter genom att fastställa en relevant nationell policy. I detta avseende bör medlemsstaterna utse en CSIRT-enhet i rollen som samordnare, och som vid behov ska fungera som mellanhand mellan den rapporterande entiteten och tillverkarna eller tillhandahållarna av IKT-produkter eller IKT-tjänster. CSIRT-samordnarens uppgifter bör särskilt omfatta att identifiera och kontakta berörda entiteter, stödja rapporterande entiteter, förhandla om tidsramar för meddelande av information och hantera samordnad information om sårbarheter som påverkar flera organisationer (meddelande av information om sårbarheter omfattande flera parter). När sårbarheter påverkar flera tillverkare eller tillhandahållare av IKT-produkter eller IKT-tjänster etablerade i fler än en medlemsstat ska den utsedda CSIRT-enheten i varje berörd medlemsstat samarbeta inom CSIRT-nätverket.
- (30) Tillträde till korrekt och läglig information om sårbarheter som påverkar IKT-produkter och -tjänster bidrar till en förbättrad riskhantering på cybersäkerhetsområdet. I detta avseende är källor till offentligt tillgänglig information om sårbarheter ett viktigt verktyg för entiteter och deras användare, men även nationella myndigheter och CSIRT-enheter. Av denna anledning bör Enisa upprätta ett sårbarhetsregister där väsentliga och viktiga entiteter och deras leverantörer, samt entiteter som inte omfattas av tillämpningsområdet för detta direktiv, på frivillig basis kan meddela information om sårbarheter och tillhandahålla sårbarhetsinformation som möjliggör för användarna att vidta lämpliga riskreducerande åtgärder.
- (31) Även om liknande sårbarhetsregister och databaser faktiskt finns, förvaltas och underhålls dessa av entiteter som inte är etablerade i unionen. Ett europeiskt sårbarhetsregister som upprätthålls av Enisa skulle ge förbättrad insyn i processen för offentliggörande innan sårbarheten offentliggjorts officiellt, samt motståndskraft i händelse av störningar eller avbrott i tillhandahållandet av liknande tjänster. För att undvika dubbelarbete och i så hög grad som möjligt eftersträva komplementaritet bör Enisa undersöka möjligheten att ingå avtal om strukturerat samarbete med liknande register i tredjelandsjurisdiktioner.
- (32) Samarbetsgruppen bör vartannat år upprätta ett arbetsprogram som omfattar de åtgärder som ska vidtas av gruppen för att genomföra dess mål och uppgifter. Tidsramen för det första program som antas enligt detta direktiv bör anpassas till tidsramen för det senaste program som antas enligt direktiv (EU) 2016/1148, i syfte att undvika potentiella avbrott i gruppens arbete.

- (33) Vid utarbetandet av vägledningsdokument bör samarbetsgruppen konsekvent kartlägga nationella lösningar och erfarenheter, bedöma hur samarbetsgruppens resultat påverkar nationella strategier, diskutera utmaningar i samband med genomförandet och formulera särskilda rekommendationer som ska beaktas för ett bättre genomförande av befintliga bestämmelser.
- (34) Samarbetsgruppen bör förbli ett flexibelt forum och kunna reagera på föränderliga och nya politiska prioriteringar och utmaningar samtidigt som tillgången till resurser beaktas. Den bör anordna regelbundna gemensamma möten med relevanta privata intressenter från hela unionen för att diskutera gruppens verksamhet och inhämta synpunkter på framväxande politiska frågor. För att stärka samarbetet på unionsnivå, bör gruppen överväga att bjuda in unionsorgan och -byråer som arbetar med frågor som rör cybersäkerhetspolitiken, såsom Europeiska it-brottcentrumet (EC3), Europeiska unionens byrå för luftfartssäkerhet (Easa) och Europeiska unionens rymdprogrambyrå (EUSPA) att delta i samarbetet.
- (35) De behöriga myndigheterna och CSIRT-enheterna bör ha befogenhet att delta i utbytesprogram för tjänstemän från andra medlemsstater i syfte att förbättra samarbetet. De behöriga myndigheterna bör vidta nödvändiga åtgärder för att tjänstemän från andra medlemsstater ska kunna spela en faktisk roll i verksamheten inom den behöriga värdmyndigheten.
- (36) Unionen bör i tillämpliga fall ingå internationella avtal, i enlighet med artikel 218 i EUF-fördraget, med tredjeländer eller internationella organisationer, och därvid tillåta och organisera deras deltagande i vissa av samarbetsgruppens och CSIRT-nätverkets verksamheter. Sådana avtal bör säkerställa ändamålsenligt skydd av uppgifter.
- (37) Medlemsstaterna bör bidra till inrättandet av en EU-ram för hantering av cyberkriser enligt rekommendation (EU) 2017/1584 genom de befintliga samarbetsnätverken, särskilt Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe), CSIRT-nätverket och samarbetsgruppen. EU-CyCLONe och CSIRT-nätverket bör samarbeta på grundval av förfaranden som fastställer formerna för detta samarbete. Arbetsordningen för EU-CyCLONe bör ytterligare specificera de förutsättningar enligt vilka nätverket ska fungera, inbegripet men inte begränsat till roller, samarbetsformer, samverkan med andra relevanta aktörer och mallar för informationsutbyte, samt kommunikationsmedel. För krishantering på unionsnivå bör berörda parter stödja sig på EU:s integrerade arrangemang för politisk krishantering (IPCR). Kommissionen bör använda Argus-förfarandet för gränsöverskridande krissamordning på hög nivå för detta ändamål. Om krisen har en yttre dimension eller en dimension som rör den gemensamma säkerhets- och försvarspolitik (GSFP) och denna dimension är betydande, bör Europeiska utrikestjänstens krishanteringsmekanism aktiveras.
- (38) Vid tillämpningen av detta direktiv bör termen *risk* avse risken för förlust eller störning orsakad av en cyberincident och bör uttryckas som en kombination av omfattningen av förlusten eller störningen och sannolikheten för att en sådan incident inträffar.
- (39) Vid tillämpningen av detta direktiv bör termen *tillbud* avse en händelse som potentiellt skulle ha kunnat orsaka skada, men som framgångsrikt hindrades från att utvecklas fullt ut.
- (40) Åtgärder för riskhantering bör omfatta åtgärder för att identifiera alla incidentrisker, för att förebygga, upptäcka och hantera incidenter och för att begränsa deras inverkan.

Säkerheten i nätverks- och informationssystem bör omfatta lagrade, överförda och behandlade uppgifters säkerhet.

- (41) För att undvika oproportionella finansiella och administrativa bördor för väsentliga och viktiga entiteter bör riskhanteringskraven för cybersäkerhet stå i proportion till den risk som det berörda nätverks- och informationssystemet utgör, med beaktande av bästa praxis för sådana åtgärder.
- (42) Väsentliga och viktiga entiteter bör säkerställa säkerheten i de nätverks- och informationssystem som de använder i sin verksamhet. Det rör sig framför allt om privata nätverks- och informationssystem som antingen förvaltas av deras interna it-personal eller vilkas säkerhet har lagts ut på entreprenad. Riskhanterings- och rapporteringskraven för cybersäkerhet enligt detta direktiv bör tillämpas på de relevanta väsentliga och viktiga entiteterna oavsett om de sköter underhållet av sina nätverks- och informationssystem internt eller lägger ut uppgifterna på entreprenad.
- (43) Det är särskilt viktigt att hantera cybersäkerhetsrisker som härrör från en entitets leveranskedja och dess förhållande till sina leverantörer, med tanke på förekomsten av incidenter där entiteter har fallit offer för cyberattacker och där illvilliga aktörer har kunnat äventyra säkerheten i en entitets nätverks- och informationssystem genom att utnyttja sårbarheter som påverkar tredje parts produkter och tjänster. Entiteterna bör därför bedöma och beakta sina leverantörers och tjänsteleverantörers övergripande produktkvalitet och cybersäkerhetspraxis, inbegripet deras förfaranden för säker utveckling.
- (44) Bland tjänsteleverantörerna har leverantörer av hanterade säkerhetstjänster (managed security services providers, MSSP) på områden som incidenthantering, penetrationstester, säkerhetsrevisioner och konsulttjänster en särskilt viktig roll när det gäller att bistå entiteter i deras arbete med att upptäcka och reagera på incidenter. Dessa MSSP har dock också själva varit mål för cyberattacker, och genom att de är nära integrerade i operatörernas verksamhet utgör de en särskild cybersäkerhetsrisk. Entiteterna bör därför visa större noggrannhet vid valet av en MSSP.
- (45) Entiteterna bör också hantera cybersäkerhetsrisker som härrör från deras samverkan och förbindelser med andra intressenter inom ett vidare ekosystem. I synnerhet bör entiteterna vidta lämpliga åtgärder för att säkerställa att deras samarbete med akademiska institutioner och forskningsinstitut sker i linje med deras cybersäkerhetsstrategier och följer god praxis när det gäller säker tillgång till och spridning av information i allmänhet och skydd av immateriella rättigheter i synnerhet. Likaså, med tanke på hur viktiga och värdefulla data är för entiteternas verksamhet, bör entiteterna, när de förlitar sig på dataomvandlings- och dataanalystjänster från tredje parter, vidta alla lämpliga cybersäkerhetsåtgärder.
- (46) För att ytterligare hantera centrala risker i leveranskedjan och hjälpa entiteter som är verksamma i sektorer som omfattas av detta direktiv att på lämpligt sätt hantera cybersäkerhetsrisker i leveranskedjan och leverantörsrelaterade cybersäkerhetsrisker bör samarbetsgruppen tillsammans med relevanta nationella myndigheter, i samarbete med kommissionen och Enisa, utföra samordnade sektorsvisa riskbedömningar av leveranskedjan, vilket redan gjorts för 5G-nät efter rekommendation (EU) 2019/534

om it-säkerhet i 5G-nät²¹, i syfte att per sektor identifiera kritiska IKT-tjänster, IKT-system eller IKT-produkter, relevanta hot och sårbarheter.

- (47) Riskbedömningar av leveranskedjan bör, mot bakgrund av den berörda sektorns särdrag, ta hänsyn till både tekniska och när så är lämpligt icke-tekniska faktorer, inbegripet de som anges i rekommendation (EU) 2019/534, i den EU-omfattande samordnade riskbedömningen av säkerhet i 5G-nät och i EU:s verktygslåda för 5G-cybersäkerhet som samarbetsgruppen enats om. För att identifiera de leveranskedjor som bör bli föremål för en samordnad riskbedömning bör följande kriterier beaktas: i) i vilken utsträckning väsentliga och viktiga entiteter använder och förlitar sig på specifika kritiska IKT-tjänster, IKT-system eller IKT-produkter, ii) specifika kritiska IKT-tjänsters, IKT-systems eller IKT-produkters relevans för att utföra kritiska eller känsliga funktioner, inbegripet behandling av personuppgifter, iii) tillgången till alternativa IKT-tjänster, IKT-system eller IKT-produkter, iv) motståndskraften i hela leveranskedjan för IKT-tjänster, IKT-system eller IKT-produkter mot störningar, och v) för framväxande IKT-tjänster, IKT-system eller IKT-produkter, deras potentiella framtida betydelse för entiteternas verksamhet.
- (48) För att rationalisera de rättsliga skyldigheter som åläggs tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster, och tillhandahållare av betrodda tjänster med anknytning till säkerheten i deras nätverks- och informationssystem, samt för att göra det möjligt för dessa entiteter och deras respektive behöriga myndigheter att dra nytta av den rättsliga ram som inrättas genom detta direktiv (inbegripet utseende av CSIRT-enheter med ansvar för risk- och incidenthantering, deltagande av behöriga myndigheter och organ i samarbetsgruppens och CSIRT-nätverkets arbete) bör de omfattas av tillämpningsområdet för detta direktiv. De motsvarande bestämmelser som anges i Europaparlamentets och rådets förordning (EU) nr 910/2014²² och Europaparlamentets och rådets direktiv (EU) 2018/1972²³ och som gäller införande av säkerhets- och anmälningskrav för dessa typer av entiteter bör därför upphävas. Reglerna om rapporteringsskyldigheter bör inte påverka tillämpningen av förordning (EU) 2016/679 och Europaparlamentets och rådets direktiv 2002/58/EG²⁴.
- (49) När så är lämpligt och för att undvika onödiga störningar bör befintliga nationella riktlinjer och nationell lagstiftning som antagits för införlivandet av bestämmelserna om säkerhetsåtgärder i artikel 40.1 i direktiv (EU) 2018/1972 samt kraven i artikel 40.2 i det direktivet när det gäller de parametrar som rör en incidents betydelse fortsätta att användas av de behöriga myndigheter som ansvarar för tillsyn och efterlevnadskontroll vid tillämpningen av detta direktiv.
- (50) Mot bakgrund av den ökande betydelsen av nummeroberoende interpersonella kommunikationstjänster är det nödvändigt att se till att sådana tjänster också omfattas

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

²² Europaparlamentets och rådets förordning (EU) nr 910/2014 av den 23 juli 2014 om elektronisk identifiering och betrodda tjänster för elektroniska transaktioner på den inre marknaden och om upphävande av direktiv 1999/93/EG (EUT L 257, 28.8.2014, s. 73).

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

²⁴ Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 31.7.2002, s. 37).

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

- (51) Den inre marknaden är mer beroende av ett fungerande internet än någonsin tidigare. Tjänster från praktiskt taget alla väsentliga och viktiga entiteter är beroende av tjänster som tillhandahålls via internet. För att säkerställa ett smidigt tillhandahållande av tjänster som levereras från väsentliga och viktiga entiteter är det viktigt att allmänna elektroniska kommunikationsnät, t.ex. stamnät för internet eller sjökablar för telekommunikation, har infört lämpliga cybersäkerhetsåtgärder och rapporterar incidenter i samband med dessa.
- (52) När så är lämpligt bör entiteterna informera sina tjänstemottagare om särskilda och betydande hot och om åtgärder dessa kan vidta för att minska den åtföljande risken för dem själva. Kravet på att informera mottagarna om sådana hot bör inte befria entiteter från skyldigheten att på egen bekostnad vidta lämpliga och omedelbara åtgärder för att förebygga eller avhjälpa cyberhot och återställa tjänstens normala säkerhetsnivå. Mottagarna bör kostnadsfritt tillhandahållas sådan information om säkerhetshot.
- (53) Särskilt bör tillhandahållare av allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster informera tjänstemottagarna om särskilda och betydande cyberhot och om åtgärder de kan vidta för att säkerställa säkerheten för sin kommunikation, t.ex. genom att använda särskilda typer av programvara eller krypteringsteknik.
- (54) För att trygga säkerheten för elektroniska kommunikationsnät och kommunikationstjänster bör användningen av kryptering, särskilt totalsträckskryptering, främjas och vid behov vara obligatorisk för tillhandahållare av sådana tjänster och nät i enlighet med principerna om automatisk och inbyggd säkerhet och automatiskt och inbyggt integritetsskydd vid tillämpningen av artikel 18. Användningen av totalsträckskryptering bör förenas med medlemsstaternas befogenheter att säkerställa skyddet av sina väsentliga säkerhetsintressen och sin allmänna säkerhet och att möjliggöra utredning, avslöjande och lagföring av brott i enlighet med unionsrätten. Lösningar för laglig åtkomst till information i totalsträckskrypterad kommunikation bör upprätthålla krypteringens effektivitet när det gäller att skydda den personliga integriteten och kommunikationssäkerheten, och samtidigt möjliggöra en effektiv brottsbekämpning.
- (55) I detta direktiv fastställs en tvåstegsstrategi för incidentrapportering för att hitta rätt balans mellan, å ena sidan, snabb rapportering som bidrar till att minska den potentiella spridningen av incidenter och gör det möjligt för entiteter att söka stöd, och, å andra sidan, ingående rapportering som drar värdefulla lärdomar av enskilda incidenter och med tiden förbättrar enskilda företags och hela sektors motståndskraft mot cyberhot. Om entiteter får kännedom om en incident bör de vara skyldiga att lämna in en första underrättelse inom 24 timmar, följt av en slutrapport senast en månad därefter. Den första underrättelsen bör endast innehålla den information som är absolut nödvändig för att göra de behöriga myndigheterna medvetna om incidenten

och för att entiteten vid behov ska kunna söka hjälp. En sådan underrättelse bör, i tillämpliga fall, ange om incidenten sannolikt har orsakats av olagliga eller avsiktligt skadliga handlingar. Medlemsstaterna bör säkerställa att kravet att lämna in denna första underrättelse inte avleder den rapporterande entitetens resurser från verksamheter i samband med incidenthantering som bör prioriteras. För att ytterligare förhindra att incidentrapporteringsskyldigheter avleder resurser från incidenthantering eller på annat sätt kan äventyra entiteternas ansträngningar i detta avseende, bör medlemsstaterna också föreskriva att den berörda entiteten, i vederbörligen motiverade fall och efter överenskommelse med de behöriga myndigheterna eller CSIRT-enheten, får avvika från tidsfristerna på 24 timmar för den första underrättelsen och en månad för slutrapporten.

- (56) Väsentliga och viktiga entiteter befinner sig ofta i en situation där en viss incident på grund av sina särdrag måste rapporteras till flera olika myndigheter till följd av anmälningsskyldigheter enligt olika rättsliga instrument. Sådana fall skapar ytterligare bördor och kan också leda till osäkerhet om format och förfaranden för sådana underrättelser. Mot bakgrund av detta och, i syfte att förenkla rapporteringen av säkerhetsincidenter, bör medlemsstaterna inrätta *en gemensam kontaktpunkt* för alla underrättelser som krävs enligt detta direktiv och även enligt annan unionslagstiftning, t.ex. förordning (EU) 2016/679 och direktiv 2002/58/EG. Enisa bör i samarbete med samarbetsgruppen utarbeta gemensamma mallar för underrättelser med hjälp av riktlinjer som skulle förenkla och rationalisera den rapporteringsinformation som krävs enligt unionsrätten och minska företagens bördor.
- (57) Om en incident misstänks ha samband med allvarlig brottslig verksamhet enligt unionsrätt eller nationell rätt, bör medlemsstaterna uppmuntra väsentliga och viktiga entiteter att, på grundval av tillämpliga straffrättsliga bestämmelser i enlighet med unionsrätten, rapportera incidenter som misstänks vara av allvarlig brottslig art till de relevanta rättsvårdande myndigheterna. Där så är lämpligt, och utan att det påverkar de bestämmelser om skydd av personuppgifter som gäller för Europol, är det önskvärt att samordning mellan behöriga myndigheter och rättsvårdande myndigheter i olika medlemsstater underlättas av EC3 och Enisa.
- (58) Säkerheten för personuppgifter undergrävs ofta till följd av incidenter. I detta sammanhang bör de behöriga myndigheterna samarbeta och utbyta information om alla relevanta frågor med dataskyddsmyndigheterna och tillsynsmyndigheterna i enlighet med direktiv 2002/58/EG.
- (59) Att upprätthålla korrekta och fullständiga databaser med domännamn och registreringsuppgifter (*WHOIS-data*) och ge laglig åtkomst till sådana uppgifter är avgörande för att säkerställa domännamnssystemets säkerhet, stabilitet och resiliens, vilket i sin tur bidrar till en hög gemensam nivå av cybersäkerhet inom unionen. Om behandlingen inbegriper personuppgifter ska sådan behandling vara förenlig med unionens dataskyddslagstiftning.
- (60) Dessa uppgifters tillgänglighet och offentliga myndigheters möjlighet att få åtkomst till dem i rätt tid, inbegripet behöriga myndigheter enligt unionslagstiftning eller nationell lagstiftning för förebyggande, utredning eller lagföring av brott, incidenthanteringsorganisationer (Cert), CSIRT-enheter, och när det gäller uppgifter om deras klienter för tillhandahållare av elektroniska kommunikationsnät och kommunikationstjänster och tillhandahållare av cybersäkerhetsteknik och cybersäkerhetstjänster som agerar för dessa kunders räkning, är avgörande för att förebygga och bekämpa missbruk av domännamnssystem, särskilt för att förebygga,

upptäcka och reagera på cybersäkerhetsincidenter. Sådan åtkomst bör vara förenlig med unionens dataskyddslagstiftning i den mån den rör personuppgifter.

- (61) För att säkerställa tillgången till korrekta och fullständiga registreringsuppgifter för domännamn bör registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster för toppdomäner samla in och garantera integriteten och tillgängligheten för registreringsuppgifterna för domännamn. I synnerhet bör registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster för toppdomäner fastställa policyer och förfaranden för insamling och lagring av korrekta och fullständiga registreringsuppgifter samt för att förhindra och korrigera felaktiga registreringsuppgifter i enlighet med unionens dataskyddsregler.
- (62) Registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster för dem bör offentliggöra registreringsuppgifter för domännamn som inte omfattas av unionens dataskyddsregler, till exempel uppgifter som rör juridiska personer²⁵. Registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster för toppdomäner bör också möjliggöra för legitima åtkomstsökande att få laglig åtkomst till specifika registreringsuppgifter för domännamn som rör fysiska personer, i enlighet med unionens dataskyddslagstiftning. Medlemsstaterna bör se till att registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster för dem utan onödigt dröjsmål besvarar ansökningar från legitima åtkomstsökande om utlämnande av registreringsuppgifter för domännamn. Registreringsenheter för toppdomäner och de entiteter som tillhandahåller domännamnsregistreringstjänster bör fastställa riktlinjer och förfaranden för offentliggörande och utlämnande av registreringsuppgifter, inbegripet servicenivåavtal för att hantera ansökningar om åtkomst från legitima åtkomstsökande. Åtkomstförfarandet kan också omfatta användning av ett gränssnitt, en portal eller ett annat tekniskt verktyg som ett effektivt system för att begära och få tillgång till registreringsuppgifter. I syfte att främja harmoniserad praxis på hela den inre marknaden får kommissionen anta riktlinjer för sådana förfaranden utan att det påverkar Europeiska dataskyddsstyrelsens befogenheter.
- (63) Alla väsentliga och viktiga entiteter enligt detta direktiv bör omfattas av jurisdiktionen i den medlemsstat där de tillhandahåller sina tjänster. Om entiteten tillhandahåller tjänster i mer än en medlemsstat bör den omfattas av dessa medlemsstaters separata och parallella jurisdiktioner samtidigt. De behöriga myndigheterna i dessa medlemsstater bör samarbeta, ge varandra ömsesidigt bistånd och vid behov genomföra gemensamma tillsynsåtgärder.
- (64) För att ta hänsyn till den gränsöverskridande karaktären hos de tjänster och den verksamhet som bedrivs av leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, tillhandahållare av nätverk för innehållsleverans, leverantörer av molntjänster, leverantörer av datacentraltjänster och digitala leverantörer bör endast en medlemsstat ha jurisdiktion över dessa entiteter. Jurisdiktion bör tilldelas den medlemsstat där respektive entitet har sitt huvudsakliga etableringsställe i unionen. Kriteriet för etableringsställe i detta direktiv förutsätter att verksamhet faktiskt bedrivs

²⁵

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

genom en stabil struktur. Den rättsliga formen för en sådan struktur, oavsett om det är en filial eller ett dotterföretag med status som juridisk person, bör inte vara den avgörande faktorn i detta avseende. Huruvida kriteriet är uppfyllt bör inte vara beroende av om nätverks- och informationssystemen är fysiskt belägna på en viss plats. Förekomsten och användningen av sådana system utgör inte i sig en sådan huvudsaklig etablering och är därför inte avgörande kriterier för att fastställa det huvudsakliga etableringsstället. Det huvudsakliga etableringsstället bör vara den plats där besluten om åtgärder för att hantera cybersäkerhetsrisker fattas i unionen. Detta motsvarar vanligtvis platsen för företagets huvudkontor i unionen. Om sådana beslut inte fattas i unionen bör det huvudsakliga etableringsstället anses vara beläget i den medlemsstat där entiteten har ett etableringsställe med flest anställda i unionen. Om tjänsterna utförs av en koncern bör det kontrollerande företagets huvudsakliga etableringsställe betraktas som koncernens huvudsakliga etableringsställe.

- (65) I de fall där en leverantör av DNS-tjänster, registreringsenhet för toppdomäner, tillhandahållare av nätverk för innehållsleverans, leverantör av molntjänster, leverantör av datacentraltjänster eller digital leverantör som inte är etablerad i unionen erbjuder tjänster inom unionen, bör den utse en företrädare. I syfte att fastställa om en sådan entitet erbjuder tjänster inom unionen bör det kontrolleras om det är uppenbart att entiteten planerar att erbjuda tjänster till personer i en eller flera medlemsstater. Enbart den omständigheten att en entitets eller en mellanhands webbplats, eller en e-postadress och andra kontaktuppgifter, är tillgängliga i unionen, eller att ett språk används som allmänt används i det tredjeland där entiteten är etablerad, är inte tillräcklig för att fastställa en sådan avsikt. Emellertid kan faktorer som att det används ett visst språk eller en viss valuta som allmänt används i en eller flera medlemsstater med möjligheten att beställa tjänster på detta andra språk, eller att kunder eller användare i unionen omnämns, göra det uppenbart att entiteten planerar att erbjuda tjänster inom unionen. Företrädaren bör agera på entitetens vägnar och det bör vara möjligt för behöriga myndigheter eller CSIRT-enheterna att kontakta företrädaren. Företrädaren bör utses uttryckligen genom en skriftlig fullmakt från entiteten att agera på dess vägnar med avseende på dess skyldigheter enligt detta direktiv, inklusive incidentrapportering.
- (66) Om uppgifter som anses vara säkerhetsskyddsklassificerade enligt nationell rätt eller unionsrätt utbyts, rapporteras eller på annat sätt delas enligt bestämmelserna i detta direktiv, bör motsvarande särskilda regler för hantering av säkerhetsskyddsklassificerade uppgifter tillämpas.
- (67) I och med att cyberhoten blir mer komplexa och sofistikerade är goda åtgärder för upptäckt och förebyggande i stor utsträckning beroende av ett regelbundet utbyte av underrättelser om hot och sårbarhet mellan entiteter. Informationsutbyte bidrar till ökad medvetenhet om cyberhot, vilket i sin tur ökar entiteternas förmåga att förhindra att hot blir verkliga incidenter och gör det möjligt för entiteterna att bättre begränsa effekterna av incidenter och återhämta sig mer effektivt. I avsaknad av vägledning på unionsnivå verkar flera faktorer ha hindrat sådant utbyte av underrättelser, särskilt osäkerheten om förenligheten med konkurrens- och ansvarsreglerna.
- (68) Entiteter bör uppmuntras att kollektivt utnyttja sina individuella kunskaper och praktiska erfarenheter på strategisk, taktisk och operativ nivå i syfte att förbättra förmågan att på lämpligt sätt bedöma, övervaka, försvara sig mot och reagera på cyberhot. Det är därför nödvändigt att på unionsnivå möjliggöra framväxten av mekanismer för frivilligt informationsutbyte. I detta syfte bör medlemsstaterna aktivt stödja och uppmuntra även relevanta entiteter som inte omfattas av detta direktivs

tillämpningsområde att delta i sådana mekanismer för informationsutbyte. Dessa mekanismer bör genomföras helt i enlighet med unionens konkurrensregler och unionens regler om uppgiftsskydd.

- (69) Behandling av personuppgifter som utförs av entiteter, offentliga myndigheter, incidenthanteringsorganisationer (Cert), CSIRT-enheter och tillhandahållare av säkerhetsteknik och säkerhetstjänster i den utsträckning som är absolut nödvändig och proportionell för att säkerställa nät- och informationssäkerhet bör utgöra ett berättigat intresse för den personuppgiftsansvarige i fråga, i enlighet med förordning (EU) 2016/679. Detta bör innebära åtgärder som rör förebyggande, upptäckt, analys och hantering av incidenter, åtgärder för att öka medvetenheten om specifika cyberhot, informationsutbyte i samband med åtgärdande av och samordnat utlämnande av information om sårbarhet, samt frivilligt informationsutbyte om dessa incidenter samt cyberhot och sårbarheter, angreppsindikatorer, taktik, tekniker och förfaranden, cybersäkerhetsvarningar och konfigurationsverktyg. Sådana åtgärder kan kräva behandling av följande typer av personuppgifter: ip-adresser, webbadresser (URL), domännamn och e-postadresser.
- (70) För att stärka de tillsynsbefogenheter och tillsynsåtgärder som bidrar till att säkerställa ett effektivt fullgörande av skyldigheter bör detta direktiv innehålla en minimiförteckning över tillsynsåtgärder och tillsynsmedel genom vilka behöriga myndigheter kan utöva tillsyn över väsentliga och viktiga entiteter. Dessutom bör detta direktiv fastställa en differentiering av tillsynssystemet mellan väsentliga och viktiga entiteter i syfte att säkerställa en rättvis balans vad gäller skyldigheterna för både entiteter och behöriga myndigheter. Väsentliga entiteter bör därför omfattas av ett fullständigt tillsynssystem (förhandstillsyn och efterhandstillsyn), medan viktiga entiteter bör omfattas av enklare tillsyn, endast i efterhand. För de senare innebär detta att viktiga entiteter inte systematiskt måste dokumentera uppfyllande av riskhanteringskraven för cybersäkerhet, och att de behöriga myndigheterna bör tillämpa en reaktiv efterhandstillsyn och därmed inte ha någon allmän skyldighet att utöva tillsyn över dessa entiteter.
- (71) För att efterlevnadskontrollen ska bli effektiv bör det fastställas en minimiförteckning över administrativa sanktioner för brott mot de riskhanterings- och rapporteringsskyldigheter för cybersäkerhet som föreskrivs i detta direktiv, med en tydlig och konsekvent ram för sådana sanktioner i hela unionen. Vederbörlig hänsyn bör tas till överträdelsens art, allvarlighetsgrad och varaktighet, de faktiska skador eller förluster som orsakats eller potentiella skador eller förluster som kunde ha uppstått, om överträdelsen är avsiktlig eller beror på försumlighet, vidtagna åtgärder för att förhindra eller begränsa skadorna och/eller förlusterna, graden av ansvar eller relevanta tidigare överträdelser, graden av samarbete med den behöriga myndigheten och andra försvårande eller förmildrande omständigheter. Påförandet av sanktioner, inbegripet administrativa sanktionsavgifter, bör omfattas av lämpliga rättssäkerhetsgarantier i överensstämmelse med de allmänna principerna inom unionsrätten och Europeiska unionens stadga om de grundläggande rättigheterna, vilket inbegriper ett effektivt rättsligt skydd och korrekt rättsligt förfarande.
- (72) För att säkerställa en effektiv efterlevnadskontroll av de skyldigheter som fastställs i detta direktiv bör varje behörig myndighet ha befogenhet att påföra eller begära påförande av administrativa sanktionsavgifter.
- (73) Om administrativa sanktionsavgifter påförs ett företag, bör ett företag i detta sammanhang anses vara ett företag i den mening som avses i artiklarna 101 och 102 i

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

- (74) Medlemsstaterna bör kunna fastställa bestämmelser om straffrättsliga påföljder för överträdelse av de nationella bestämmelser som införlivar detta direktiv. Påförandet av straffrättsliga påföljder för överträdelse av sådana nationella bestämmelser och relaterade administrativa sanktioner bör dock inte medföra ett åsidosättande av principen *ne bis in idem* enligt domstolens tolkning.
- (75) När detta direktiv inte harmoniserar administrativa sanktioner eller när så är nödvändigt i andra fall, till exempel vid fall av allvarliga överträdelse av de skyldigheter som fastställs i detta direktiv, bör medlemsstaterna genomföra ett system med effektiva, proportionella och avskräckande sanktioner. Dessa sanktioners art, straffrättsliga eller administrativa, bör fastställas i medlemsstaternas nationella rätt.
- (76) För att de sanktioner som är tillämpliga på överträdelse av de skyldigheter som fastställs i detta direktiv ska bli mer effektiva och avskräckande bör de behöriga myndigheterna ges befogenhet att tillämpa sanktioner i form av tillfälligt upphävande av en certifiering eller auktorisation för en del av eller alla tjänster som tillhandahålls av en väsentlig entitet och införande av ett tillfälligt förbud för en fysisk person att utöva ledande funktioner. Med tanke på sanktionernas stränghet och påverkan på entiteternas verksamheter och i sista hand deras konsumenter bör sådana sanktioner endast tillämpas proportionellt mot överträdelsens allvarlighetsgrad och med beaktande av de särskilda omständigheterna i varje enskilt fall, inbegripet om överträdelsen är avsiktlig eller beror på försumlighet samt vidtagna åtgärder för att förhindra eller begränsa skadorna och/eller förlusterna. Sådana sanktioner bör endast tillämpas som sista utväg, dvs. först efter det att de andra relevanta åtgärder för efterlevnadskontroll som fastställs i detta direktiv har uttömts, och endast fram till dess att de entiteter som omfattas av sanktionerna vidtar nödvändiga åtgärder för att avhjälpa de brister eller uppfylla de krav från den behöriga myndigheten för vilka sanktionerna tillämpades. Påförandet av sådana sanktioner måste omfattas av lämpliga rättssäkerhetsgarantier i enlighet med de allmänna principerna i unionsrätten och Europeiska unionens stadga om de grundläggande rättigheterna, inbegripet effektivt rättsligt skydd, korrekt rättsförfarande, oskuldspresumtion och rätten till försvar.
- (77) Detta direktiv bör fastställa regler för samarbete mellan de behöriga myndigheterna och tillsynsmyndigheterna i enlighet med förordning (EU) 2016/679 för att hantera överträdelse som rör personuppgifter.
- (78) Detta direktiv bör syfta till att säkerställa en hög ansvarsnivå för riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter på organisationsnivå. Av dessa skäl bör ledningsorganen för de entiteter som omfattas av detta direktiv godkänna riskåtgärderna för cybersäkerhet och övervaka deras genomförande.
- (79) Det bör införas en mekanism för sakkunnigbedömning som gör det möjligt för experter utsedda av medlemsstaterna att bedöma genomförandet av

cybersäkerhetsstrategier, inbegripet medlemsstaternas kapacitetsnivå och tillgängliga resurser.

- (80) För att ta hänsyn till nya cyberhot, teknisk utveckling eller sektorsspecifika särdrag bör befogenheten att anta akter i enlighet med artikel 290 i EUF-fördraget delegeras till kommissionen med avseende på de delar som rör riskhanteringsåtgärder som krävs enligt detta direktiv. Kommissionen bör också ges befogenhet att anta delegerade akter som fastställer vilka kategorier av väsentliga entiteter som ska vara skyldiga att erhålla ett certifikat och enligt vilka specifika europeiska ordningar för cybersäkerhetscertifiering detta ska ske. Det är särskilt viktigt att kommissionen genomför lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå, och att dessa samråd genomförs i enlighet med principerna i det interinstitutionella avtalet om bättre lagstiftning av den 13 april 2016²⁶. För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter erhåller Europaparlamentet och rådet alla handlingar samtidigt som medlemsstaternas experter, och deras experter ges systematiskt tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.
- (81) I syfte att säkerställa enhetliga villkor för genomförandet av de relevanta bestämmelserna i detta direktiv med avseende på de förfaranden som krävs för samarbetsgruppens verksamhet, de tekniska aspekterna av riskhanteringsåtgärder eller typen av information i incidentunderrättelser samt formatet och förfarandet för sådana underrättelser, bör kommissionen ges genomförandebefogenheter. Dessa befogenheter bör utövas i enlighet med Europaparlamentets och rådets förordning (EU) nr 182/2011²⁷.
- (82) Detta direktiv bör med jämna mellanrum ses över av kommissionen i samråd med berörda parter, främst i syfte att avgöra behovet av ändringar med hänsyn till samhällsutvecklingen, den politiska utvecklingen, den tekniska utvecklingen eller ändrade marknadsvillkor.
- (83) Eftersom målet för detta direktiv, nämligen att uppnå en hög gemensam cybersäkerhetsnivå i unionen, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i fördraget om Europeiska unionen. I enlighet med proportionalitetsprincipen i samma artikel går detta direktiv inte utöver vad som är nödvändigt för att uppnå detta mål.
- (84) Detta direktiv respekterar de grundläggande rättigheterna och iakttar de principer som erkänns i Europeiska unionens stadga om de grundläggande rättigheterna, i synnerhet rätten till respekt för privatliv och kommunikationer, skydd av personuppgifter, näringsfriheten, rätten till egendom, rätten till ett effektivt rättsmedel och rätten att yttra sig. Detta direktiv bör genomföras i enlighet med dessa rättigheter och principer.

²⁶ EUT L 123, 12.5.2016, s. 1.

²⁷ Europaparlamentets och rådets förordning (EU) nr 182/2011 av den 16 februari 2011 om fastställande av allmänna regler och principer för medlemsstaternas kontroll av kommissionens utövande av sina genomförandebefogenheter (EUT L 55, 28.2.2011, s. 13).

KAPITEL I

Allmänna bestämmelser

Artikel 1

Innehåll

1. I detta direktiv fastställs åtgärder för att säkerställa en hög gemensam cybersäkerhetsnivå i unionen.
2. Direktivet fastställer i detta syfte följande:
 - (a) Skyldigheter för medlemsstaterna att anta nationella strategier för cybersäkerhet och utse behöriga nationella myndigheter, gemensamma kontaktpunkter och enheter för hantering av it-säkerhetsincidenter (CSIRT-enheter).
 - b) Riskhanterings- och rapporteringsskyldigheter beträffande cybersäkerhet för entiteter av den typ som betecknas som väsentliga entiteter i bilaga I och viktiga entiteter i bilaga II.
 - (c) Skyldigheter när det gäller informationsutbyte om cybersäkerhet.

Artikel 2

Tillämpningsområde

1. Detta direktiv är tillämpligt på offentliga och privata entiteter av den typ som betecknas som väsentliga entiteter i bilaga I och viktiga entiteter i bilaga II. Detta direktiv är inte tillämpligt på entiteter som räknas som mikroföretag och små företag i den mening som avses i kommissionens rekommendation 2003/361/EG²⁸.
2. Oavsett entiteternas storlek är dock detta direktiv också i följande fall tillämpligt på entiteter som avses i bilagorna I och II:
 - (a) Följande entiteter som tillhandahåller nedanstående tjänster:
 - i) Allmänna elektroniska kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster som avses i punkt 8 i bilaga I.
 - ii) Tillhandahållare av betrodda tjänster som avses i punkt 8 i bilaga I.
 - iii) De registreringsenheter för toppdomäner och leverantörer av domännamnssystemtjänster (DNS) som avses i punkt 8 i bilaga I.
 - b) Entiteten är en offentlig förvaltningsentitet enligt definitionen i artikel 4.23.
 - c) Entiteten är den enda leverantören av en tjänst i en medlemsstat.

²⁸

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

- d) En potentiell störning av den tjänst som entiteten tillhandahåller skulle kunna påverka skyddet för människors liv och hälsa, den allmänna säkerheten eller folkhälsan.
- e) En potentiell störning av den tjänst som entiteten tillhandahåller skulle kunna medföra systemrisker, särskilt för de sektorer där sådana störningar skulle kunna få gränsöverskridande konsekvenser.
- f) Entiteten är kritisk på grund av sin särskilda betydelse på regional eller nationell nivå för en särskild sektor eller typ av tjänst eller för andra av denna entitet beroende sektorer i medlemsstaten.
- g) Entiteten identifieras som en kritisk entitet enligt Europaparlamentets och rådets direktiv (EU) XXXX/XXXX²⁹ [direktivet om kritiska entiteters motståndskraft] eller som en entitet likvärdig med en kritisk entitet i enlighet med artikel 7 i det direktivet.

Medlemsstaterna ska upprätta en förteckning över entiteter som identifierats i enlighet med leden b–f och överlämna den till kommissionen senast den [sex månader efter tidsfristen för införlivande]. Medlemsstaterna ska regelbundet och minst vartannat år därefter se över förteckningen och vid behov uppdatera den.

3. Detta direktiv påverkar inte medlemsstaternas befogenheter när det gäller att upprätthålla allmän säkerhet, försvar och nationell säkerhet i enlighet med unionsrätten.
4. Detta direktiv påverkar inte tillämpningen av rådets direktiv 2008/114/EG³⁰ eller Europaparlamentets och rådets direktiv 2011/93/EU³¹ och 2013/40/EU³².
5. Utan att det påverkar tillämpningen av artikel 346 i EUF-fördraget får information som är konfidentiell enligt unionsbestämmelser och nationella bestämmelser, såsom bestämmelser om affärshemligheter, utbytas med kommissionen och andra relevanta myndigheter endast när ett sådant utbyte är nödvändigt för att tillämpa detta direktiv. Den information som utbyts ska begränsas till vad som är relevant och proportionellt för ändamålet med utbytet. Vid utbytet ska informationens konfidentialitet bevaras och väsentliga eller viktiga entiteters säkerhets- och affärsintressen skyddas.
6. Om det i sektorsspecifika akter i unionsrätten föreskrivs att väsentliga eller viktiga entiteter ska anta åtgärder för att hantera cybersäkerhetsrisker eller underrätta någon om incidenter eller betydande cyberhot, och om dessa krav har minst samma verkan som de skyldigheter som fastställs i detta direktiv, ska de relevanta bestämmelserna i detta direktiv, inbegripet om tillsyn och efterlevnadskontroll i kapitel VI, inte tillämpas.

²⁹ [ange fullständig titel och EUT-hänvisning om detta är känt]

³⁰ Rådets direktiv 2008/114/EG av den 8 december 2008 om identifiering av, och klassificering som, europeisk kritisk infrastruktur och bedömning av behovet att stärka skyddet av denna (EUT L 345, 23.12.2008, s. 75).

³¹ Europaparlamentets och rådets direktiv 2011/93/EU av den 13 december 2011 om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi samt om ersättande av rådets rambeslut 2004/68/RIF (EUT L 335, 17.12.2011, s. 1).

³² Europaparlamentets och rådets direktiv 2013/40/EU av den 12 augusti 2013 om angrepp mot informationssystem och om ersättande av rådets rambeslut 2005/222/RIF (EUT L 218, 14.8.2013, s. 8).

Artikel 3

Minimiharmonisering

Utan att det påverkar tillämpningen av deras övriga skyldigheter enligt unionsrätten får medlemsstaterna i enlighet med detta direktiv anta eller behålla bestämmelser som säkerställer en högre cybersäkerhetsnivå.

Artikel 4

Definitioner

I detta direktiv gäller följande definitioner:

- (1) *nätverks- och informationssystem*:
 - a) Ett elektroniskt kommunikationsnät i den mening som avses i artikel 2.1 i direktiv (EU) 2018/1972.
 - b) En enhet eller en grupp enheter som är sammankopplade eller hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av digitala uppgifter.
 - c) Digitala uppgifter som lagras, behandlas, hämtas eller överförs med sådana hjälpmedel som omfattas av leden a och b för att de ska kunna drivas, användas, skyddas och underhållas.
- (2) *säkerhet i nätverks- och informationssystem*: nätverks- och informationssystemets förmåga att med en viss tillförlitlighetsnivå motstå åtgärder som undergräver tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de besläktade tjänster som erbjuds genom eller är tillgängliga via dessa nätverks- och informationssystem.
- (3) *cybersäkerhet*: cybersäkerhet i den mening som avses i artikel 2.1 i Europaparlamentets och rådets förordning (EU) 2019/881³³.
- (4) *nationell strategi för cybersäkerhet*: en enhetlig ram i en medlemsstat med strategiska mål och prioriteringar för säkerheten i nätverks- och informationssystem i den medlemsstaten.
- (5) *incident*: varje händelse som undergräver tillgängligheten, riktigheten, integriteten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de besläktade tjänster som erbjuds genom eller är tillgängliga via nätverks- och informationssystem.
- (6) *incidenthantering*: alla åtgärder och förfaranden som syftar till att upptäcka, analysera, begränsa och reagera på en incident.
- (7) *cyberhot*: ett cyberhot i den mening som avses i artikel 2.8 i förordning (EU) 2019/881.

³³ Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten) (EUT L 151, 7.6.2019, s. 15).

- (8) *sårbarhet*: en svaghet, känslighet eller brist hos en tillgång, ett system, en process eller en kontroll som kan utnyttjas genom ett cyberhot.
- (9) *företrädare*: en i unionen etablerad fysisk eller juridisk person som uttryckligen har utsetts att agera för i) en leverantör av DNS-tjänster, en registreringsenhet för toppdomäner, en leverantör av molntjänster, en leverantör av datacentraltjänster eller en leverantör av nätverk för innehållsleverans enligt punkt 8 i bilaga I eller ii) ej i unionen etablerade entiteter enligt punkt 6 i bilaga II till vilka en nationell behörig myndighet eller en CSIRT-enhet kan vända sig i stället för entiteten, i frågor som gäller de skyldigheter som den entiteten har enligt detta direktiv.
- (10) *standard*: en standard i den mening som avses i artikel 2.1 i Europaparlamentets och rådets förordning (EU) nr 1025/2012³⁴.
- (11) *teknisk specifikation*: en teknisk specifikation i den mening som avses i artikel 2.4 i förordning (EU) nr 1025/2012.
- (12) *internetknutpunkt (IXP)*: en nätfacilitet som möjliggör sammankoppling av mer än två oberoende nät (autonoma system), främst i syfte att underlätta utbytet av internettrafik; en IXP tillhandahåller sammankoppling enbart för autonoma system och kräver inte att den internettrafik som passerar mellan två deltagande autonoma system ska passera genom ett tredje autonomt system och ändrar inte heller trafiken eller påverkar den på något annat sätt.
- (13) *domännamnssystem (DNS)*: ett hierarkiskt distribuerat namngivningssystem som gör det möjligt för slutanvändare att nå tjänster och resurser på internet.
- (14) *leverantör av DNS-tjänster*: en entitet som tillhandahåller rekursiva eller auktoritativa tjänster för att lösa domännamnsfrågor till internetsslutanvändare och andra leverantörer av DNS-tjänster.
- (15) *registreringsenhet för toppdomäner*: en enhet som har delegerats en specifik toppdomän och som ansvarar för administrationen av toppdomänen, inbegripet registreringen av domännamn under toppdomänen och den tekniska driften av toppdomänen, inbegripet drift av dess namnservrar, underhåll av dess databaser och distribution av zonfiler för toppdomänen mellan namnservrar.
- (16) *digital tjänst*: en tjänst i den mening som avses i artikel 1.1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535³⁵.
- (17) *marknadsplats online*: en digital tjänst i den mening som avses i artikel 2 n i Europaparlamentets och rådets direktiv 2005/29/EG³⁶.

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

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

³⁶ Europaparlamentets och rådets direktiv 2005/29/EG av den 11 maj 2005 om otillbörliga affärsmetoder som tillämpas av näringsidkare gentemot konsumenterna på den inre marknaden och om ändring av rådets direktiv 84/450/EEG och Europaparlamentets och rådets direktiv 97/7/EG, 98/27/EG och 2002/65/EG samt Europaparlamentets och rådets förordning (EG) nr 2006/2004 (direktiv om otillbörliga affärsmetoder) (EUT L 149, 11.6.2005, s. 22).

- (18) *sökmotor*: en digital tjänst i den mening som avses i artikel 2.5 i Europaparlamentets och rådets förordning (EU) 2019/1150³⁷.
- (19) *molntjänst*: en digital tjänst som möjliggör administration av beställtjänster och bred fjärråtkomst till en skalbar och elastisk pool av delbara och distribuerade dataresurser.
- (20) *datacentraltjänst*: en tjänst som omfattar strukturer, eller grupper av strukturer, avsedda för centraliserad inkvartering, sammankoppling och drift av it- och nätutrustning som tillhandahåller datalagrings-, databehandlings- och datatransporttjänster samt alla anläggningar och infrastrukturer för kraftdistribution och miljökontroll.
- (21) *nätverk för innehållsleverans*: ett nätverk av geografiskt spridda servrar vars syfte är att säkerställa hög tillgänglighet för, tillgång till eller snabb leverans av digitalt innehåll och digitala tjänster till internetanvändare för innehålls- och tjänsteleverantörers räkning.
- (22) *plattform för sociala nätverkstjänster*: en plattform som gör det möjligt för slutanvändare att interagera, dela och upptäcka innehåll, finna andra användare och kommunicera med andra via flera enheter, särskilt genom chattar, inlägg, videor och rekommendationer.
- (23) *offentlig förvaltningsentitet*: en entitet i en medlemsstat som uppfyller följande kriterier:
- (a) Den har inrättats för att tillgodose behov i det allmännas intresse och har inte industriell eller kommersiell karaktär.
 - (b) Den har ställning som juridisk person.
 - (c) Den finansieras till största delen av staten, en regional myndighet eller andra offentlighetsrättsliga organ, eller står under administrativ tillsyn av sådana myndigheter eller organ, eller har ett förvaltnings-, lednings- eller kontrollorgan där mer än hälften av ledamöterna utses av staten, regionala myndigheter eller andra offentlighetsrättsliga organ.
 - (d) Den har befogenhet att rikta administrativa eller reglerande beslut till fysiska eller juridiska personer som påverkar deras rättigheter när det gäller gränsöverskridande rörlighet för personer, varor, tjänster eller kapital.
- Offentliga förvaltningsentiteter som bedriver verksamhet på områdena allmän säkerhet, brottsbekämpning, försvar eller nationell säkerhet ska undantas.
- (24) *entitet*: varje fysisk eller juridisk person som bildats och erkänts som sådan enligt nationell rätt där den etablerats och som i eget namn får utöva rättigheter och ha skyldigheter.
- (25) *väsentlig entitet*: varje entitet av en typ som betecknas som en väsentlig entitet i bilaga I.
- (26) *viktig entitet*: varje entitet av en typ som betecknas som en viktig entitet i bilaga II.

³⁷

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

KAPITEL II

Samordnade regelverk för cybersäkerhet

Artikel 5

Nationell strategi för cybersäkerhet

1. Varje medlemsstat ska anta en nationell strategi för cybersäkerhet som anger strategiska mål och relevanta politiska och reglerande åtgärder, i syfte att uppnå och upprätthålla en hög cybersäkerhetsnivå. Den nationella strategin för cybersäkerhet ska särskilt inbegripa följande:
 - (a) Ett fastställande av mål och prioriteringar för medlemsstatens strategi för cybersäkerhet.
 - (b) En styrningsram för att uppnå dessa mål och prioriteringar, inbegripet de politiska åtgärder som avses i punkt 2 och roller och ansvarsområden för offentliga organ och entiteter samt andra relevanta aktörer.
 - (c) En bedömning för att identifiera relevanta tillgångar och cybersäkerhetsrisker i den medlemsstaten.
 - (d) En identifiering av åtgärder som säkerställer beredskap inför, svar på och återställande efter incidenter, inklusive samarbete mellan offentlig och privat sektor.
 - (e) En förteckning över de olika myndigheter och aktörer som är involverade i genomförandet av den nationella strategin för cybersäkerhet.
 - (f) En politisk ram för förbättrad samordning mellan de behöriga myndigheterna enligt detta direktiv och enligt Europaparlamentets och rådets direktiv (EU) XXXX/XXXX³⁸ [direktivet om kritiska entiteters motståndskraft], i syfte att utbyta information om incidenter och cyberhot och utföra tillsynsuppgifter.
2. Som en del av den nationella strategin för cybersäkerhet ska medlemsstaterna särskilt anta följande:
 - a) En politik för cybersäkerhet i leveranskedjan för IKT-produkter och IKT-tjänster som används av väsentliga och viktiga entiteter när de tillhandahåller sina tjänster.
 - b) Riktlinjer för att inkludera och specificera cybersäkerhetsrelaterade krav för IKT-produkter och IKT-tjänster vid offentlig upphandling.
 - c) En politik för att främja och underlätta samordnad information om sårbarheter i den mening som avses i artikel 6.
 - d) En politik för att upprätthålla den allmänna tillgängligheten och integriteten hos den offentliga kärnan i det öppna internet.
 - e) En politik för att främja och utveckla cybersäkerhetskompetens, medvetandehöjande åtgärder samt forsknings- och utvecklingsinitiativ.
 - f) En politik för stöd till akademiska institutioner och forskningsinstitut för att utveckla cybersäkerhetsverktyg och säker nätinфраstruktur.

³⁸

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

- g) En politik, relevanta förfaranden och lämpliga verktyg för informationsutbyte för att stödja ett frivilligt informationsutbyte om cybersäkerhet mellan företag i enlighet med unionsrätten.
 - h) En politik som tillgodoser särskilda behov hos små och medelstora företag, särskilt de som inte omfattas av detta direktiv, när det gäller vägledning och stöd för att förbättra deras motståndskraft mot cyberhot.
3. Medlemsstaterna ska meddela sina nationella strategier för cybersäkerhet till kommissionen inom tre månader från det att de antagits. Medlemsstaterna får undanta specifik information från detta meddelande om och i den utsträckning det är absolut nödvändigt för att upprätthålla den nationella säkerheten.
4. Medlemsstaterna ska minst vart fjärde år bedöma sina nationella strategier för cybersäkerhet på grundval av centrala resultatindikatorer och vid behov ändra dem. Europeiska unionens cybersäkerhetsbyrå (Enisa) ska på begäran bistå medlemsstaterna vid utarbetandet av en nationell strategi och centrala resultatindikatorer för bedömningen av strategin.

Artikel 6

Samordnad information om sårbarheter och ett europeiskt sårbarhetsregister

1. Varje medlemsstat ska utse en av sina CSIRT-enheter enligt artikel 9 till samordnare för den samordnade informationen om sårbarheter. Den utsedda CSIRT-enheten ska fungera som betrodd mellanhand och vid behov underlätta interaktionen mellan en rapporterande entitet och tillverkare eller leverantörer av IKT-produkter eller IKT-tjänster. Om en rapporterad sårbarhet berör flera tillverkare eller leverantörer av IKT-produkter eller IKT-tjänster i unionen ska den utsedda CSIRT-enheten i varje berörd medlemsstat samarbeta med CSIRT-nätverket.
2. Enisa ska utveckla och underhålla ett europeiskt sårbarhetsregister. I detta syfte ska Enisa inrätta och underhålla lämpliga informationssystem, riktlinjer och förfaranden, särskilt för att göra det möjligt för viktiga och väsentliga entiteter och deras leverantörer av nätverks- och informationssystem att lämna information om och registrera sårbarheter hos IKT-produkter eller IKT-tjänster, samt för att ge alla berörda parter tillgång till den information om sårbarheter som finns i registret. Registret ska särskilt innehålla information som beskriver sårbarheten, den berörda IKT-produkten eller IKT-tjänsten och hur allvarlig sårbarheten är med tanke på de omständigheter under vilka den kan utnyttjas, tillgången till relaterade programfixar och, i avsaknad av tillgängliga programfixar, vägledning riktad till användare av sårbara produkter och tjänster om hur riskerna med meddelade sårbarheter kan minskas.

Artikel 7

Nationella ramar för hantering av cybersäkerhetskriser

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

2. För tillämpning av detta direktiv ska varje medlemsstat identifiera vilka kapaciteter, tillgångar och förfaranden som kan användas i händelse av en kris.
3. Varje medlemsstat ska anta en nationell incident- och krishanteringsplan för cybersäkerhet där mål och villkor för hanteringen av storskaliga cyberincidenter och cyberkriser fastställs. Planen ska särskilt innehålla följande:
 - a) Målen för nationella beredskapsåtgärder och beredskapsverksamheter.
 - b) De nationella behöriga myndigheternas uppgifter och ansvarsområden.
 - c) Krishanteringsförfaranden och kanaler för informationsutbyte.
 - d) Beredskapsåtgärder, inbegripet övningar och utbildningsverksamhet.
 - e) Berörda offentliga och privata parter och berörd infrastruktur.
 - f) Nationella förfaranden och arrangemang mellan relevanta nationella myndigheter och organ för att säkerställa att medlemsstaten på ett ändamålsenligt sätt kan delta i och stödja en samordnad hantering av storskaliga cyberincidenter och cyberkriser på unionsnivå.
4. Medlemsstaterna ska meddela kommissionen när en behörig myndighet utsetts enligt punkt 1 och lämna in sina nationella incident- och krishanteringsplaner för cybersäkerhet enligt punkt 3 inom tre månader från det att myndigheterna utsetts och dessa planer antagits. Medlemsstaterna får undanta specifik information från planen om och i den utsträckning det är absolut nödvändigt för den nationella säkerheten.

Artikel 8

Nationella behöriga myndigheter och gemensamma kontaktpunkter

1. Varje medlemsstat ska utse en eller flera behöriga myndigheter med ansvar för cybersäkerhet och för de tillsynsuppgifter som avses i kapitel VI i detta direktiv. Medlemsstaterna får för detta ändamål utse en eller flera befintliga myndigheter.
2. De behöriga myndigheter som avses i punkt 1 ska övervaka tillämpningen av detta direktiv på nationell nivå.
3. Varje medlemsstat ska utse en nationell gemensam kontaktpunkt för cybersäkerhet (nedan kallad *gemensam kontaktpunkt*). Om en medlemsstat bara utser en behörig myndighet, ska denna behöriga myndighet också vara den gemensamma kontaktpunkten i den medlemsstaten.
4. Varje gemensam kontaktpunkt ska utöva en sambandsfunktion som säkerställer ett gränsöverskridande samarbete mellan medlemsstatens myndigheter och relevanta myndigheter i andra medlemsstater och ett sektorsövergripande samarbete med andra nationella behöriga myndigheter i medlemsstaten.
5. Medlemsstaterna ska säkerställa att de behöriga myndigheter som avses i punkt 1 och de gemensamma kontaktpunkterna har tillräckliga resurser för att på ett ändamålsenligt och effektivt sätt kunna utföra de uppgifter de tilldelas och därigenom uppnå målen med detta direktiv. Medlemsstaterna ska säkerställa att de utsedda företrädarna i den samarbetsgrupp som avses i artikel 12 samarbetar på ett ändamålsenligt, effektivt och säkert sätt.
6. Varje medlemsstat ska utan onödigt dröjsmål underrätta kommissionen om utseendet av den behöriga myndighet som avses i punkt 1 och den gemensamma kontaktpunkt

som avses i punkt 3 och deras uppgifter samt alla senare ändringar. Varje medlemsstat ska offentliggöra utseendet. Kommissionen ska offentliggöra en förteckning över utsedda gemensamma kontaktpunkter.

Artikel 9

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

1. Varje medlemsstat ska utse en eller flera CSIRT-enheter som ska uppfylla kraven i artikel 10.1, omfattande minst de sektorer, delsektorer och entiteter som avses i bilagorna I och II, och som ansvarar för hanteringen av incidenter i enlighet med ett tydligt fastställt förfarande. En CSIRT-enhet får inrättas inom en behörig myndighet som avses i artikel 8.
2. Medlemsstaterna ska säkerställa att varje CSIRT-enhet har tillräckliga resurser för att på ett ändamålsenligt sätt kunna utföra sina uppgifter enligt artikel 10.2.
3. Medlemsstaterna ska säkerställa att varje CSIRT-enhet har tillgång till en lämplig, säker och motståndskraftig kommunikations- och informationsinfrastruktur för utbyte av information med väsentliga och viktiga entiteter och andra relevanta berörda parter. För detta ändamål ska medlemsstaterna se till att CSIRT-enheterna bidrar till införandet av säkra verktyg för informationsutbyte.
4. CSIRT-enheterna ska samarbeta och vid behov utbyta relevant information i enlighet med artikel 26 med betrodda sektoriella eller sektorsövergripande grupper av väsentliga och viktiga entiteter.
5. CSIRT-enheter ska delta i sakkunnigbedömningar som organiseras i enlighet med artikel 16.
6. Medlemsstaterna ska säkerställa ett ändamålsenligt, effektivt och säkert samarbete mellan sina CSIRT-enheter i det CSIRT-nätverk som avses i artikel 13.
7. Medlemsstaterna ska utan onödigt dröjsmål meddela kommissionen de CSIRT-enheter som utsetts i enlighet med punkt 1, den CSIRT-samordnare som utsetts i enlighet med artikel 6.1 och deras respektive uppgifter i förhållande till de entiteter som avses i bilagorna I och II.
8. Medlemsstaterna får begära Enisas bistånd vid inrättandet av nationella CSIRT-enheter.

Artikel 10

Krav på CSIRT-enheter och deras uppgifter

1. CSIRT-enheter ska uppfylla följande krav:
 - a) De ska säkerställa en hög nivå av tillgänglighet för sina kommunikationstjänster genom att undvika felkritiska systemdelar och ska kunna kontaktas och kontakta andra när som helst och på flera olika sätt. De ska tydligt ange kommunikationskanalerna och underrätta användargrupper och samarbetspartner om dessa.
 - b) Deras lokaler och de informationssystem som de använder sig av ska vara belägna på säkra platser.

- c) De ska ha ett ändamålsenligt system för handläggning och dirigering av förfrågningar, särskilt för att underlätta ändamålsenliga och effektiva överlämnanden.
 - d) De ska ha tillräckligt med personal för att ständigt kunna vara tillgängliga.
 - e) De ska utrustas med system med inbyggd redundans och reservlokaler för att säkerställa kontinuiteten i deras tjänster.
 - f) De ska kunna delta i internationella samarbetsnätverk.
2. CSIRT-enheter ska ha följande uppgifter:
- a) Övervakning av cyberhot, sårbarheter och incidenter på nationell nivå.
 - b) Tillhandahållande av tidiga varningar, larm, meddelanden och spridning av information till väsentliga och viktiga entiteter samt till andra relevanta berörda parter om cyberhot, sårbarheter och incidenter.
 - c) Vidtagande av åtgärder till följd av incidenter.
 - d) Tillhandahållande av dynamisk risk- och incidentanalys och situationsmedvetenhet när det gäller cybersäkerhet.
 - e) Tillhandahållande, på begäran av en entitet, av en proaktiv skanning av de nätverks- och informationssystem som används för att tillhandahålla deras tjänster.
 - f) Deltagande i CSIRT-nätverket och ömsesidigt bistånd till andra medlemmar i nätverket på deras begäran.
3. CSIRT-enheter ska upprätta samarbetsförbindelser med relevanta aktörer inom den privata sektorn i syfte att bättre uppnå direktivets mål.
4. För att underlätta samarbetet ska CSIRT-enheterna främja antagande och användning av gemensamma eller standardiserade metoder, klassificeringssystem och taxonomier när det gäller följande:
- a) Förfaranden för incidenthantering.
 - b) Hantering av cybersäkerhetskriser.
 - c) Samordnad information om sårbarheter.

Artikel 11

Samarbete på nationell nivå

1. Om de är separata ska de behöriga myndigheter som avses i artikel 8, den gemensamma kontaktpunkten och CSIRT-enheten eller CSIRT-enheterna i en och samma medlemsstat samarbeta sinsemellan när det gäller fullgörandet av skyldigheter enligt detta direktiv.
2. Medlemsstaterna ska se till att antingen deras behöriga myndigheter eller deras CSIRT-enheter mottar underrättelser om incidenter, betydande cyberhot och tillbud som lämnas in i enlighet med detta direktiv. Om en medlemsstat beslutar att dess CSIRT-enheter inte ska motta sådana underrättelser ska CSIRT-enheterna, i den mån det är nödvändigt för att de ska kunna utföra sina uppgifter, beviljas tillgång till

uppgifter om incidenter som underrättats av väsentliga eller viktiga entiteter i enlighet med artikel 20.

3. Varje medlemsstat ska se till att dess behöriga myndigheter eller CSIRT-enheter informerar sin gemensamma kontaktpunkt om de underrättelser om incidenter, betydande cyberhot och tillbud som lämnas in i enlighet med detta direktiv.
4. I den utsträckning det är nödvändigt för ett ändamålsenligt fullgörande av de uppgifter och skyldigheter som fastställs i detta direktiv ska medlemsstaterna säkerställa ett lämpligt samarbete mellan behöriga myndigheter och gemensamma kontaktpunkter, brottsbekämpande myndigheter, dataskyddsmyndigheter, myndigheter med ansvar för kritisk infrastruktur enligt direktiv (EU) XXXX/XXXX [direktivet om kritiska entiteters motståndskraft] och de nationella finansmyndigheter som utsetts i enlighet med Europaparlamentets och rådets förordning (EU) XXXX/XXXX³⁹ [DORA-förordningen] i den medlemsstaten.
5. Medlemsstaterna ska säkerställa att deras behöriga myndigheter regelbundet lämnar information till de behöriga myndigheter som utsetts i enlighet med direktiv (EU) XXXX/XXXX [direktivet om kritiska entiteters motståndskraft] om cybersäkerhetsrisker, cyberhot och incidenter som berör väsentliga entiteter som identifierats som kritiska eller som likvärdiga med kritiska entiteter, i enlighet med direktiv (EU) XXXX/XXXX [direktivet om kritiska entiteters motståndskraft], samt om de åtgärder som behöriga myndigheter vidtar till följd av dessa risker och incidenter.

KAPITEL III

Samarbete

Artikel 12

Samarbetsgrupp

1. För att stödja och underlätta strategiskt samarbete och informationsutbyte mellan medlemsstaterna på direktivets tillämpningsområde inrättas härmed en samarbetsgrupp.
2. Samarbetsgruppen ska utföra sina uppgifter på grundval av de tvååriga arbetsprogram som avses i punkt 6.
3. Samarbetsgruppen ska bestå av företrädare för medlemsstater, kommissionen och Enisa. Europeiska utrikestjänsten ska delta som observatör i samarbetsgruppens verksamhet. De europeiska tillsynsmyndigheterna i enlighet med artikel 17.5 c i förordning (EU) XXXX/XXXX [DORA-förordningen] får delta i samarbetsgruppens verksamhet.

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

Kommissionen ska tillhandahålla sekretariatet.

³⁹ [ange fullständig titel och EUT-hänvisning om detta är känt]

4. Samarbetsgruppen ska ha följande uppgifter:
 - a) Vägledning till behöriga myndigheter angående införlivande och genomförande av detta direktiv.
 - b) Utbyte av bästa praxis och information i fråga om genomförandet av detta direktiv, bland annat när det gäller cyberhot, incidenter, sårbarheter, tillbud, initiativ för att öka medvetenheten, utbildning, övningar och kompetens, kapacitetsuppbyggnad, standarder och tekniska specifikationer.
 - c) Utbyte av råd och samarbete med kommissionen om framväxande politiska initiativ för cybersäkerhet.
 - d) Utbyte av råd och samarbete med kommissionen om utkast till kommissionens genomförandeakter eller delegerade akter som antas i enlighet med detta direktiv.
 - e) Utbyte av bästa praxis och information med relevanta institutioner, organ och byråer på unionsnivå.
 - f) Diskussioner om de rapporter från sakkunnigbedömningar som avses i artikel 16.7.
 - g) Diskussioner om resultat av sådan gemensam tillsynsverksamhet i gränsöverskridande fall som avses i artikel 34.
 - h) Strategisk vägledning till CSIRT-nätverket om specifika framväxande frågor.
 - i) Bidrag till cybersäkerhetskapaciteten i hela unionen genom att underlätta utbytet av nationella tjänstemän i form av ett kapacitetsuppbyggnadsprogram som inbegriper personal från medlemsstaternas behöriga myndigheter eller CSIRT-enheter.
 - j) Anordnande av regelbundna gemensamma möten med relevanta privata intressenter från hela unionen för att diskutera gruppens verksamhet och inhämta synpunkter på framväxande politiska frågor.
 - k) Diskussioner om det arbete som utförts i samband med cybersäkerhetsövningar, inbegripet det arbete som utförs av Enisa.
5. Samarbetsgruppen får begära en teknisk rapport från CSIRT-nätverket om utvalda frågor.
6. Samarbetsgruppen ska senast den... [24 månader efter dagen för detta direktivs ikraftträdande] och därefter vartannat år upprätta ett arbetsprogram för de åtgärder som ska vidtas för att genomföra dess mål och uppgifter. Tidsramen för det första program som antas enligt detta direktiv ska anpassas till tidsramen för det sista program som antas enligt direktiv (EU) 2016/1148.
7. Kommissionen får anta genomförandeakter i vilka fastställs de förfaranden som krävs för samarbetsgruppens verksamhet. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 37.2.
8. Samarbetsgruppen ska regelbundet och minst en gång om året sammanträda med den grupp för kritiska entiteters motståndskraft som inrättats enligt direktiv (EU) XXXX/XXXX [direktivet om kritiska entiteters motståndskraft], för att främja strategiskt samarbete och informationsutbyte.

Artikel 13
CSIRT-nätverk

1. För att bidra till utvecklingen av förtroende och tillit och för att främja ett snabbt och ändamålsenligt operativt samarbete mellan medlemsstaterna inrättas härmed ett nätverk för nationella CSIRT-enheter.
2. CSIRT-nätverket ska bestå av företrädare för medlemsstaternas CSIRT-enheter och Cert-EU. Kommissionen ska som observatör delta i CSIRT-nätverket. Enisa ska tillhandahålla sekretariatet och aktivt stödja samarbetet mellan CSIRT-enheterna.
3. CSIRT-nätverket ska ha följande uppgifter:
 - (a) Att utbyta information om CSIRT-enheternas kapacitet.
 - (b) Att utbyta relevant information om incidenter, tillbud, cyberhot, risker och sårbarheter.
 - (c) Att, på begäran av en företrädare för CSIRT-nätverket som potentiellt berörs av en incident, utbyta och diskutera information om den incidenten och relaterade cyberhot, risker och sårbarheter.
 - (d) Att, på begäran av en företrädare för CSIRT-nätverket, diskutera och om möjligt genomföra en samordnad åtgärd till följd av en incident som har identifierats inom den medlemsstatens jurisdiktion.
 - (e) Att ge medlemsstaterna stöd när det gäller att hantera gränsöverskridande incidenter i enlighet med detta direktiv.
 - (f) Att samarbeta med och ge stöd till utsedda CSIRT-enheter som avses i artikel 6 när det gäller hanteringen av samordnad information från flera parter om sårbarheter som berör flera tillverkare eller leverantörer av IKT-produkter, IKT-tjänster och IKT-processer som är etablerade i olika medlemsstater.
 - (g) Att diskutera och identifiera ytterligare former av operativt samarbete, inbegripet när det gäller
 - i) kategorier av cyberhot och incidenter,
 - ii) tidiga varningar,
 - iii) ömsesidigt bistånd,
 - iv) principer och metoder för samordning i samband med åtgärder mot gränsöverskridande risker och incidenter,
 - v) bidrag till den nationella incident- och krishanteringsplan för cybersäkerhet som avses i artikel 7.3.
 - (h) Att informera samarbetsgruppen om sin verksamhet och om ytterligare former av operativt samarbete som diskuteras enligt led g och vid behov begära vägledning i sistnämnda avseende.
 - (i) Att utvärdera cybersäkerhetsövningar, bland annat sådana som anordnas av Enisa.
 - (j) Att på begäran av en enskild CSIRT-enhet diskutera den enhetens kapacitet och beredskap.

- (k) Att samarbeta och utbyta information med säkerhetscentrum (SOC) på regional nivå och unionsnivå, för att förbättra den gemensamma situationsmedvetenheten om incidenter och hot i hela unionen.
 - (l) Att diskutera de rapporter från sakkunnigbedömningar som avses i artikel 16.7.
 - (m) Att utfärda riktlinjer för att underlätta en mer enhetlig operativ praxis när det gäller tillämpningen av bestämmelserna i denna artikel om operativt samarbete.
4. I samband med den översyn som avses i artikel 35 ska CSIRT-nätverket, inom [24 månader efter dagen för detta direktivs ikraftträdande] och därefter vartannat år, bedöma de framsteg som gjorts med det operativa samarbetet och utarbeta en rapport. Rapporten ska särskilt innehålla slutsatser om resultaten av de sakkunnigbedömningar som avses i artikel 16 och som utförts med avseende på nationella CSIRT-enheter, inbegripet slutsatser och rekommendationer i enlighet med den artikeln. Rapporten ska även lämnas till samarbetsgruppen.
 5. CSIRT-nätverket ska anta sin arbetsordning.

Artikel 14

Det europeiska kontaktnätverket för cyberkriser (EU-CyCLONe)

1. För att stödja en samordnad hantering av storskaliga cyberincidenter och cyberkriser på operativ nivå och säkerställa ett regelbundet informationsutbyte mellan medlemsstaterna och unionens institutioner, organ och byråer inrättas härmed Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe).
2. EU-CyCLONe ska bestå av de företrädare för medlemsstaternas krishanteringsmyndigheter som utsetts i enlighet med artikel 7, kommissionen och Enisa. Enisa ska tillhandahålla nätverkets sekretariat och stödja ett säkert informationsutbyte.
3. EU-CyCLONe ska ha följande uppgifter:
 - a) Att öka beredskapen för hantering av storskaliga incidenter och kriser.
 - b) Att utveckla en gemensam situationsmedvetenhet om relevanta händelser som rör cybersäkerhet.
 - c) Att samordna hanteringen av storskaliga incidenter och kriser och ge stöd till beslutsfattande på politisk nivå i samband med sådana incidenter och kriser.
 - d) Att diskutera de nationella incident- och krishanteringsplaner för cybersäkerhet som avses i artikel 7.3.
4. EU-CyCLONe ska anta sin arbetsordning.
5. EU-CyCLONe ska regelbundet rapportera till samarbetsgruppen om cyberhot, incidenter och trender, med särskild inriktning på deras inverkan på väsentliga och viktiga entiteter.
6. EU-CyCLONe ska samarbeta med CSIRT-nätverket på grundval av överenskomna förfaranden.

Artikel 15

Rapport om cybersäkerhetssituationen i unionen

1. Enisa ska, i samarbete med kommissionen, vartannat år utfärda en rapport om cybersäkerhetssituationen i unionen. Rapporten ska särskilt innehålla en bedömning av följande:
 - (a) Utvecklingen av cybersäkerhetskapaleten i hela unionen.
 - (b) De tekniska, ekonomiska och mänskliga resurser som är tillgängliga för de behöriga myndigheterna och cybersäkerhetspolitiken samt genomförandet av tillsynsåtgärder och efterlevnadskontroll mot bakgrund av resultaten av de sakkunnigbedömningar som avses i artikel 16.
 - (c) Ett cybersäkerhetsindex som möjliggör en aggregerad bedömning av nivån på cybersäkerhetskapaleten.
2. Rapporten ska innehålla särskilda politiska rekommendationer för att höja cybersäkerhetsnivån i hela unionen och en sammanfattning av resultaten för den aktuella perioden från de tekniska lägesrapporter om cybersäkerhet i EU som Enisa utfärdat i enlighet med artikel 7.6 i förordning (EU) 2019/881.

Artikel 16

Sakkunnigbedömningar

1. Kommissionen ska, efter samråd med samarbetsgruppen och Enisa och senast 18 månader efter det att detta direktiv har trätt i kraft, fastställa metoden för och innehållet i ett system för sakkunnigbedömningar som utvärderar hur ändamålsenlig medlemsstaternas cybersäkerhetspolitik är. Bedömningarna ska utföras av tekniska experter för cybersäkerhet från andra medlemsstater än den granskade och ska omfatta åtminstone följande:
 - i) Ändamålsenligheten hos genomförandet av de riskhanteringsåtgärder för cybersäkerhet och rapporteringsskyldigheter som avses i artiklarna 18 och 20.
 - ii) Kapacitetsnivån, inbegripet tillgängliga ekonomiska, tekniska och mänskliga resurser, och effektiviteten i de nationella behöriga myndigheternas arbete.
 - iii) CSIRT-enheternas operativa kapacitet och effektivitet.
 - iv) Effektiviteten i det ömsesidiga bistånd som avses i artikel 34.
 - v) Effektiviteten i den ram för informationsutbyte som avses i artikel 26 i detta direktiv.
2. Metoden ska innefatta objektiva, icke-diskriminerande, rättvisa och transparenta kriterier på grundval av vilka medlemsstaterna ska utse experter som ska få utföra sakkunnigbedömningarna. Enisa och kommissionen ska utse experter som ska delta som observatörer i sakkunnigbedömningarna. Kommissionen ska, med stöd av Enisa och inom ramen för den metod som avses i punkt 1, fastställa ett objektivt, icke-diskriminerande, rättvist och transparent system för urval och slumpvis tilldelning av experter för varje sakkunnigbedömning.
3. De organisatoriska aspekterna av sakkunnigbedömningarna ska fastställas av kommissionen, med stöd av Enisa, och ska, efter samråd med samarbetsgruppen,

baseras på kriterier som fastställs inom ramen för den metod som avses i punkt 1. Sakkunnigbedömningarna ska utvärdera de aspekter som avses i punkt 1 för alla medlemsstater och sektorer, inbegripet riktade frågor som är specifika för en eller flera medlemsstater eller en eller flera sektorer.

4. Sakkunnigbedömningar ska inbegripa faktiska eller virtuella besök på plats och distansbaserade utbyten. Med hänsyn till principen om gott samarbete ska de medlemsstater som granskas förse de utsedda experterna med den begärda information som krävs för de aspekter som granskas. All information som erhålls genom en sakkunnigbedömning får endast användas för dess ändamål. De experter som deltar i sakkunnigbedömningen får inte lämna ut känslig eller konfidentiell information som erhållits under denna bedömning till någon tredje part.
5. När aspekter har granskats i en medlemsstat ska de inte bli föremål för ytterligare sakkunnigbedömning i den medlemsstaten under de två år som följer på slutförandet av en sakkunnigbedömning, om inte annat beslutas av kommissionen efter samråd med Enisa och samarbetsgruppen.
6. Medlemsstaterna ska se till att de andra medlemsstaterna, kommissionen och Enisa utan onödigt dröjsmål får information om alla risker för intressekonflikter som rör utsedda experter.
7. Experter som deltar i sakkunnigbedömningar ska utarbeta rapporter om resultat och slutsatser av dessa. Rapporterna ska lämnas till kommissionen, samarbetsgruppen, CSIRT-nätverket och Enisa. Rapporterna ska diskuteras i samarbetsgruppen och CSIRT-nätverket. Rapporterna får offentliggöras på samarbetsgruppens särskilda webbplats.

KAPITEL IV

Riskhanterings- och rapporteringskrav för cybersäkerhet

AVSNITT I

Riskhantering och rapportering i fråga om cybersäkerhet

Artikel 17

Styrning

1. Medlemsstaterna ska säkerställa att väsentliga och viktiga entiteters ledningsorgan godkänner de riskhanteringsåtgärder för cybersäkerhet som dessa entiteter vidtar för att följa artikel 18, övervakar genomförandet av dem och står till svars om entiteterna inte fullgör sina skyldigheter enligt den artikeln.
2. Medlemsstaterna ska säkerställa att ledningsorganens medlemmar regelbundet genomgår särskild utbildning för att skaffa sig tillräckliga kunskaper och kompetenser så att de förstår och kan bedöma cybersäkerhetsrisker och praxis för hantering av cybersäkerhet och deras inverkan på entitetens verksamhet.

Artikel 18

Riskhanteringsåtgärder för cybersäkerhet

1. Medlemsstaterna ska säkerställa att väsentliga och viktiga entiteter vidtar lämpliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder för att tillhandahålla sina tjänster. Med beaktande av den senaste tekniska utvecklingen ska dessa åtgärder säkerställa en säkerhetsnivå i nätverks- och informationssystem som är lämplig i förhållande till den föreliggande risken.
2. De åtgärder som avses i punkt 1 ska åtminstone inbegripa
 - (a) strategier för riskanalys och informationssystemens säkerhet,
 - (b) incidenthantering (förebyggande, upptäckt och åtgärder till följd av incidenter),
 - (c) driftskontinuitet och krishantering,
 - (d) säkerhet i leveranskedjan, inbegripet säkerhetsaspekter som rör förbindelserna mellan varje entitet och dess leverantörer eller tjänsteleverantörer, såsom leverantörer av datalagrings- och databehandlingstjänster eller hanterade säkerhetstjänster,
 - (e) säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem, inbegripet hantering av och information om sårbarheter,
 - (f) strategier och förfaranden (testning och revision) för att bedöma effektiviteten i riskhanteringsåtgärderna för cybersäkerhet,
 - (g) användning av kryptografi och kryptering.
3. Medlemsstaterna ska säkerställa att entiteter, när de överväger de lämpliga åtgärder som avses i punkt 2 d, beaktar de sårbarheter som är specifika för varje leverantör och tjänsteleverantör och den övergripande kvaliteten på deras leverantörers produkter och cybersäkerhetspraxis, inbegripet deras förfaranden för säker utveckling.
4. Medlemsstaterna ska säkerställa att om en entitet finner att dess tjänster eller uppgifter inte uppfyller kraven i punkt 2, ska den utan onödigt dröjsmål vidta alla nödvändiga korrigerande åtgärder för att den berörda tjänsten ska uppfylla kraven.
5. Kommissionen får anta genomförandeakter för att fastställa de tekniska och metodologiska specifikationerna för de aspekter som avses i punkt 2. När kommissionen utarbetar dessa akter ska den följa det granskningsförfarande som avses i artikel 37.2 och i största möjliga utsträckning följa internationella och europeiska standarder samt relevanta tekniska specifikationer.
6. Kommissionen ska ges befogenhet att anta delegerade akter i enlighet med artikel 36 för att komplettera de aspekter som anges i punkt 2 med hänsyn till nya cyberhot, teknisk utveckling eller sektorsspecifika särdrag.

Artikel 19

EU-samordnade riskbedömningar av kritiska leveranskedjor

1. Samarbetsgruppen får, i samarbete med kommissionen och Enisa, utföra samordnade säkerhetsriskbedömningar av specifika kritiska leveranskedjor för IKT-tjänster, IKT-system eller IKT-produkter, med beaktande av tekniska och, i relevanta fall, icke-tekniska riskfaktorer.
2. Kommissionen ska, efter samråd med samarbetsgruppen och Enisa, identifiera de specifika kritiska IKT-tjänster, IKT-system eller IKT-produkter som kan bli föremål för den samordnade riskbedömning som avses i punkt 1.

Artikel 20

Rapporteringsskyldigheter

1. Medlemsstaterna ska säkerställa att väsentliga och viktiga entiteter utan onödigt dröjsmål underrättar de behöriga myndigheterna eller CSIRT-enheten i enlighet med punkterna 3 och 4 om alla incidenter som har en betydande inverkan på tillhandahållandet av deras tjänster. När så är lämpligt ska dessa entiteter utan onödigt dröjsmål underrätta mottagarna av deras tjänster om incidenter som sannolikt inverkar negativt på tillhandahållandet av de berörda tjänsterna. Medlemsstaterna ska säkerställa att dessa entiteter bland annat rapporterar information som gör det möjligt för de behöriga myndigheterna eller CSIRT-enheten att fastställa incidentens eventuella gränsöverskridande verkningar.
2. Medlemsstaterna ska säkerställa att väsentliga och viktiga entiteter utan onödigt dröjsmål underrättar de behöriga myndigheterna eller CSIRT-enheten om alla betydande cyberhot som dessa entiteter identifierar och som potentiellt skulle ha kunnat leda till en betydande incident.

I tillämpliga fall ska dessa entiteter utan onödigt dröjsmål underrätta de mottagare av deras tjänster som kan påverkas av ett betydande cyberhot om eventuella åtgärder eller avhjälpande arrangemang som dessa mottagare kan vidta som svar på hotet. När så är lämpligt ska entiteterna också underrätta dessa mottagare om själva hotet. En underrättelse ska inte medföra ökat ansvar för den underrättande entiteten.
3. En incident ska anses vara betydande om
 - (a) den har orsakat eller kan orsaka betydande driftsstörningar eller ekonomiska förluster för den berörda entiteten,
 - (b) den har påverkat eller kan påverka andra fysiska eller juridiska personer genom att vålla betydande materiella eller immateriella förluster.
4. När det gäller det underrättelseförfarande som avses i punkt 1 ska medlemsstaterna se till att de berörda entiteterna lämnar följande till de behöriga myndigheterna eller CSIRT-enheten:
 - (a) Utan onödigt dröjsmål och under alla omständigheter inom 24 timmar efter att ha fått kännedom om incidenten, en första underrättelse där det i tillämpliga fall ska anges om incidenten antas ha orsakats av olagliga eller avsiktligt skadliga handlingar.

- (b) På begäran av en behörig myndighet eller en CSIRT-enhet, en delrapport om relevanta statusuppdateringar.
- (c) Senast en månad efter inlämningen av den underrättelse som avses i led a, en slutrapport som minst ska innehålla följande:
 - i) En detaljerad beskrivning av incidenten, dess allvarlighetsgrad och dess konsekvenser.
 - ii) Den typ av hot eller grundorsak som sannolikt utlöst incidenten.
 - iii) Tillämpade och pågående avhjälpande åtgärder.

Medlemsstaterna ska föreskriva att den berörda entiteten i vederbörligen motiverade fall och i samförstånd med de behöriga myndigheterna eller CSIRT-enheten får frånga de tidsfrister som anges i leden a och c.

5. De behöriga nationella myndigheterna eller CSIRT-enheten ska inom 24 timmar efter mottagandet av den första underrättelse som avses i punkt 4 a lämna ett svar till den underrättande entiteten, inbegripet initial återkoppling om incidenten och, på entitetens begäran, vägledning om genomförandet av möjliga avhjälpande åtgärder. Om CSIRT-enheten inte har mottagit den underrättelse som avses i punkt 1 ska vägledningen tillhandahållas av den behöriga myndigheten i samarbete med CSIRT-enheten. CSIRT-enheten ska tillhandahålla ytterligare tekniskt stöd om den berörda entiteten begär det. Om incidenten misstänks vara av brottslig art ska de behöriga nationella myndigheterna eller CSIRT-enheten också tillhandahålla vägledning om rapportering av incidenten till brottsbekämpande myndigheter.
6. När så är lämpligt, och särskilt om den incident som avses i punkt 1 berör två eller flera medlemsstater, ska den behöriga myndigheten eller CSIRT-enheten informera andra berörda medlemsstater och Enisa om incidenten. Därvid ska de behöriga myndigheterna, CSIRT-enheter och gemensamma kontaktpunkter, i enlighet med unionsrätten eller nationell lagstiftning som är förenlig med unionsrätten, bevara entitetens säkerhets- och affärsintressen samt den tillhandahållna informationens konfidentialitet.
7. Om allmänhetens medvetenhet är nödvändig för att förhindra en incident eller för att hantera en pågående incident, eller om information om incidenten på annat sätt ligger i allmänhetens intresse, får den behöriga myndigheten eller CSIRT-enheten och, om det är lämpligt, myndigheterna eller CSIRT-enheterna i andra berörda medlemsstater, efter samråd med den berörda entiteten, informera allmänheten om incidenten eller kräva att entiteten gör det.
8. På begäran av den behöriga myndigheten eller CSIRT-enheten ska den gemensamma kontaktpunkten vidarebefordra underrättelser som mottagits i enlighet med punkterna 1 och 2 till de gemensamma kontaktpunkterna i andra berörda medlemsstater.
9. Den gemensamma kontaktpunkten ska varje månad lämna in en sammanfattande rapport till Enisa med anonymiserade och aggregerade uppgifter om incidenter, betydande cyberhot och tillbud som underrättats i enlighet med punkterna 1 och 2 och i enlighet med artikel 27. För att bidra till att jämförbar information lämnas får Enisa utfärda teknisk vägledning om parametrarna för den information som tas med i den sammanfattande rapporten.
10. De behöriga myndigheterna ska förse de behöriga myndigheter som utsetts i enlighet med direktiv (EU) XXXX/XXXX [direktivet om kritiska entiteters motståndskraft] med information om incidenter och cyberhot som underrättats i enlighet med

punkterna 1 och 2 av väsentliga entiteter som identifierats som kritiska eller som likvärdiga med kritiska entiteter, i enlighet med direktiv (EU) XXXX/XXXX [direktivet om kritiska entiteters motståndskraft].

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

Artikel 21

Användning av europeiska ordningar för cybersäkerhetscertifiering

1. För kontroll av att vissa krav enligt artikel 18 är uppfyllda får medlemsstaterna kräva att väsentliga och viktiga entiteter certifierar vissa IKT-produkter, IKT-tjänster och IKT-processer enligt särskilda europeiska ordningar för cybersäkerhetscertifiering som antagits i enlighet med artikel 49 i förordning (EU) 2019/881. De produkter, tjänster och processer som är föremål för certifiering kan utvecklas av en väsentlig eller viktig entitet eller upphandlas från tredje part.
2. Kommissionen ska ges befogenhet att anta delegerade akter som anger vilka kategorier av väsentliga entiteter som ska vara skyldiga att erhålla ett certifikat och enligt vilka specifika europeiska ordningar för cybersäkerhetscertifiering enligt punkt 1 som detta ska ske. Dessa delegerade akter ska antas i enlighet med artikel 36.
3. Kommissionen kan begära att Enisa utarbetar ett förslag till certifieringsordning i enlighet med artikel 48.2 i förordning (EU) 2019/881 i fall där det inte finns någon lämplig europeisk ordning för cybersäkerhetscertifiering för tillämpningen av punkt 2.

Artikel 22

Standardisering

1. För att främja en enhetlig tillämpning av artikel 18.1 och 18.2 ska medlemsstaterna, utan att föreskriva eller gynna användning av en viss typ av teknik, uppmuntra användningen av europeiska eller internationellt accepterade standarder och specifikationer av relevans för säkerheten i nätverks- och informationssystem.
2. Enisa ska i samarbete med medlemsstaterna utarbeta råd och riktlinjer för de tekniska områden som ska beaktas när det gäller punkt 1 samt för redan befintliga standarder, inklusive medlemsstaternas nationella standarder, som skulle kunna täcka dessa områden.

Artikel 23

Databaser över domännamn och registreringsuppgifter

1. För att bidra till säkerheten, stabiliteten och motståndskraften hos domännamnssystemet ska medlemsstaterna säkerställa att registreringsenheter för toppdomäner och de enheter som tillhandahåller domännamnsregistreringstjänster för toppdomäner samlar in och upprätthåller korrekta och fullständiga registreringsuppgifter för domännamn i en särskild databas med tillbörlig aktsamhet i enlighet med unionens dataskyddslagstiftning när det gäller personuppgifter.
2. Medlemsstaterna ska se till att de databaser med registreringsuppgifter för domännamn som avses i punkt 1 innehåller relevant information för att identifiera och kontakta innehavarna av domännamnen och de kontaktpunkter som administrerar domännamnen under toppdomänerna.
3. Medlemsstaterna ska se till att registreringsenheter för toppdomäner och de enheter som tillhandahåller domännamnsregistreringstjänster för toppdomäner har strategier och förfaranden för att säkerställa att databaserna innehåller korrekt och fullständig information. Medlemsstaterna ska se till att sådana strategier och förfaranden offentliggörs.
4. Medlemsstaterna ska se till att registreringsenheter för toppdomäner och de enheter som tillhandahåller domännamnsregistreringstjänster för toppdomäner utan onödigt dröjsmål efter registreringen av ett domännamn offentliggör domänregistreringsuppgifter som inte är personuppgifter.
5. Medlemsstaterna ska se till att registreringsenheter för toppdomäner och de enheter som tillhandahåller domännamnsregistreringstjänster för toppdomäner ger åtkomst till specifika registreringsuppgifter för domännamn på lagliga och vederbörligen motiverade begäranden från legitima åtkomstsökande, i enlighet med unionens dataskyddslagstiftning. Medlemsstaterna ska se till att registreringsenheter för toppdomäner och de enheter som tillhandahåller domännamnsregistreringstjänster för toppdomäner utan onödigt dröjsmål besvarar alla begäranden om åtkomst. Medlemsstaterna ska se till att strategier och förfaranden för utlämning av sådana uppgifter offentliggörs.

Avsnitt II

Jurisdiktion och registrering

Artikel 24

Jurisdiktion och territorialitet

1. Leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster och leverantörer av nätverk för innehållsleverans som avses i punkt 8 i bilaga I samt digitala leverantörer som avses i punkt 6 i bilaga II ska anses omfattas av jurisdiktionen i den medlemsstat där de har sitt huvudsakliga etableringsställe i unionen.
2. Vid tillämpning av detta direktiv ska entiteter som avses i punkt 1 anses ha sitt huvudsakliga etableringsställe i unionen i den medlemsstat där besluten om riskhanteringsåtgärder för cybersäkerhet fattas. Om sådana beslut inte fattas vid något etableringsställe i unionen ska det huvudsakliga etableringsstället anses vara beläget i den medlemsstat där entiteterna har det etableringsställe som har flest anställda i unionen.

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

Artikel 25

Register över väsentliga och viktiga entiteter

1. Enisa ska skapa och upprätthålla ett register över de väsentliga och viktiga entiteter som avses i artikel 24.1. Entiteterna ska lämna följande uppgifter till Enisa senast [12 månader efter direktivets ikraftträdande]:
 - (a) Entitetens namn.
 - (b) Adressen till entitetens huvudsakliga etableringsställe och andra rättsligt giltiga etableringsställen i unionen eller, om entiteten inte är etablerad i unionen, till dess företrädare som utsetts i enlighet med artikel 24.3.
 - (c) Aktuella kontaktuppgifter, inklusive e-postadresser och telefonnummer till entiteten.
2. De entiteter som avses i punkt 1 ska underrätta Enisa om alla ändringar av de uppgifter som de lämnat enligt punkt 1 utan dröjsmål och under alla omständigheter inom tre månader från den dag då ändringen fått verkan.
3. När uppgifterna enligt punkt 1 inkommit ska Enisa vidarebefordra dem till de gemensamma kontaktpunkterna beroende på den angivna platsen för varje entitets huvudsakliga etableringsställe eller, om entiteten inte är etablerad i unionen, för dess utsedda företrädare. Om en entitet som avses i punkt 1 utöver sitt huvudsakliga etableringsställe i unionen har ytterligare etableringsställen i andra medlemsstater ska Enisa också informera de gemensamma kontaktpunkterna i dessa medlemsstater.
4. Om en entitet underlåter att registrera sin verksamhet eller lämna relevanta uppgifter inom den tidsfrist som anges i punkt 1, ska varje medlemsstat där entiteten tillhandahåller tjänster vara behörig att säkerställa att entiteten fullgör de skyldigheter som fastställs i detta direktiv.

KAPITEL V

Informationsutbyte

Artikel 26

Arrangemang för informationsutbyte om cybersäkerhet

1. Utan att det påverkar tillämpningen av förordning (EU) 2016/679 ska medlemsstaterna säkerställa att väsentliga och viktiga entiteter får utbyta relevant information om cybersäkerhet sinsemellan, inbegripet information om cyberhot, sårbarheter, angreppsindikatorer, taktik, tekniker och förfaranden, cybersäkerhetsvarningar och konfigurationsverktyg, om sådant informationsutbyte
 - (a) syftar till att förebygga, upptäcka, reagera på eller begränsa incidenter,
 - (b) höjer cybersäkerhetsnivån, särskilt genom att öka medvetenheten om cyberhot, begränsa eller hindra sådana hots spridningsförmåga eller stödja en rad defensiva förmågor, avhjälpande av och information om sårbarheter, metoder för att upptäcka hot, strategier för begränsning av hot eller reaktions- och återhämtningsfaser.
2. Medlemsstaterna ska se till att informationsutbytet sker inom betrodda grupper av väsentliga och viktiga entiteter. Sådant utbyte ska genomföras med hjälp av arrangemang för informationsutbyte med hänsyn till den potentiellt känsliga karaktären hos den information som utbyts och i enlighet med de unionsrättsliga bestämmelser som avses i punkt 1.
3. Medlemsstaterna ska fastställa regler som anger förfarandet för, de operativa aspekterna av (inbegripet användning av särskilda IKT-plattformar), innehållet i och villkoren för de arrangemang för informationsutbyte som avses i punkt 2. Sådana regler ska också fastställa närmare bestämmelser om offentliga myndigheters deltagande i sådana arrangemang, liksom operativa aspekter, inbegripet användning av särskilda it-plattformar. Medlemsstaterna ska erbjuda stöd för tillämpningen av sådana arrangemang i enlighet med den politik som avses i artikel 5.2 g.
4. Väsentliga och viktiga entiteter ska underrätta de behöriga myndigheterna om sitt deltagande i de arrangemang för informationsutbyte som avses i punkt 2, när de ingår sådana arrangemang eller, om de utträder ur sådana arrangemang, när utträdet får verkan.
5. I enlighet med unionsrätten ska Enisa stödja inrättandet av de arrangemang för informationsutbyte om cybersäkerhet som avses i punkt 2 genom att tillhandahålla bästa praxis och vägledning.

Artikel 27

Frivillig underrättelse om relevant information

Utan att det påverkar tillämpningen av artikel 3 ska medlemsstaterna säkerställa att entiteter som inte ingår i detta direktivs tillämpningsområde på frivillig basis kan lämna in underrättelser om betydande incidenter, cyberhot eller tillbud. Vid behandlingen av underrättelserna ska medlemsstaterna agera i enlighet med det förfarande som anges i artikel 20. Medlemsstaterna får ge behandling av obligatoriska underrättelser företräde framför behandling av frivilliga underrättelser. En frivillig rapportering får inte leda till att den rapporterade entiteten åläggs ytterligare skyldigheter som den inte skulle ha blivit föremål för om den inte hade lämnat in underrättelser.

KAPITEL VI

Tillsyn och efterlevnadskontroll

Artikel 28

Allmänna aspekter på tillsyn och efterlevnadskontroll

1. Medlemsstaterna ska se till att de behöriga myndigheterna på ett ändamålsenligt sätt övervakar och vidtar de åtgärder som krävs för att säkerställa att detta direktiv efterlevs, särskilt de skyldigheter som anges i artiklarna 18 och 20.
2. De behöriga myndigheterna ska ha ett nära samarbete med dataskyddsmyndigheter när de behandlar incidenter som medför personuppgiftsincidenter.

Artikel 29

Tillsyn och efterlevnadskontroll i fråga om väsentliga entiteter

1. Medlemsstaterna ska se till att de tillsyns- eller efterlevnadskontrollåtgärder som åläggs väsentliga entiteter angående de skyldigheter som anges i detta direktiv är effektiva, proportionella och avskräckande, med beaktande av omständigheterna i varje enskilt fall.
2. Medlemsstaterna ska se till att behöriga myndigheter, när de utövar sina tillsynsuppgifter avseende väsentliga entiteter, har befogenhet att underställa dessa entiteter
 - a) inspektioner på plats och distansbaserad tillsyn, inklusive slumpvisa kontroller,
 - b) regelbundna revisioner,
 - c) riktade säkerhetsrevisioner baserade på riskbedömningar eller tillgänglig riskrelaterad information,
 - d) säkerhetsskanningar på grundval av objektiva, icke-diskriminerande, rättvisa och transparenta riskbedömningskriterier,
 - e) begäranden om information som behövs för att bedöma de cybersäkerhetsåtgärder som antagits av entiteten, inbegripet dokumenterade cybersäkerhetsstrategier, samt fullgörandet av skyldigheten att underrätta Enisa i enlighet med artikel 25.1 och 25.2,
 - f) begäranden om tillgång till uppgifter, handlingar eller annan information som behövs för att de ska kunna utföra sina tillsynsuppgifter,
 - g) begäranden om bevis på genomförandet av cybersäkerhetsstrategier, t.ex. resultaten av säkerhetsrevisioner som utförts av en kvalificerad revisor och respektive underliggande bevis.
3. När de behöriga myndigheterna utövar sina befogenheter enligt punkt 2 e–g ska de ange syftet med en begäran och specificera den begärda informationen.
4. Medlemsstaterna ska se till att behöriga myndigheter, när de kontrollerar väsentliga entiteters efterlevnad, har befogenhet att
 - (a) utfärda varningar om entiteters bristande fullgörande av de skyldigheter som fastställs i detta direktiv,

- (b) utfärda bindande instruktioner eller ett föreläggande om att dessa entiteter ska avhjälpa konstaterade brister eller överträdelser av de skyldigheter som fastställs i detta direktiv,
- (c) ålägga dessa entiteter att upphöra med beteenden som inte överensstämmer med de skyldigheter som fastställs i detta direktiv och att avstå från att upprepa sådana beteenden,
- (d) ålägga dessa entiteter att se till att deras riskhanteringsåtgärder och/eller rapporteringsskyldigheter överensstämmer med de skyldigheter som fastställs i artiklarna 18 och 20, på det sätt som specificeras och inom en angiven tidsperiod,
- (e) ålägga dessa entiteter att informera den eller de fysiska eller juridiska personer till vilka de tillhandahåller tjänster eller verksamheter som potentiellt kan beröras av ett betydande cyberhot om eventuella skyddsåtgärder eller avhjälpande åtgärder som dessa fysiska eller juridiska personer kan vidta som svar på hotet,
- (f) ålägga dessa entiteter att inom en rimlig tidsfrist genomföra de rekommendationer som lämnats till följd av en säkerhetsrevision,
- (g) utse en övervakningsansvarig med väldefinierade uppgifter under en fastställd tidsperiod för att övervaka att entiteter fullgör sina skyldigheter enligt artiklarna 18 och 20,
- (h) ålägga dessa entiteter att offentliggöra aspekter av bristande fullgörande av de skyldigheter som fastställs i detta direktiv på ett specificerat sätt,
- (i) göra ett offentligt uttalande som identifierar den eller de juridiska och fysiska personer som är ansvariga för överträdelsen av en skyldighet som fastställs i detta direktiv och överträdelsens art,
- (j) påföra eller begära att relevanta organ eller domstolar i enlighet med nationell lagstiftning påför administrativa sanktionsavgifter enligt artikel 31 utöver eller i stället för de åtgärder som avses i leden a–i i denna punkt, beroende på omständigheterna i varje enskilt fall.

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

- (a) tillfälligt upphäva eller begära att ett certifierings- eller auktorisationsorgan tillfälligt upphäver en certifiering eller auktorisation för en del av eller alla tjänster eller verksamheter som tillhandahålls av en väsentlig entitet,
- (b) införa eller begära att relevanta organ eller domstolar i enlighet med nationell lagstiftning inför ett tillfälligt förbud för personer som på nivån för verkställande direktör eller juridiskt ombud har ledningsansvar i den väsentliga entiteten och alla andra fysiska personer som hålls ansvariga för överträdelsen att utöva ledningsfunktioner i den entiteten.

Dessa sanktioner ska endast tillämpas till dess att entiteten vidtar nödvändiga åtgärder för att avhjälpa bristerna eller uppfylla de krav från den behöriga myndigheten som gav upphov till sanktionerna.

6. Medlemsstaterna ska se till att varje fysisk person som ansvarar för eller agerar som företrädare för en väsentlig entitet har befogenhet att säkerställa att entiteten fullgör de skyldigheter som fastställs i detta direktiv, på grundval av en befogenhet att företräda entiteten, att fatta beslut på dess vägnar eller att utöva kontroll över entiteten. Medlemsstaterna ska se till att dessa fysiska personer kan hållas ansvariga för överträdelser av sitt uppdrag att säkerställa att de skyldigheter som fastställs i detta direktiv fullgörs.
7. När de behöriga myndigheterna tillämpar efterlevnadskontrollåtgärder eller sanktioner i enlighet med punkterna 4 och 5 ska de iaktta rätten till försvar och ta hänsyn till omständigheterna i varje enskilt fall och som ett minimum ta vederbörlig hänsyn till följande:
 - (a) Överträdelsens svårighetsgrad och de överträdde bestämmelsernas betydelse. Som överträdelser som bör betraktas som allvarliga kan nämnas upprepade överträdelser, underlåtenhet att underrätta eller avhjälpa incidenter med betydande störande effekt, underlåtenhet att avhjälpa brister enligt bindande instruktioner från behöriga myndigheter, hindrande av revisioner eller övervakningsverksamhet som den behöriga myndigheten beordrat efter det att en överträdelse konstaterats och tillhandahållande av falsk eller grovt felaktig information i fråga om riskhanteringskrav eller rapporteringsskyldigheter enligt artiklarna 18 och 20.
 - (b) Överträdelsens varaktighet, inbegripet upprepade överträdelser.
 - (c) De faktiska skador eller förluster som uppstått eller potentiella skador eller förluster som skulle ha kunnat orsakats, i den mån de kan fastställas. Vid bedömningen av denna aspekt ska hänsyn bland annat tas till faktiska eller potentiella finansiella eller ekonomiska förluster, effekter på andra tjänster och det antal användare som berörs eller kan bli berörda.
 - (d) Om överträdelsen skett med uppsåt eller genom oaktsamhet.
 - (e) De åtgärder som entiteten vidtagit för att förhindra eller minska skadan och/eller förlusterna.
 - (f) Efterlevnad av godkända uppförandekoder eller godkända certifieringsmekanismer.
 - (g) Huruvida den eller de fysiska eller juridiska personer som hålls ansvariga samarbetar med de behöriga myndigheterna.
8. De behöriga myndigheterna ska utförligt motivera sina beslut angående efterlevnadskontroll. Innan sådana beslut fattas ska de behöriga myndigheterna underrätta de berörda entiteterna om sina preliminära slutsatser och ge dessa entiteter en rimlig tidsfrist för att lämna synpunkter.
9. Medlemsstaterna ska se till att deras behöriga myndigheter informerar de relevanta behöriga myndigheter i den berörda medlemsstaten som utsetts i enlighet med direktiv (EU) XXXX/XXXX [direktivet om kritiska entiteters motståndskraft] när de utövar sina tillsyns- och efterlevnadskontrollbefogenheter för att säkerställa att en väsentlig entitet som identifierats som kritisk eller som likvärdig med en kritisk entitet i enlighet med direktiv (EU) XXXX/XXXX [direktivet om kritiska entiteters

motståndskraft] fullgör skyldigheter enligt detta direktiv. På begäran av behöriga myndigheter enligt direktiv (EU) XXXX/XXXX [direktivet om kritiska entiteters motståndskraft] får de behöriga myndigheterna utöva sina tillsyns- och efterlevnadskontrollbefogenheter avseende en väsentlig entitet som identifierats som kritisk eller som likvärdig med en kritisk entitet.

Artikel 30

Tillsyn och efterlevnadskontroll i fråga om viktiga entiteter

1. När medlemsstaterna får bevis eller indikationer på att en viktig entitet inte fullgör de skyldigheter som fastställs i detta direktiv, särskilt artiklarna 18 och 20, ska de se till att de behöriga myndigheterna vid behov vidtar åtgärder i form av tillsynsåtgärder i efterhand.
2. Medlemsstaterna ska se till att de behöriga myndigheterna, när de utövar sina tillsynsuppgifter avseende viktiga entiteter, har befogenhet att underställa dessa entiteter
 - (a) inspektioner på plats och distansbaserad tillsyn i efterhand,
 - (b) riktade säkerhetsrevisioner baserade på riskbedömningar eller tillgänglig riskrelaterad information,
 - (c) säkerhetsskanningar på grundval av objektiva, rättvisa och transparenta riskbedömningskriterier,
 - (d) begäranden om all information som behövs för att i efterhand bedöma cybersäkerhetsåtgärder, inbegripet dokumenterade cybersäkerhetsstrategier, samt fullgörandet av skyldigheten att underrätta Enisa i enlighet med artikel 25.1 och 25.2,
 - (e) begäranden om tillgång till uppgifter, handlingar och/eller information som behövs för utförandet av tillsynsuppgifter.
3. När de behöriga myndigheterna utövar sina befogenheter i enlighet med punkt 2 d eller e ska de ange syftet med begäran och specificera vilken information som begärs.
4. Medlemsstaterna ska se till att de behöriga myndigheterna, när de kontrollerar viktiga entiteters efterlevnad, har befogenhet att
 - (a) utfärda varningar om entiteters bristande fullgörande av de skyldigheter som fastställs i detta direktiv,
 - (b) utfärda bindande instruktioner eller ett föreläggande om att dessa entiteter ska avhjälpa konstaterade brister eller överträdelser av de skyldigheter som fastställs i detta direktiv,
 - (c) ålägga dessa entiteter att upphöra med beteenden som inte överensstämmer med de skyldigheter som fastställs i detta direktiv och att avstå från att upprepa sådana beteenden,
 - (d) ålägga dessa entiteter att se till att deras riskhanteringsåtgärder eller rapporteringsskyldigheter överensstämmer med de skyldigheter som fastställs i artiklarna 18 och 20, på det sätt som specificeras och inom en angiven tidsperiod,

- (e) ålägga dessa entiteter att informera den eller de fysiska eller juridiska personer till vilka de tillhandahåller tjänster eller verksamheter som potentiellt kan beröras av ett betydande cyberhot om eventuella skyddsåtgärder eller avhjälpande åtgärder som dessa fysiska eller juridiska personer kan vidta som svar på hotet,
 - (f) ålägga dessa entiteter att inom en rimlig tidsfrist genomföra de rekommendationer som lämnats till följd av en säkerhetsrevision,
 - (g) ålägga dessa entiteter att offentliggöra aspekter av bristande fullgörande av de skyldigheter som fastställs i detta direktiv på ett specificerat sätt,
 - (h) göra ett offentligt uttalande som identifierar den eller de juridiska och fysiska personer som är ansvariga för överträdelsen av en skyldighet som fastställs i detta direktiv och överträdelsens art,
 - (i) påföra eller begära att relevanta organ eller domstolar i enlighet med nationell lagstiftning påför administrativa sanktionsavgifter enligt artikel 31 utöver eller i stället för de åtgärder som avses i leden a–h i denna punkt, beroende på omständigheterna i varje enskilt fall.
5. Artikel 29.6–29.8 ska också tillämpas på de tillsyns- och efterlevnadskontrollåtgärder som föreskrivs i denna artikel för de viktiga entiteter som förtecknas i bilaga II.

Artikel 31

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

1. Medlemsstaterna ska se till att de administrativa sanktionsavgifter som påförs väsentliga och viktiga entiteter i enlighet med denna artikel för överträdelser av de skyldigheter som fastställs i detta direktiv i varje enskilt fall är effektiva, proportionella och avskräckande.
2. Administrativa sanktionsavgifter ska, beroende på omständigheterna i varje enskilt fall, påföras utöver eller i stället för de åtgärder som avses i artikel 29.4 a–i, artikel 29.5 och artikel 30.4 a–h.
3. När beslut fattas om huruvida administrativa sanktionsavgifter ska påföras och om avgiftsbeloppet ska i varje enskilt fall vederbörlig hänsyn tas till åtminstone de faktorer som anges i artikel 29.7.
4. Medlemsstaterna ska se till att överträdelser av skyldigheterna enligt artikel 18 eller artikel 20, i enlighet med punkterna 2 och 3 i den här artikeln, medför administrativa sanktionsavgifter på minst 10 000 000 EUR eller minst 2 % av den totala globala årsomsättningen under det föregående räkenskapsåret för det företag som den väsentliga eller viktiga entiteten tillhör, beroende på vilken siffra som är högst.
5. Medlemsstaterna får föreskriva befogenhet att förelägga viten för att tvinga en väsentlig eller viktig entitet att upphöra med en överträdelse i enlighet med ett föregående beslut av den behöriga myndigheten.
6. Utan att det påverkar behöriga myndigheters befogenheter enligt artiklarna 29 och 30 får varje medlemsstat fastställa regler för huruvida och i vilken utsträckning administrativa sanktionsavgifter kan påföras offentliga förvaltningsentiteter som

avses i artikel 4.23 och som omfattas av de skyldigheter som föreskrivs i detta direktiv.

Artikel 32

Överträdelser som innebär personuppgiftsincidenter

1. Om de behöriga myndigheterna har indikationer på att en väsentlig eller viktig entitets överträdelse av de skyldigheter som fastställs i artiklarna 18 och 20 innebär en personuppgiftsincident, enligt definitionen i artikel 4.12 i förordning (EU) 2016/679 och som ska anmälas i enlighet med artikel 33 i den förordningen, ska de informera de tillsynsmyndigheter som är behöriga i enlighet med artiklarna 55 och 56 i den förordningen inom en rimlig tidsperiod.
2. Om de tillsynsmyndigheter som är behöriga i enlighet med artiklarna 55 och 56 i förordning (EU) 2016/679 beslutar att utöva sina befogenheter enligt artikel 58.2 i i den förordningen och påföra administrativa sanktionsavgifter, ska de behöriga myndigheterna inte påföra någon administrativ sanktionsavgift för samma överträdelse enligt artikel 31 i detta direktiv. De behöriga myndigheterna får dock tillämpa de efterlevnadskontrollåtgärder eller utöva de sanktionsbefogenheter som föreskrivs i artikel 29.4 a–i, artikel 29.5 och artikel 30.4 a–h i detta direktiv.
3. Om den tillsynsmyndighet som är behörig enligt förordning (EU) 2016/679 är etablerad i en annan medlemsstat än den behöriga myndigheten, får den behöriga myndigheten informera den tillsynsmyndighet som är etablerad i samma medlemsstat.

Artikel 33

Sanktioner

1. Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av nationella bestämmelser som antagits enligt detta direktiv och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande.
2. Medlemsstaterna ska till kommissionen anmäla dessa regler och åtgärder senast [två] år efter ikraftträdandet av detta direktiv samt utan onödigt dröjsmål eventuella ändringar som berör dem.

Artikel 34

Ömsesidigt bistånd

1. Om en väsentlig eller viktig entitet tillhandahåller tjänster i mer än en medlemsstat eller har sitt huvudsakliga etableringsställe eller en företrädare i en medlemsstat medan dess nätverks- och informationssystem är belägna i en eller flera andra medlemsstater, ska den behöriga myndigheten i den medlemsstat där det huvudsakliga etableringsstället eller ett annat etableringsställe eller företrädaren finns

och de behöriga myndigheterna i dessa andra medlemsstater vid behov samarbeta med och bistå varandra. Detta samarbete ska åtminstone omfatta följande:

- (a) Att de behöriga myndigheter som tillämpar tillsyns- eller efterlevnadskontrollåtgärder i en medlemsstat via den gemensamma kontaktpunkten informerar och samråder med de behöriga myndigheterna i övriga berörda medlemsstater om de tillsyns- och efterlevnadskontrollåtgärder som vidtagits och uppföljningen av dem, i enlighet med artiklarna 29 och 30.
 - (b) Att en behörig myndighet får begära att en annan behörig myndighet vidtar de tillsyns- eller efterlevnadskontrollåtgärder som avses i artiklarna 29 och 30.
 - (c) Att en behörig myndighet, efter att ha mottagit en motiverad begäran från en annan behörig myndighet, ska bistå den andra behöriga myndigheten så att de tillsyns- eller efterlevnadskontrollåtgärder som avses i artiklarna 29 och 30 kan genomföras på ett ändamålsenligt, effektivt och konsekvent sätt. Sådant ömsesidigt bistånd får omfatta begäranden om information och tillsynsåtgärder, inbegripet begäranden om att utföra inspektioner på plats, distansbaserad tillsyn eller riktade säkerhetsrevisioner. En behörig myndighet till vilken en begäran om bistånd riktas får bara avslå begäran om det efter ett utbyte med övriga berörda myndigheter, Enisa och kommissionen fastställs att myndigheten antingen inte är behörig att tillhandahålla det begärda biståndet eller att det begärda biståndet inte står i proportion till den behöriga myndighetens tillsynsuppgifter i enlighet med artikel 29 eller artikel 30.
2. När så är lämpligt och i samförstånd får behöriga myndigheter från olika medlemsstater genomföra de gemensamma tillsynsåtgärder som avses i artiklarna 29 och 30.

KAPITEL VII

Övergångsbestämmelser och slutbestämmelser

Artikel 35

Översyn

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

Artikel 36

Utövande av delegeringen

1. Befogenheten att anta delegerade akter ges till kommissionen med förbehåll för de villkor som anges i denna artikel.
2. Den befogenhet att anta delegerade akter som avses i artiklarna 18.6 och 21.2 ska ges till kommissionen för en period på fem år från och med den [...].
3. Den delegering av befogenhet som avses i artiklarna 18.6 och 21.2 får när som helst återkallas av Europaparlamentet eller rådet. Ett beslut om återkallelse innebär att delegeringen av den befogenhet som anges i beslutet upphör att gälla. Beslutet får verkan dagen efter det att det offentliggörs i Europeiska unionens officiella tidning, eller vid ett senare i beslutet angivet datum. Det påverkar inte giltigheten av delegerade akter som redan har trätt i kraft.
4. Innan kommissionen antar en delegerad akt, ska den samråda med experter som utsetts av varje medlemsstat i enlighet med principerna i det interinstitutionella avtalet om bättre lagstiftning av den 13 april 2016.
5. Så snart kommissionen antar en delegerad akt ska den samtidigt delge Europaparlamentet och rådet denna.
6. En delegerad akt som antas enligt artiklarna 18.6 och 21.2 ska träda i kraft endast om varken Europaparlamentet eller rådet har gjort invändningar mot den delegerade akten inom en period på två månader från den dag då akten delgavs Europaparlamentet och rådet, eller om både Europaparlamentet och rådet, före utgången av den perioden, har underrättat kommissionen om att de inte kommer att invända. Denna period ska förlängas med två månader på Europaparlamentets eller rådets initiativ.

Artikel 37

Kommittéförfarande

1. Kommissionen ska biträdas av en kommitté. Denna kommitté ska vara en kommitté i den mening som avses i förordning (EU) nr 182/2011.
2. När det hänvisas till denna punkt ska artikel 5 i förordning (EU) nr 182/2011 tillämpas.
3. Om kommitténs yttrande ska inhämtas genom skriftligt förfarande, ska det förfarandet avslutas utan resultat om kommitténs ordförande, inom tidsfristen för att avge yttrandet, så beslutar eller en kommittéledamot så begär.

Artikel 38

Införlivande

1. Medlemsstaterna ska senast den ... [18 månader efter dagen för detta direktivs ikraftträdande] anta och offentliggöra de lagar och andra författningar som är nödvändiga för att följa detta direktiv. De ska genast underrätta kommissionen om detta. De ska tillämpa dessa bestämmelser från och med den ... [en dag efter den dag som avses i första stycket].

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

Artikel 39

Ändring av förordning (EU) nr 910/2014

Artikel 19 i förordning (EU) nr 910/2014 ska utgå.

Artikel 40

Ändring av direktiv (EU) 2018/1972

Artiklarna 40 och 41 i direktiv (EU) 2018/1972 ska utgå.

Artikel 41

Upphävande

Direktiv (EU) 2016/1148 ska upphöra att gälla med verkan ... [datum för tidsfristen för införlivande av direktivet].

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

Artikel 42

Ikraftträdande

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

Artikel 43

Adressater

Detta direktiv riktar sig till medlemsstaterna.

Utfärdat i Bryssel den

På Europaparlamentets vägnar
Ordförande

På rådets vägnar
Ordförande

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT

Innehåll

1.	GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET	2
1.1.	Förslagets eller initiativets titel	2
1.2.	Berörda politikområden (<i>programkluster</i>)	2
1.3.	Typ av förslag eller initiativ	2
1.4.	Grunder för förslaget eller initiativet	2
1.4.1.	Krav som ska uppfyllas på kort eller lång sikt, inbegripet en detaljerad tidsplan för genomförandet av initiativet	2
1.4.2.	Mervärdet i unionens intervention (som kan följa av flera faktorer, t.ex. samordningsfördelar, rättssäkerhet, ökad effektivitet eller komplementaritet). Med ”mervärdet i unionens intervention” i denna punkt avses det värde en åtgärd från unionens sida tillför utöver det värde som annars skulle ha skapats av enbart medlemsstaterna.	2
1.4.3.	Erfarenheter från tidigare liknande åtgärder	3
1.4.4.	Förenlighet och eventuella synergieffekter med andra relevanta instrument	3
1.5.	Varaktighet och budgetkonsekvenser	4
1.6.	Planerad metod för genomförandet	4
2.	FÖRVALTNING	6
2.1.	Regler om uppföljning och rapportering	6
2.2.	Förvaltnings- och kontrollsystem	6
2.2.1.	Motivering av den genomförandemetod, de finansieringsmekanismer, de betalningsvillkor och den kontrollstrategi som föreslås	6
2.2.2.	Uppgifter om identifierade risker och om det eller de interna kontrollsystem som inrättats för att begränsa riskerna	6
2.2.3.	Beräkning och motivering av kontrollernas kostnadseffektivitet (dvs. förhållandet mellan kostnaden för kontrollerna och värdet av de medel som förvaltas) och en bedömning av den förväntade risken för fel (vid betalning och vid avslutande)	6
2.3.	Åtgärder för att förebygga bedrägeri och oriktigheter	6
3.	BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET	7
3.1.	Rubrik i den fleråriga budgetramen och föreslagna nya budgetrubriker i den årliga budgetens utgiftsdel	7
3.2.	Beräknad inverkan på utgifter	8
3.2.1.	Sammanfattning av den beräknade inverkan på utgifterna	8
3.2.2.	Sammanfattning av beräknad inverkan på de administrativa anslagen	11
3.2.3.	Bidrag från tredje part	13

3.3.	Beräknad inverkan på inkomsterna	13
------	--	----

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1. Förslaget eller initiativets titel

Förslag till direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148

1.2. Berörda politikområden (*programkluster*)

Kommunikationsnät, innehåll och teknik

1.3. Typ av förslag eller initiativ

☐ en ny åtgärd

☐ en ny åtgärd som bygger på ett pilotprojekt eller en förberedande åtgärd⁴⁰

☒ en förlängning av en befintlig åtgärd

☐ en sammanslagning eller omdirigering av en eller flera åtgärder mot en annan/en ny åtgärd

1.4. Grunder för förslaget eller initiativet

1.4.1. *Krav som ska uppfyllas på kort eller lång sikt, inbegripet en detaljerad tidsplan för genomförandet av initiativet*

Syftet med översynen är att öka cyberresiliensen för ett stort antal företag med verksamhet i EU inom alla relevanta sektorer, minska bristen på enhetlighet för motståndskraften på den inre marknaden inom de sektorer som redan omfattas av direktivet och förbättra den gemensamma situationsmedvetenheten och den kollektiva förmågan att förbereda sig och reagera.

1.4.2. *Mervärdet i unionens intervention (som kan följa av flera faktorer, t.ex. samordningsfördelar, rättssäkerhet, ökad effektivitet eller komplementaritet). Med "mervärdet i unionens intervention" i denna punkt avses det värde en åtgärd från unionens sida tillför utöver det värde som annars skulle ha skapats av enbart medlemsstaterna.*

Det kan inte finnas en effektiv motståndskraft mot cyberhot i unionen om frågan hanteras på olika sätt genom ett nationellt eller regionalt silotänkande. Syftet med NIS-direktivet var att hantera denna brist genom att fastställa en ram för säkerhet i nätverks- och informationssystem på en nationell nivå och på EU-nivå. Den första periodiska översynen av NIS-direktivet pekade dock på ett antal inneboende brister som så småningom skulle lett till betydande skillnader mellan medlemsstaterna i fråga om kapacitet, planering och skyddsnivå vilket också skulle påverkat lika villkor för liknande företag på den inre marknaden.

Ett EU-ingripande utöver de nuvarande åtgärderna i NIS-direktivet motiveras främst av följande skäl: i) problemets gränsöverskridande karaktär, ii) EU-åtgärdernas potential att förbättra och underlätta en effektiv nationell politik, och iii) bidraget av samordnade och samarbetsinriktade nät- och informationssäkerhetspolitiska åtgärder för ett effektivt skydd av personuppgifter och integritet.

⁴⁰

I den mening som avses i artikel 58.2 a eller b i budgetförordningen.

De angivna målen kan därför bättre uppnås med hjälp av åtgärder på EU-nivå än av åtgärder vidtagna av de enskilda medlemsstaterna.

1.4.3. Erfarenheter från tidigare liknande åtgärder

NIS-direktivet är det första övergripande instrumentet för den inre marknaden som syftar till att förbättra motståndskraften mot cybersäkerhetsrisker hos nät och system i unionen. Det har redan i hög grad bidragit till att höja den gemensamma nivån på cybersäkerhet bland medlemsstaterna. Översynen av direktivets funktion och genomförande har dock pekat på ett antal brister som, utöver den ökande digitaliseringen och behovet av mer aktuella svarsalternativ, måste hanteras i en reviderad rättsakt.

1.4.4. Förenlighet och eventuella synergieffekter med andra relevanta instrument

Det nya förslaget är helt förenligt med och överensstämmer med andra relaterade initiativ, såsom förslaget till förordning om digital operativ motståndskraft i finanssektorn samt förslaget till direktiv om motståndskraften hos kritiska leverantörer av samhällsviktiga tjänster. Det är också förenligt med den europeiska kodexen för elektronisk kommunikation, den allmänna dataskyddsförordningen och eIDA-förordningen.

Förslaget är en viktig del av EU:s strategi för en säkerhetsunion.

1.5. Varaktighet och budgetkonsekvenser

☐ **begränsad varaktighet**

- ☐ verkan från och med [den DD/MM]ÅÅÅÅ till och med [den DD/MM]ÅÅÅÅ
- ☐ budgetkonsekvenser från och med ÅÅÅÅ till och med ÅÅÅÅ för åtagandebemyndiganden och från och med ÅÅÅÅ till och med ÅÅÅÅ för betalningsbemyndiganden.

☒ **obegränsad varaktighet**

- Efter en inledande period 2022–2025
- beräknas genomförandetakten nå en stabil nivå.

1.6. Planerad metod för genomförandet⁴¹

Direkt förvaltning som sköts av kommissionen

- ☒ av dess avdelningar, vilket också inbegriper personalen vid unionens delegationer,
- ☐ av genomförandeorgan

☐ **Delad förvaltning** med medlemsstaterna

☐ **Indirekt förvaltning** genom att uppgifter som ingår i budgetgenomförandet anförtros

- ☐ tredjeländer eller organ som de har utsett
- ☐ internationella organisationer och organ kopplade till dem (ange vilka)
- ☐ EIB och Europeiska investeringsfonden
- ☒ organ som avses i artiklarna 70 och 71 i budgetförordningen
- ☐ offentligrättsliga organ
- ☐ privaträttsliga organ som har anförtrotts offentliga förvaltningsuppgifter i den utsträckning som de lämnar tillräckliga ekonomiska garantier
- ☐ organ som omfattas av privaträtten i en medlemsstat, som anförtrotts genomförandeuppgifter inom ramen för ett offentlig-privat partnerskap och som lämnar tillräckliga ekonomiska garantier
- ☐ personer som anförtrotts genomförandet av särskilda åtgärder inom Gusp enligt avdelning V i fördraget om Europeiska unionen och som fastställs i den relevanta grundläggande rättsakten
- *Vid fler än en metod, ange kompletterande uppgifter under "Anmärkningar".*

Anmärkningar

Europeiska unionens cybersäkerhetsbyrå Enisa, som har fått ett nytt permanent mandat genom cybersäkerhetsakten, skulle bistå medlemsstaterna och kommissionen i genomförandet av det reviderade NIS-direktivet.

⁴¹

Närmare förklaringar av de olika metoderna för genomförande med hänvisningar till respektive bestämmelser i budgetförordningen återfinns på BudgWeb:
<https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx>

Som ett resultat av det reviderade NIS-direktivet kommer Enisa från och med 2022/23 att ansvara för ytterligare åtgärdsområden. Dessa åtgärdsområden skulle omfattas av Enisas allmänna uppgifter i enlighet med dess mandat, men de kommer att leda till ytterligare arbetsbelastning för byrån. Enisa kommer närmare bestämt inom ramen för kommissionens förslag till ett reviderat NIS-direktiv att utöver sina nuvarande åtgärdsområden särskilt bland annat införliva följande uppgifter i sitt arbetsprogram: i) utveckla och underhålla ett europeiskt sårbarhetsregister (artikel 6.2 i förslaget), ii) tillhandahålla sekretariatet för Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe), (artikel 14 i förslaget), utfärda en årlig rapport om cybersäkerhetssituationen i unionen (artikel 15 i förslaget), iii) stödja anordnandet av sakkunnigbedömningar mellan medlemsstaterna (artikel 16 i förslaget), iv) samla in aggregerade uppgifter om incidenter från medlemsstaterna och utfärda teknisk vägledning (artikel 20.9 i förslaget), v) skapa och upprätthålla ett register över entiteter som tillhandahåller gränsöverskridande tjänster (artikel 25 i förslaget).

Därför kommer en begäran om fem ytterligare heltidsekvivalenter att göras från och med 2022 med motsvarande budget på cirka 0,61 miljoner euro per år för att täcka dessa nya tjänster (se separat finansieringsöversikt för byråer).

2. FÖRVALTNING

2.1. Regler om uppföljning och rapportering

Ange intervall och andra villkor för sådana åtgärder:

Kommissionen kommer regelbundet att se över hur direktivet fungerar och rapportera till Europaparlamentet och rådet, första gången tre år efter direktivets ikraftträdande.

Kommissionen kommer också att utvärdera om medlemsstaterna har införlivat direktivet korrekt.

2.2. Förvaltnings- och kontrollsystem

2.2.1. *Motivering av den genomförandemetod, de finansieringsmekanismer, de betalningsvillkor och den kontrollstrategi som föreslås*

Den enhet inom GD CNECT som ansvarar för politikområdet kommer att ansvara för genomförandet av direktivet.

2.2.2. *Uppgifter om identifierade risker och om det eller de interna kontrollsystem som inrättats för att begränsa riskerna*

Mycket låg risk eftersom det redan finns ett ekosystem för NIS-direktivet.

2.2.3. *Beräkning och motivering av kontrollernas kostnadseffektivitet (dvs. förhållandet mellan kostnaden för kontrollerna och värdet av de medel som förvaltas) och en bedömning av den förväntade risken för fel (vid betalning och vid avslutande)*

Inte relevant. Endast användning av administrativ budget ("ramanslag").

2.3. Åtgärder för att förebygga bedrägeri och oriktigheter

Beskriv förebyggande åtgärder (befintliga eller planerade), t.ex. från strategi för bedrägeribekämpning.

Inte relevant. Endast användning av administrativ budget ("ramanslag").

3. BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET

3.1. Rubrik i den fleråriga budgetramen och föreslagna nya budgetrubriker i den årliga budgetens utgiftsdel

Rubrik i den fleråriga budgetramen	Budgetrubrik	Typ av utgifter	Bidrag			
	Nummer [Rubrik...7.....]	Diff./Icke-diff. ⁴²	från Efta-länder ⁴³	från kandidat-länder ⁴⁴	från tredje-länder	enligt artikel [21.2 b] i budgetförordningen
	20 02 06 förvaltningsutgifter					
	20 02 06	Icke-diff.	NEJ	NEJ	NEJ	NEJ

⁴² Diff. = differentierade anslag/Icke-diff. = icke-differentierade anslag.

⁴³ Efta: Europeiska frihandelssammanslutningen.

⁴⁴ Kandidatländer och i förekommande fall potentiella kandidatländer i västra Balkan.

3.2. Beräknad inverkan på utgifter

3.2.1. Sammanfattning av den beräknade inverkan på utgifterna

Miljoner euro (avrundat till tre decimaler)

Rubrik i den fleråriga budgetramen	<...>	[Rubrik.....]
------------------------------------	-------	---------------

			2021	2022	2023	2024	2025	2026	2027	Efter 2027	TOTALT
Driftsanslag (uppdelade enligt de budgetrubriker som förtecknas under 3.1)	Åtaganden	(1)									
	Betalningar	(2)									
Anslag av administrativ natur som finansieras genom ramanslagen för programmet ⁴⁵	Åtaganden = betalningar	(3)									
TOTALA anslag för ramanslagen för programmet	Åtaganden	=1+3									
	Betalningar	=2+3									

Rubrik i den fleråriga budgetramen	7	”Administrativa utgifter” Möten: Plenarmöten i samarbetsgruppen äger vanligtvis rum fyra gånger per år. Kommissionen täcker catering- och resekostnader för representanter från 27 medlemsstater (en representant per medlemsstat). Kostnaderna för ett möte kan uppgå till 15 000 euro. Tjänsteresor: Tjänsteresor är kopplade till översynen av genomförandet av NIS-direktivet. Exempel: Under ett år (maj 2019–juli 2020) skulle vi anordna så kallade landsbesök för nät- och informationssäkerhet och besöka samtliga 27 medlemsstater
------------------------------------	---	---

⁴⁵ Detta avser tekniskt eller administrativt stöd för genomförandet av vissa av Europeiska unionens program och åtgärder (tidigare s.k. BA-poster) samt indirekta och direkta forskningsåtgärder.

		för att diskutera genomförandet av NIS-direktivet i hela EU.
--	--	--

Detta avsnitt ska fyllas i med hjälp av det datablad för budgetuppgifter av administrativ natur som först ska föras in i [bilagan till finansieringsöversikt för rättsakt](#), vilken ska laddas upp i DECIDE som underlag för samråden mellan kommissionens avdelningar.

Miljoner euro (avrundat till tre decimaler)

		2021	2022	2023	2024	2025	2026	2027	<i>Efter 2027</i>	TOTALT
Personalresurser		1,14	1,14	1,14	1,14	1,14	1,14	1,14		7,98
Övriga administrativa utgifter		0,09	0,09	0,09	0,09	0,09	0,09	0,09		0,63
Totala anslag för RUBRIK 7 i den fleråriga budgetramen	(summa åtaganden = summa betalningar)	1,23	1,23	1,23	1,23	1,23	1,23	1,23		8,61

Miljoner euro (avrundat till tre decimaler)

		2021	2022	2023	2024	2025	2026	2027	<i>Efter 2027</i>	TOTALT
TOTALA anslag för samtliga RUBRIKER i den fleråriga budgetramen	Åtaganden									
	Betalningar									

3.2.2. Sammanfattning av beräknad inverkan på de administrativa anslagen

- ☐ Förslaget/initiativet kräver inte att anslag av administrativ natur tas i anspråk
- ☒ Förslaget/initiativet kräver att anslag av administrativ natur tas i anspråk enligt följande:

Miljoner euro (avrundat till tre decimaler)

År	2021	2022	2023	2024	2025	2026	2027	TOTALT
----	------	------	------	------	------	------	------	--------

RUBRIK 7 i den fleråriga budgetramen								
Personalresurser	1,14	1,14	1,14	1,14	1,14	1,14	1,14	7,98
Övriga administrativa utgifter	0,09	0,09	0,09	0,09	0,09	0,09	0,09	0,63
Delsumma RUBRIK 7 i den fleråriga budgetramen	1,23	1,23	1,23	1,23	1,23	1,23	1,23	8,61

Utanför RUBRIK 7⁴⁶ i den fleråriga budgetramen								
Personalresurser								
Andra administrativa kostnader								
Delsumma utanför RUBRIK 7 i den fleråriga budgetramen								

TOTALT	1,23	1,23	1,23	1,23	1,23	1,23	1,23	8,61
---------------	------	------	------	------	------	------	------	------

Personalbehov och andra administrativa kostnader ska täckas genom anslag inom generaldirektoratet vilka redan har avdelats för förvaltningen av åtgärden i fråga, eller genom en omfördelning av anslag inom generaldirektoratet, om så krävs kompletterad med ytterligare resurser som kan tilldelas det förvaltande generaldirektoratet som ett led i det årliga förfarandet för tilldelning av anslag och med hänsyn tagen till begränsningar i fråga om budgetmedel.

⁴⁶

Detta avser tekniskt eller administrativt stöd för genomförandet av vissa av Europeiska unionens program och åtgärder (tidigare s.k. BA-poster) samt indirekta och direkta forskningsåtgärder.

3.2.2.1. Beräknat personalbehov

- ☐ Förslaget/initiativet kräver inte att personalresurser tas i anspråk
- ☒ Förslaget/initiativet kräver att personalresurser tas i anspråk enligt följande:

Beräkningarna ska anges i heltidsekvivalenter

År	2021	2022	2023	2024	2025	2026	2027
•Tjänster som tas upp i tjänsteförteckningen (tjänstemän och tillfälligt anställda)							
Vid huvudkontoret eller kommissionens kontor i medlemsstaterna	6	6	6	6	6	6	6
Vid delegationer							
Forskningsåtgärder							
• Extern personal (i heltidsekvivalenter) – kontraktsanställda, lokalanställda, nationella experter, vikarier och unga experter som tjänstgör vid delegationerna ⁴⁷							
Rubrik 7							
Som finansieras genom RUBRIK 7 i den fleråriga budgetramen	- vid huvudkontoret	3	3	3	3	3	3
	- vid delegationer						
Som finansieras genom ramanslagen för programmet ⁴⁸	- vid huvudkontoret						
	- vid delegationer						
Forskningsåtgärder							
Annat (ange)							
TOTALT	9	9	9	9	9	9	9

Personalbehoven ska täckas med personal inom generaldirektoratet vilka redan har avdelats för förvaltningen av åtgärden i fråga, eller genom en omfördelning av personal inom generaldirektoratet, om så krävs kompletterad med ytterligare resurser som kan tilldelas det förvaltande generaldirektoratet som ett led i det årliga förfarandet för tilldelning av anslag och med hänsyn tagen till begränsningar i fråga om budgetmedel.

Beskrivning av arbetsuppgifter:

Tjänstemän och tillfälligt anställda	- Förberedelse av delegerade akter i enlighet med artikel 18.6, artikel 21.2 och artikel 36. - Utarbetande av genomförandeakter i enlighet med artikel 12.8, artikel 18.5 och artikel 20.11. - Tillhandahållande av ett sekretariat för samarbetsgruppen. - Anordnande av plenarmöten och arbetsmöten inom samarbetsgruppen. - Samordning av medlemsstaternas arbete med olika dokument (riktlinjer, verktygslådor osv.). - Kontakter med andra avdelningar inom kommissionen, Enisa och nationella myndigheter i syfte att genomföra NIS-direktivet. - Analys av nationella metoder och bästa praxis i samband med genomförandet av NIS-direktivet.
Extern personal	Stöd till alla ovanstående uppgifter enligt behov

⁴⁷ [I denna fotnot förklaras vissa initialförkortningar som inte används i den svenska versionen].
⁴⁸ Särskilt tak för finansiering av extern personal genom driftsanslag (tidigare s.k. BA-poster).

3.2.3. Bidrag från tredje part

Förslaget/initiativet:

- ☒ innehåller inga bestämmelser om samfinansiering från tredje parter
- ☐ innehåller bestämmelser om samfinansiering från tredje parter enligt följande uppskattning:

Anslag i miljoner euro (avrundat till tre decimaler)

År	2021	2022	2023	2024	2025	2026	2027	TOTALT
Ange vilket organ som deltar i samfinansieringen								
TOTALA anslag som tillförs genom samfinansiering								

3.3. Beräknad inverkan på inkomsterna

- ☒ Förslaget/initiativet påverkar inte budgetens inkomstsida.
- ☐ Förslaget/initiativet påverkar inkomsterna på följande sätt:
 - ☐ påverkan på egna medel
 - ☐ påverkan på andra inkomster

ange om inkomsterna har avsatts för utgiftsposter ☐

Miljoner euro (avrundat till tre decimaler)

Budgetrubrik i den årliga budgetens inkomstsidan:	Förslagets/initiativets inverkan på inkomsterna ⁴⁹						
	2021	2022	2023	2024	2025	2026	2027
Artikel							

För inkomster avsatta för särskilda ändamål, ange vilka budgetrubriker i utgiftsdelen som berörs.

Övriga anmärkningar (t.ex. vilken metod/formel som har använts för att beräkna inverkan på inkomsterna eller andra relevanta uppgifter).

⁴⁹ Vad gäller traditionella egna medel (tullar, sockeravgifter) ska nettobeloppen anges, dvs. bruttobeloppen minus 20 % avdrag för uppbördskostnader.

BILAGA

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT

Förslagets eller initiativets namn

Förslag till ett direktiv om ändring av Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen

1. **STORLEK PÅ OCH KOSTNAD FÖR PERSONALBEHOVET**
2. **KOSTNAD FÖR ÖVRIGA ADMINISTRATIVA UTGIFTER**
3. **METOD FÖR BERÄKNING AV KOSTNADERNA**
 - 3.1 **Personalresurser**
 - 3.2 **Övriga administrativa utgifter**

Denna bilaga, som ska fyllas i av de generaldirektorat eller avdelningar som deltar i förslaget/initiativet, ska åtfölja finansieringsöversikten för rättsakten när internremissen inleds.

Tabellerna används som källa för tabellerna i finansieringsöversikten för rättsakten. De är uteslutande avsedda för internt bruk inom kommissionen.

1. Kostnad för personalbehovet

- ☐ Förslaget/initiativet kräver inte att personalresurser tas i anspråk
- ☒ Förslaget/initiativet kräver att personalresurser tas i anspråk enligt följande:

Miljoner euro (avrundat till tre decimaler)

RUBRIK 7 n fleråriga budgetramen		2021		2022		2023		2024		2025		2026		2027		TOT
		Heltidsekvivalent	Anslag	Heltidsekvivalent	Anslag	Heltidsekvivalent	Anslag	Heltidsekvivalent	Anslag	Heltidsekvivalent	Anslag	Heltidsekvivalent	Anslag	Heltidsekvivalent	Anslag	Heltidsekvivalent
ster som tas upp i tjänsteförteckningen (tjänstemän och tillfälligt anställda)																
ontoret sionens i sstaterna	AD	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	6	0,9	42
	AST															
unionens ioner	AD															
	AST															
rn personal ⁵⁰ 0,24																
slag	Kontraktanställda	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	3	0,24	21
	Nationella experter															
	Vikarier															
unionens	Kontraktanställda															

⁵⁰ [I denna fotnot förklaras vissa initialförkortningar som inte används i den svenska versionen]

ioner	Lokalanställda															
	Nationella experter															
	Vikarier															
	Unga experter som tjänstgör vid delegationerna															
ubrik (ilken)																
mma – RIK 7 leråriga etramen		9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	9	1,14	63

Personalbehoven ska täckas med personal inom generaldirektoratet vilka redan har avdelats för förvaltningen av åtgärden i fråga, eller genom en omfördelning av personal inom generaldirektoratet, om så krävs kompletterad med ytterligare resurser som kan tilldelas det förvaltande generaldirektoratet som ett led i det årliga förfarandet för tilldelning av anslag och med hänsyn tagen till begränsningar i fråga om budgetmedel.

Utanför RUBRIK 7		2021		2022		2023		2024		2025		2025		2025		
n fleråriga budgetramen		Heltidsekvivalent	Anslag	Heltidsekvivalent	Anslag	Heltidsekvivalent	Anslag	Heltidsekvivalent	Anslag	Heltidsekvivalent	Anslag	Heltidsekvivalent	Anslag	Heltidsekvivalent	Anslag	Heltidsekvivalent
om tas upp i tjänsteförteckningen (tjänstemän och tillfälligt anställda)																
gärder	AD															
	AST															
ersonal ⁵¹																
- vid huvudkontoret	Kontraktsanställda															
	Nationella experter															
	Vikarier															
- vid unionens delegationer	Kontraktsanställda															
	Lokalanställda															
	Nationella experter															
	Vikarier															
	Unga experter som tjänstgör vid delegationerna															
gärder)	Kontraktsanställda															
	Nationella experter															

⁵¹ [I denna fotnot förklaras vissa initialförkortningar som inte används i den svenska versionen]

	Vikarier															
etrubrik (ange																
a – utanför RIK 7 fleråriga etramen																

Personalbehoven ska täckas med personal inom generaldirektoratet vilka redan har avdelats för förvaltningen av åtgärden i fråga, eller genom en omfördelning av personal inom generaldirektoratet, om så krävs kompletterad med ytterligare resurser som kan tilldelas det förvaltande generaldirektoratet som ett led i det årliga förfarandet för tilldelning av anslag och med hänsyn tagen till begränsningar i fråga om budgetmedel.

Beräknad inverkan på Enisas personalresurser

Europeiska unionens cybersäkerhetsbyrå Enisa, som har fått ett nytt permanent mandat genom cybersäkerhetsakten, skulle bistå medlemsstaterna och kommissionen i genomförandet av det reviderade NIS-direktivet.

Som ett resultat av det reviderade NIS-direktivet kommer Enisa från och med 2022/23 att ansvara för ytterligare åtgärdsområden. Dessa åtgärdsområden skulle omfattas av Enisas allmänna uppgifter i enlighet med dess mandat, men de kommer att leda till ytterligare arbetsbelastning för byrån. Enisa kommer närmare bestämt inom ramen för kommissionens förslag till ett reviderat NIS-direktiv att utöver sina nuvarande åtgärdsområden särskilt bland annat införliva följande uppgifter i sitt arbetsprogram: i) utveckla och underhålla ett europeiskt sårbarhetsregister (artikel 6.2 i förslaget), ii) tillhandahålla sekretariatet för Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe), (artikel 14 i förslaget), utfärda en årlig rapport om cybersäkerhetssituationen i unionen (artikel 15 i förslaget), iii) stödja anordnandet av sakkunnigbedömningar mellan medlemsstaterna (artikel 16 i förslaget), iv) samla in aggregerade uppgifter om incidenter från medlemsstaterna och utfärda teknisk vägledning (artikel 20.9 i förslaget), v) skapa och upprätthålla ett register över entiteter som tillhandahåller gränsöverskridande tjänster (artikel 25 i förslaget).

Därför kommer en begäran om fem ytterligare heltidsekvivalenter att göras från och med 2022 med motsvarande budget på cirka 0,61 miljoner euro per år för att täcka dessa nya tjänster (se separat finansieringsöversikt för byråer).

Därför kommer en begäran om ytterligare fem heltidsekvivalenter att göras från och med 2022 med motsvarande budget för att täcka dessa nya poster.

- ☐ Förslaget/initiativet kräver inte att anslag av administrativ natur tas i anspråk
- ☒ Förslaget/initiativet kräver att anslag av administrativ natur tas i anspråk enligt följande:

Miljoner euro (avrundat till tre decimaler)

	År N ⁵² 2022	År N+1 2023	År N+2 2024	År N+3 2025	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)	TOTALT
--	-------------------------------	-------------------	-------------------	-------------------	---	--------

⁵² Med år N avses det år då förslaget eller initiativet ska börja genomföras. Ersätt "N" med det förväntade första genomförandeåret (till exempel 2021). Detsamma för följande år.

Tillfälligt anställda (AD-tjänster)	0,450	0,450	0,450	0,450	0,450	0,450		2,7
Tillfälligt anställda (AST-tjänster)								
Kontraktsanställda	0,160	0,160	0,160	0,160	0,160	0,160		
Nationella experter								0,96

TOTALT	0,61	0,61	0,61	0,61	0,61	0,61		3,66
---------------	-------------	-------------	-------------	-------------	-------------	-------------	--	-------------

Personalbehov (i heltidsekvivalenter):

	År N ⁵³ 2022	År N+1 2023	År N+2 2024	År N+3 2025	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)	TOTALT
--	-------------------------------	-------------------	-------------------	-------------------	---	--------

Tillfälligt anställda (AD-tjänster)	3	3	3	3	3	3		18
Tillfälligt anställda (AST-tjänster)								
Kontraktsanställda	2	2	2	2	2	2		12

⁵³ Med år N avses det år då förslaget eller initiativet ska börja genomföras. Ersätt ”N” med det förväntade första genomförandeåret (till exempel 2021). Detsamma för följande år.

Nationella experter								
---------------------	--	--	--	--	--	--	--	--

TOTALT	5	5	5	5	5	5		30
--------	---	---	---	---	---	---	--	----

2.
Kostnad för övriga administrativa utgifter

☐
Förslaget/initiativet kräver inte att administrativa anslag tas i anspråk

☒
Förslaget/initiativet kräver att administrativa anslag tas i anspråk enligt följande:

Miljoner euro (avrundat till tre decimaler)

RUBRIK 7 i den fleråriga budgetramen	2021	2022	2023	2024	2025	2026	2027	Totalt
<u>Vid huvudkontoret</u>								
Tjänsteresor och representationsutgifter	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,21
Kostnader för konferenser och möten	0,06	0,06	0,06	0,06	0,06	0,06	0,06	0,42
Kommittéer ⁵⁴								
Studier och samråd								
Informations- och förvaltningssystem								

54
Ange typ av kommitté och den grupp till vilken den hör.

IKT-utrustning och IKT-tjänster ⁵⁵								
Andra budgetrubriker (<i>ange vid behov</i>)								
<u>Vid unionens delegationer</u>								
Utgifter för tjänsteresor, konferenser och representation								
Vidareutbildning av personal								
Förvärv, hyra och därmed sammanhängande utgifter								
Utrustning, möbler, materiel och tjänster								
Delsumma RUBRIK 7 i den fleråriga budgetramen	0,09	0,09	0,09	0,09	0,09	0,09	0,09	0,63

⁵⁵ IKT: Informations- och kommunikationsteknik: DIGIT ska rådfrågas.

Miljoner euro (avrundat till tre decimaler)

Utanför RUBRIK 7 i den fleråriga budgetramen	2021	2022	2023	2024	2025	2026	2027	Totalt
Utgifter för tekniskt och administrativt stöd (gäller ej extern personal) som finansieras från driftsanslag (f.d. "BA-poster")								
- vid huvudkontoret								
- vid unionens delegationer								
Andra administrativa utgifter för forskning								
Andra budgetrubriker (ange vid behov)								
Delsumma för belopp utanför RUBRIK 7 i den fleråriga budgetramen								

TOTALT RUBRIK 7 och utanför RUBRIK 7 i den fleråriga budgetramen	1,23	1,23	1,23	1,23	1,23	1,23	1,23	8,61
--	------	------	------	------	------	------	------	-------------

De administrativa kostnaderna ska täckas genom anslag som redan har avdelats för att förvalta åtgärden i fråga och/eller som har omfördelats, om så krävs kompletterade med ytterligare resurser som kan tilldelas det förvaltande generaldirektoratet som ett led i det årliga förfarandet för tilldelning av anslag och med hänsyn tagen till befintliga begränsningar i fråga om budgetmedel.

3. Metod för beräkning av kostnader

3.1 Personalresurser

I denna del beskrivs den beräkningsmetod som använts för uppskattning av personalbehovet (antaganden om arbetsbörda, inklusive specifika arbeten (arbetsbeskrivningar i Sysper 2), personalkategorier och motsvarande genomsnittliga kostnader).

RUBRIK 7 i den fleråriga budgetramen
<u>ANM.:</u> De genomsnittliga kostnaderna för varje personalkategori vid huvudkontoret finns på BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/pre/legalbasis/Pages/pre-040-020_preparation.aspx
• Tjänstemän och tillfälligt anställda <u>Sex heltidsekvivalenter (genomsnittlig kostnad 0,150) = 0,9 per år</u> - Förberedelse av delegerade akter i enlighet med artikel 18.6, artikel 21.2 och artikel 36. - Utarbetande av genomförandeakter i enlighet med artikel 12.8, artikel 18.5 och artikel 20.11. - Tillhandahållande av ett sekretariat för samarbetsgruppen. - Anordnande av plenarmöten och arbetsmöten inom samarbetsgruppen. - Samordning av medlemsstaternas arbete med olika dokument (riktlinjer, verktygslådor osv.). - Kontakter med andra avdelningar inom kommissionen, Enisa och nationella myndigheter i syfte att genomföra NIS-direktivet. - Analys av nationella metoder och bästa praxis i samband med genomförandet av NIS-direktivet.
• Extern personal <u>Tre kontraktanställda (genomsnittlig kostnad 0,08) = 0,24 per år</u> - Stöd till alla ovanstående uppgifter enligt behov

Utanför RUBRIK 7 i den fleråriga budgetramen
• Enbart tjänster som finansieras via forskningsbudgeten
• Extern personal

3.2 Övriga administrativa utgifter

Ange vilken beräkningsmetod som använts för varje budgetpost.

Ange särskilt vilka antaganden de bygger på (antal möten per år, genomsnittliga kostnader etc.).

RUBRIK 7 i den fleråriga budgetramen

Möten: Plenarmöten i arbetsgruppen äger vanligtvis rum fyra gånger per år. Kommissionen täcker catering- och resekostnader för representanter från 27 medlemsstater (en representant per medlemsstat). Kostnaderna för ett möte kan uppgå till 15 000 euro, vilket innebär 60 000 euro per år.

Tjänsteresor: Tjänsteresor är kopplade till översynen av genomförandet av NIS-direktivet. Exempel: Under ett år (maj 2019–juli 2020) skulle vi anordna så kallade landsbesök för nät- och informationssäkerhet och besöka samtliga 27 medlemsstater för att diskutera genomförandet av NIS-direktivet i hela EU.

Utanför RUBRIK 7 i den fleråriga budgetramen

BILAGA 7

till

KOMMISSIONENS BESLUT

**om interna regler riktade till kommissionens avdelningar avseende genomförandet av
Europeiska unionens allmänna budget (Europeiska kommissionens avsnitt)**

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT – ”BYRÅER”

Denna finansieringsöversikt för rättsakter omfattar begäran om att öka Enisas personal med fem heltidsekvivalenter från och med 2022 för att utföra kompletterande verksamhet i samband med genomförandet av NIS-direktivet. Denna verksamhet omfattas redan av Enisas mandat.

Contents

1.	GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET ...	16
1.1.	Förslagets eller initiativets titel	16
1.2.	Berörda politikområden	16
1.3.	Typ av förslag	16
1.4.	Mål	16
1.4.1.	Allmänt/allmänna mål:.....	16
1.4.2.	Specifikt/specifika mål:.....	16
1.4.3.	Verkan eller resultat som förväntas	18
1.4.4.	Prestationsindikatorer.....	18
1.5.	Grunder för förslaget eller initiativet	19
1.5.1.	Krav som ska uppfyllas på kort eller lång sikt, inbegripet en detaljerad tidsplan för genomförandet av initiativet	19
1.5.2.	Mervärdet i unionens intervention (som kan följa av flera faktorer, t.ex. samordningsfördelar, rättssäkerhet, ökad effektivitet eller komplementaritet). Med ”mervärdet i unionens intervention” i denna punkt avses det värde en åtgärd från unionens sida tillför utöver det värde som annars skulle ha skapats av enbart medlemsstaterna.	20
1.5.3.	Erfarenheter från tidigare liknande åtgärder	20
1.5.4.	Förenlighet med den fleråriga budgetramen och eventuella synergieffekter med andra relevanta instrument	20
1.5.5.	En bedömning av de olika finansieringsalternativ som finns att tillgå, inbegripet möjligheter till omfördelning	20
1.6.	Varaktighet för och budgetkonsekvenser av förslaget eller initiativet	21
1.7.	Planerad metod för genomförandet.....	21
2.	FÖRVALTNING	23
2.1.	Regler om uppföljning och rapportering.....	23
2.2.	Förvaltnings- och kontrollsystem.....	23
2.2.1.	Motivering av den genomförandemetod, de finansieringsmekanismer, de betalningsvillkor och den kontrollstrategi som föreslås	23
2.2.2.	Uppgifter om identifierade risker och om det eller de interna kontrollsystem som inrättats för att begränsa riskerna.....	23
2.2.3.	Beräkning och motivering av kontrollernas kostnadseffektivitet (dvs. förhållandet mellan kostnaden för kontrollerna och värdet av de medel som förvaltas) och en bedömning av den förväntade risken för fel (vid betalning och vid avslutande)	23
2.3.	Åtgärder för att förebygga bedrägeri och oriktigheter	24

3.	BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET	24
3.1.	Berörda rubriker i den fleråriga budgetramen och budgetrubriker i den årliga budgetens utgiftsdel.....	24
3.2.	Beräknad inverkan på utgifter	26
3.2.1.	Sammanfattning av den beräknade inverkan på utgifterna	26
3.2.2.	Beräknad inverkan på [organets] anslag	28
3.2.3.	Beräknad inverkan på Enisas personalresurser	29
3.2.4.	Förenlighet med den gällande fleråriga budgetramen.....	32
3.2.5.	Bidrag från tredje part	32
3.3.	Beräknad inverkan på inkomsterna.....	33

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1. Förslaget eller initiativets titel

Förslag till direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, och om upphävande av direktiv (EU) 2016/1148

1.2. Berörda politikområden

Kommunikationsnät, innehåll och teknik

1.3. Typ av förslag

- ☐ en ny åtgärd
- ☐ en ny åtgärd som bygger på ett pilotprojekt eller en förberedande åtgärd⁵⁶
- ☒ en förlängning av en befintlig åtgärd
- ☐ en sammanslagning av en eller flera åtgärder mot en annan/en ny åtgärd

1.4. Mål

1.4.1. Allmänt/allmänna mål:

Syftet med översynen är att öka cyberresiliensen för ett stort antal företag med verksamhet i EU inom alla relevanta sektorer, minska bristen på enhetlighet för motståndskraften på den inre marknaden inom de sektorer som redan omfattas av direktivet och förbättra den gemensamma situationsmedvetenheten och den kollektiva förmågan att förbereda sig och reagera.

1.4.2. Specifikt/specifika mål:

För att ta itu med problemet med en låg nivå av cyberresiliens hos företag som är verksamma inom EU är det särskilda målet att säkerställa att entiteter inom alla sektorer som är beroende av nätverks- och informationssystem och som tillhandahåller nyckeltjänster till ekonomin och samhället som helhet är skyldiga att vidta cybersäkerhetsåtgärder och rapportera incidenter i syfte att öka den övergripande cyberresiliensnivån på hela den inre marknaden.

För att ta itu med bristen på enhetlig motståndskraft mellan medlemsstater och sektorer är det särskilda målet att säkerställa att alla entiteter som är verksamma inom de sektorer som omfattas av den rättsliga ramen för NIS och som är av liknande storlek och har en jämförbar roll omfattas av samma regelverk (är antingen inom eller utanför tillämpningsområdet), oavsett vilken jurisdiktion de hör till inom EU.

För att säkerställa att alla entiteter som är verksamma inom sektorer täckta av NIS-ramen måste uppfylla samma skyldigheter grundade på konceptet riskhantering i fråga om säkerhetsåtgärder, och måste rapportera alla incidenter på grundval av en enhetlig uppsättning kriterier, är de särskilda målen att säkerställa att de behöriga myndigheterna tillämpar de regler som fastställs i det rättsliga instrumentet på ett effektivare sätt genom samordnade tillsyns- och verkställighetsåtgärder samt att säkerställa en jämförbar resursnivå i medlemsstaterna som

⁵⁶

I den mening som avses i artikel 58.2 a eller b i budgetförordningen.

gör det möjligt för de behöriga myndigheterna att fullgöra den kärnverksamhet som fastställs i NIS-ramen.

För att ta itu med problemet med gemensam situationsmedvetenhet och avsaknad av gemensam krishantering, är det särskilda målet att säkerställa att nödvändig information utbyts mellan medlemsstaterna genom att det införs tydliga skyldigheter för behöriga myndigheter att utbyta information och samarbeta när det gäller cyberhot och cyberincidenter och genom att det utvecklas gemensam operativ krishanteringsförmåga på unionsnivå.

1.4.3. Verkan eller resultat som förväntas

Beskriv den verkan som förslaget eller initiativet förväntas få på de mottagare eller den del av befolkningen som berörs.

Förslaget förväntas medföra betydande fördelar: Uppskattningar tyder på att det kan leda till en minskning av kostnaderna för cyberincidenter med 11,3 miljarder euro. Det sektoriella tillämpningsområdet skulle utvidgas avsevärt inom NIS-ramen, men utöver ovannämnda fördelar skulle den börda som kan skapas av nät- och informationssäkerhetskraven, särskilt ur tillsynssynpunkt, också balanseras för både de nya entiteter som ska omfattas och de behöriga myndigheterna. Detta beror på att den nya NIS-ramen skulle inrätta en tvåstegsstrategi, med fokus på stora entiteter och centrala entiteter och en differentiering av tillsynssystem som endast medger efterhandstillsyn för ett stort antal av dessa, särskilt de som anses vara ”viktiga” men ännu inte ”väsentliga”.

På det hela taget skulle förslaget leda till effektiva kompromisser och synergier, med den bästa potentialen av alla analyserade politiska alternativ för att säkerställa en ökad och konsekvent nivå av cyberresiliens hos centrala entiteter i hela unionen som så småningom skulle leda till kostnadsbesparingar för både företag och samhället.

Förslaget skulle också leda till vissa efterlevnads- och fullgörandekostnader för de berörda myndigheterna i medlemsstaterna (en total ökning på cirka 20–30 % av resurserna uppskattades). Den nya ramen skulle dock också medföra betydande fördelar genom en bättre överblick över och bättre samverkan med viktiga företag, förbättrat gränsöverskridande operativt samarbete samt mekanismer för ömsesidigt bistånd och sakkunnigbedömningar. Detta skulle leda till en generell ökning av cybersäkerhetskapaciteten i alla medlemsstater.

De företag som skulle omfattas av NIS-ramen uppskattas behöva öka sina nuvarande utgifter för IKT-säkerhet med högst 22 % under de första åren efter införandet av den nya NIS-ramen (detta skulle vara 12 % för företag som redan omfattas av det nuvarande NIS-direktivet). Denna genomsnittliga ökning av utgifterna för IKT-säkerhet skulle dock leda till en proportionell nytta av sådana investeringar, särskilt på grund av en betydande minskning av kostnaderna för cybersäkerhetsincidenter (uppskattningsvis 118 miljarder euro under tio år).

Små företag och mikroföretag skulle inte omfattas av NIS-ramens tillämpningsområde. För medelstora företag kan man förvänta sig en ökning av utgifterna för IKT-säkerhet under de första åren efter införandet av den nya NIS-ramen. Samtidigt skulle en höjning av säkerhetskraven för dessa entiteter också stimulera deras cybersäkerhetskapacitet och bidra till att förbättra deras IKT-riskhantering.

Medlemsstaternas budgetar och förvaltningar skulle påverkas på följande vis: En beräknad ökning på cirka 20–30 % av resurserna förväntas på kort och medellång sikt.

Inga andra betydande negativa konsekvenser förväntas. Förslaget förväntas leda till mer robust cybersäkerhetskapacitet och skulle följaktligen ha en mer betydande dämpande effekt på antalet incidenter och deras allvarlighetsgrad, inbegripet för dataintrång. Det kommer sannolikt också att ha en positiv inverkan på säkerställandet av lika villkor i medlemsstaterna för alla entiteter som omfattas av NIS-direktivets tillämpningsområde och minska asymmetrierna i fråga om information om cybersäkerhet.

1.4.4. Prestationsindikatorer

Ange indikatorer för övervakning av framsteg och resultat.

Bedömningen av indikatorerna kommer att utföras av kommissionen, med stöd av Enisa och samarbetsgruppen, med början tre år efter ikraftträdandet av den nya NIS-rättsakten. Följande är några av de övervakningsindikatorer utifrån vilka resultatet av NIS-granskningen skulle bedömas:

- **Förbättrad hantering av incidenter:** Genom att vidta cybersäkerhetsåtgärder förbättrar företagen inte bara sin förmåga att helt undvika vissa incidenter, utan också sin kapacitet att hantera incidenter. Mått på framgång är därför i) den genomsnittliga tid det tar att upptäcka en incident, ii) den genomsnittliga tid det tar för organisationer att återhämta sig från en incident, samt iii) den genomsnittliga kostnaden för en skada orsakad av en incident.
- **Ökad medvetenhet om cybersäkerhetsrisker bland företagens högsta ledning:** Genom att kräva att företag vidtar åtgärder skulle ett reviderat NIS-direktiv bidra till att öka medvetenheten på högsta ledningsnivå om cybersäkerhetsrelaterade risker. Detta kan mätas genom att undersöka i vilken utsträckning företag som omfattas av NIS-direktivet prioriterar cybersäkerhet i företagets interna policyer och processer, vilket framgår av intern dokumentation, relevanta utbildningsprogram och medvetandehöjande åtgärder för de anställda samt prioritering av säkerhetsrelaterade IKT-investeringar. Ledningen för alla väsentliga och viktiga entiteter bör också vara medveten om de regler som fastställs i NIS-direktivet.
- **Utgjämning av sektorsspecifika utgifter:** Utgifterna för IKT-säkerhet varierar avsevärt mellan olika sektorer i EU. Genom att kräva att företag i fler sektorer vidtar åtgärder bör avvikelser från de genomsnittliga sektorsspecifika utgifterna för IKT-säkerhet som en procentandel av de totala IKT-utgifterna minska mellan olika sektorer och mellan medlemsstaterna.
- **Starkare behöriga myndigheter och ökat samarbete:** Ett reviderat NIS-direktiv skulle eventuellt ge behöriga myndigheter ytterligare uppgifter. Detta skulle ha en mätbar inverkan på de finansiella och mänskliga resurser som avsatts för cybersäkerhetsbyråer på nationell nivå och bör också ha en positiv inverkan på de behöriga myndigheternas förmåga att proaktivt samarbeta och därmed öka antalet fall där de behöriga myndigheterna samverkar med varandra för att hantera gränsöverskridande incidenter eller att utföra gemensam tillsynsverksamhet.
- **Ökat informationsutbyte:** Det reviderade NIS-direktivet skulle också förbättra informationsutbytet mellan företag och med behöriga myndigheter. Ett av målen för översynen skulle kunna vara att öka antalet entiteter som deltar i de olika formerna av informationsutbyte.

1.5. Grunder för förslaget eller initiativet

1.5.1. *Krav som ska uppfyllas på kort eller lång sikt, inbegripet en detaljerad tidsplan för genomförandet av initiativet*

Förslaget syftar till att öka cyberresiliensen för ett stort antal företag med verksamhet i EU inom alla relevanta sektorer, minska bristen på enhetlighet för motståndskraften på den inre marknaden inom de sektorer som redan omfattas av direktivet och förbättra den gemensamma situationsmedvetenheten och den kollektiva förmågan att förbereda sig och reagera. Det kommer att bygga vidare på vad som har uppnåtts genom genomförandet av direktiv (EU) 2016/1148 under de senaste fyra åren.

- 1.5.2. *Mervärdet i unionens intervention (som kan följa av flera faktorer, t.ex. samordningsfördelar, rättssäkerhet, ökad effektivitet eller komplementaritet). Med "mervärdet i unionens intervention" i denna punkt avses det värde en åtgärd från unionens sida tillför utöver det värde som annars skulle ha skapats av enbart medlemsstaterna.*

Det kan inte finnas en effektiv motståndskraft mot cyberhot i unionen om frågan hanteras på olika sätt genom ett nationellt eller regionalt silotänkande. Syftet med NIS-direktivet var att hantera denna brist genom att fastställa en ram för säkerhet i nätverks- och informationssystem på en nationell nivå och på EU-nivå. Den första periodiska översynen av NIS-direktivet pekade dock på ett antal inneboende brister som så småningom skulle lett till betydande skillnader mellan medlemsstaterna i fråga om kapacitet, planering och skyddsnivå vilket också skulle påverkat lika villkor för liknande företag på den inre marknaden.

Ett EU-ingripande utöver de nuvarande åtgärderna i NIS-direktivet motiveras främst av följande skäl: i) problemets gränsoverskridande karaktär, ii) EU-åtgärdernas potential att förbättra och underlätta en effektiv nationell politik, och iii) bidraget av samordnade och samarbetsinriktade nät- och informationssäkerhetspolitiska åtgärder för ett effektivt skydd av personuppgifter och integritet.

De angivna målen kan därför bättre uppnås med hjälp av åtgärder på EU-nivå än av åtgärder vidtagna av de enskilda medlemsstaterna.

- 1.5.3. *Erfarenheter från tidigare liknande åtgärder*

NIS-direktivet är det första övergripande instrumentet för den inre marknaden som syftar till att förbättra motståndskraften mot cybersäkerhetsrisker hos nät och system i unionen. Direktivet har redan i hög grad bidragit till att höja den gemensamma nivån för cybersäkerhet bland medlemsstaterna sedan det trädde i kraft 2016. Översynen av direktivets funktion och genomförande har dock pekat på ett antal brister som, utöver den ökande digitaliseringen och behovet av mer aktuella svarsalternativ, måste hanteras i en reviderad rättsakt.

- 1.5.4. *Förenlighet med den fleråriga budgetramen och eventuella synergieffekter med andra relevanta instrument*

Det nya förslaget är helt förenligt med och överensstämmer med andra relaterade initiativ, såsom förslaget till förordning om digital operativ motståndskraft i finanssektorn samt förslaget till direktiv om motståndskraften hos kritiska leverantörer av samhällsviktiga tjänster. Det är också förenligt med den europeiska kodexen för elektronisk kommunikation, den allmänna dataskyddsförordningen och eIDA-förordningen.

Förslaget är en viktig del av EU:s strategi för en säkerhetsunion.

- 1.5.5. *En bedömning av de olika finansieringsalternativ som finns att tillgå, inbegripet möjligheter till omfördelning*

Enisas förvaltning av dessa uppgifter kräver särskilda profiler och ytterligare arbetsbelastning som inte kan absorberas utan ökade personalresurser.

1.6. Varaktighet för och budgetkonsekvenser av förslaget eller initiativet

☐ begränsad varaktighet

- ☐ Förslaget/initiativet har verkan från och med [den DD/MM]ÅÅÅÅ till och med [den DD/MM]ÅÅÅÅ
- ☐ Budgetkonsekvenser från och med ÅÅÅÅ till och med ÅÅÅÅ

☒ obegränsad varaktighet

- Efter en inledande period 2022–2025,
- beräknas genomförandetakten nå en stabil nivå.

1.7. Planerad metod för genomförandet⁵⁷

☒ Direkt förvaltning som sköts av kommissionen

genom

- ☐ genomförandeorgan

☐ Delad förvaltning med medlemsstaterna

☒ Indirekt förvaltning genom att uppgifter som ingår i budgetgenomförandet anförtros

☐ internationella organisationer och organ kopplade till dem (ange vilka)

☐ EIB och Europeiska investeringsfonden

☒ organ som avses i artiklarna 70 och 71

☐ offentligrättsliga organ

☐ privaträttsliga organ som har anförtrotts offentliga förvaltningsuppgifter i den utsträckning som de lämnar tillräckliga ekonomiska garantier

☐ organ som omfattas av privaträtten i en medlemsstat, som anförtrotts genomförandeuppgifter inom ramen för ett offentlig-privat partnerskap och som lämnar tillräckliga ekonomiska garantier

☐ personer som anförtrotts genomförandet av särskilda åtgärder inom Gusp enligt avdelning V i fördraget om Europeiska unionen och som fastställs i den relevanta grundläggande rättsakten

Anmärkningar

Europeiska unionens cybersäkerhetsbyrå Enisa, som har fått ett nytt permanent mandat genom cybersäkerhetsakten, skulle bistå medlemsstaterna och kommissionen i genomförandet av det reviderade NIS-direktivet.

Som ett resultat av det reviderade NIS-direktivet kommer Enisa från och med 2022/23 att ansvara för ytterligare åtgärdsområden. Dessa åtgärdsområden skulle omfattas av Enisas allmänna uppgifter i enlighet med dess mandat, men de kommer att leda till ytterligare arbetsbelastning för byrån. Enisa kommer närmare bestämt inom ramen för kommissionens förslag till ett reviderat NIS-direktiv att

⁵⁷

Närmare förklaringar av de olika metoderna för genomförande med hänvisningar till respektive bestämmelser i budgetförordningen återfinns på BudgWeb: <https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx>.

utöver sina nuvarande åtgärdsområden särskilt bland annat införliva följande uppgifter i sitt arbetsprogram: i) utveckla och underhålla ett europeiskt sårbarhetsregister (artikel 6.2 i förslaget), ii) tillhandahålla sekretariatet för Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe), (artikel 14 i förslaget), utfärda en årlig rapport om cybersäkerhetssituationen i unionen (artikel 15 i förslaget), iii) stödja anordnandet av sakkunnigbedömningar mellan medlemsstaterna (artikel 16 i förslaget), iv) samla in aggregerade uppgifter om incidenter från medlemsstaterna och utfärda teknisk vägledning (artikel 20.9 i förslaget), v) skapa och upprätthålla ett register över entiteter som tillhandahåller gränsöverskridande tjänster (artikel 25 i förslaget).

Därför kommer en begäran om ytterligare fem heltidsekvivalenter att göras från och med 2022 med motsvarande budget på omkring 0,61 miljoner euro för att täcka dessa nya poster.

2. FÖRVALTNING

2.1. Regler om uppföljning och rapportering

Ange intervall och andra villkor för sådana åtgärder:

Kommissionen kommer regelbundet att se över hur direktivet fungerar och rapportera till Europaparlamentet och rådet, första gången tre år efter direktivets ikraftträdande.

Kommissionen kommer också att utvärdera om medlemsstaterna har införlivat direktivet korrekt.

Uppföljningen och rapporteringen av förslaget kommer att följa de principer som anges i Enisas permanenta mandat enligt förordning (EU) 2019/881 (cybersäkerhetsakten).

De datakällor som används för den planerade uppföljningen skulle till största delen komma från Enisa, samarbetsgruppen, CSIRT-nätverket och medlemsstaternas myndigheter. Utöver uppgifterna i rapporterna (inklusive de årliga verksamhetsrapporterna) från Enisa, samarbetsgruppen och CSIRT-nätverket, kan särskilda verktyg för uppgiftsinsamling vid behov användas (t.ex. enkäter till de nationella myndigheterna, Eurobarometern, rapporter från ”månaden för cybersäkerhet”-kampanjen och EU-omfattande övningar).

2.2. Förvaltnings- och kontrollsystem

2.2.1. *Motivering av den genomförandemetod, de finansieringsmekanismer, de betalningsvillkor och den kontrollstrategi som föreslås*

Den enhet inom GD CNECT som ansvarar för politikområdet kommer att ansvara för genomförandet av direktivet.

När det gäller Enisas förvaltning innehåller artikel 15 i cybersäkerhetsakten en detaljerad förteckning över kontrollfunktionerna för Enisas styrelse.

Enligt artikel 31 i cybersäkerhetsakten är den verkställande direktören ansvarig för att Enisas budget genomförs och kommissionens internrevisor har samma befogenheter gentemot Enisa som gentemot kommissionens avdelningar. Enisas styrelse avger ett yttrande om Enisas slutliga räkenskaper.

2.2.2. *Uppgifter om identifierade risker och om det eller de interna kontrollsystem som inrättats för att begränsa riskerna*

Mycket låg risk, eftersom ekosystemet för NIS redan finns och redan omfattar Enisa, som har ett permanent mandat efter ikraftträdandet av cybersäkerhetsakten 2019.

2.2.3. *Beräkning och motivering av kontrollernas kostnadseffektivitet (dvs. förhållandet mellan kostnaden för kontrollerna och värdet av de medel som förvaltas) och en bedömning av den förväntade risken för fel (vid betalning och vid avslutande)*

Den begärda budgetökningen gäller avdelning 1 och är avsedd att finansiera löner. Detta innebär en mycket låg risk för fel på betalningsnivå.

2.3. Åtgärder för att förebygga bedrägeri och oriktigheter

Beskriv förebyggande åtgärder (befintliga eller planerade), t.ex. från strategi för bedrägeribekämpning.

Enisas förebyggande åtgärder och skyddsåtgärder skulle vara tillämpliga, särskilt följande:

- Betalningar för beställda tjänster eller undersökningar ska kontrolleras av byrån innan utbetalningen görs, med beaktande av villkoren i avtalen, ekonomiska principer samt god ekonomisk och administrativ sed. Åtgärder för bedrägeribekämpning (övervakning, rapporteringskrav osv.) kommer att ingå i alla avtal och kontrakt mellan byrån och dess betalningsmottagare.

- Bestämmelserna i Europaparlamentets och rådets förordning (EG) nr 883/2013 av den 25 maj 1999 om utredningar som utförs av Europeiska byrån för bedrägeribekämpning (Olaf) ska tillämpas fullt ut i syfte att bekämpa bedrägerier, korruption och annan olaglig verksamhet.

- I enlighet med artikel 33 av cybersäkerhetsakten ska Enisa senast den 28 december 2019 ansluta sig till det interinstitutionella avtalet av den 25 maj 1999 mellan Europaparlamentet, Europeiska unionens råd och Europeiska gemenskapernas kommission om interna utredningar som utförs av Europeiska byrån för bedrägeribekämpning (Olaf). Enisa ska utan dröjsmål utfärda lämpliga bestämmelser som är tillämpliga på alla anställda vid byrån.

3. BERÄKNADE BUDGETKONSEKVENSER AV FÖRSLAGET ELLER INITIATIVET

3.1. Berörda rubriker i den fleråriga budgetramen och budgetrubriker i den årliga budgetens utgiftsdel

- Befintliga budgetrubriker (även kallade ”budgetposter”)

Redovisa enligt de berörda rubrikerna i den fleråriga budgetramen i nummerföljd.

Rubrik i den fleråriga budgetramen	Budgetrubrik	Typ av utgifter	Bidrag			
	Nummer		från Efta-länder ⁵⁹	från kandidat-länder ⁶⁰	från tredje-länder	enligt artikel 21.2 b i budgetförordningen
2	02 10 04	/Icke-diff.	JA	NEJ	NEJ	/NEJ

- Nya budgetrubriker som föreslås

Redovisa enligt de berörda rubrikerna i den fleråriga budgetramen i nummerföljd.

Rubrik i den fleråriga budgetramen	Budgetrubrik	Typ av anslag	Bidrag			
	Nummer		från Efta-länder	från kandidat-länder	från tredje-länder	enligt artikel 21.2 b i budgetförordningen

⁵⁸ Diff. = differentierade anslag/Icke-diff. = icke-differentierade anslag.

⁵⁹ Efta: Europeiska frihandelssammanslutningen.

⁶⁰ Kandidatländer och i förekommande fall potentiella kandidatländer i västra Balkan.

	[XX.YY.YY.YY]		JA/NEJ	JA/NEJ	JA/NEJ	JA/NEJ
--	---------------	--	--------	--------	--------	--------

3.2. Beräknad inverkan på utgifter

3.2.1. Sammanfattning av den beräknade inverkan på utgifterna

Miljoner euro (avrundat till tre decimaler)

Rubrik i den fleråriga budgetramen	Nummer	[Rubrik...2 Inre marknaden, innovation och den digitala ekonomin.....]
------------------------------------	--------	--

[Organ]: <...ENISA....>			År N ⁶¹ 2022	År N+1 2023	År N+2 2024	År N+3 2025	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6) 2026 2027			TOTALT
Avdelning 1:	Åtaganden	(1)	0,61	0,61	0,61	0,61	0,61	0,61		3,66
	Betalningar	(2)	0,61	0,61	0,61	0,61	0,61	0,61		3,66
Avdelning 2:	Åtaganden	(1a)								
	Betalningar	(2 a)								
Avdelning 3:	Åtaganden	(3 a)								
	Betalningar	(3b)								
TOTALA anslag för [organ] <ENISA.....>	Åtaganden	=1+1a +3a	0,61	0,61	0,61	0,61	0,61	0,61		3,66
	Betalningar	=2+2a +3b	0,61	0,61	0,61	0,61	0,61	0,61		3,66

⁶¹ Med år N avses det år då förslaget eller initiativet ska börja genomföras. Ersätt ”N” med det förväntade första genomförandeåret (till exempel 2021). Detsamma för följande år.

Rubrik i den fleråriga budgetramen	5	”Administrativa utgifter”
---	----------	----------------------------------

Miljoner euro (avrundat till tre decimaler)

		År N	År N+1	År N+2	År N+3	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)		TOTALT
GD: <.....>								
• Personalresurser								
• Övriga administrativa utgifter								
GD TOTALT <....>	Anslag							

TOTALA anslag för RUBRIK 5 i den fleråriga budgetramen	(summa åtaganden = summa betalningar)								
---	--	--	--	--	--	--	--	--	--

Miljoner euro (avrundat till tre decimaler)

		År N ⁶² 2022	År N+1 2023	År N+2 2024	År N+3 2025	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6) 2026 2027		TOTALT
TOTALA anslag för RUBRIK 1 till 5 i den fleråriga budgetramen	Åtaganden	0,61	0,61	0,61	0,61	0,61	0,61	3,66
	Betalningar	0,61	0,61	0,61	0,61	0,61	0,61	3,66

⁶² Med år N avses det år då förslaget eller initiativet ska börja genomföras. Ersätt ”N” med det förväntade första genomförandeåret (till exempel 2021). Detsamma för följande år.

3.2.2. Beräknad inverkan på [organets] anslag

- ☐x Förslaget/initiativet kräver inte att driftsanslag tas i anspråk
- ☐ Förslaget/initiativet kräver att driftsanslag tas i anspråk enligt följande:

Åtagandebemyndiganden i miljoner euro (avrundat till tre decimaler)

Ange mål och output ⇓			År N	År N+1	År N+2	År N+3	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)										TOTALT	
	OUTPUT																	
	Typ ⁶³	Genomsnittliga kostnader	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Antal	Kostn.	Totalt antal	Totala kostnader
SPECIFIKT MÅL nr 1 ⁶⁴ ...																		
- Output																		
- Output																		
- Output																		
Delsumma för specifikt mål nr 1																		
SPECIFIKT MÅL nr 2...																		
- Output																		
Delsumma för specifikt mål nr 2																		
TOTALA KOSTNADER																		

⁶³ Output som ska anges är de produkter eller tjänster som levererats (t.ex. antal studentutbyten som har finansierats eller antal kilometer väg som har byggts).
⁶⁴ Mål som redovisats under punkt 1.4.2: "Specifikt/specifika mål...".

3.2.3. Beräknad inverkan på Enisas personalresurser

3.2.3.1. Sammanfattning

Som ett resultat av det reviderade NIS-direktivet kommer Enisa från och med 2022/23 att ha ytterligare uppgifter. Dessa uppgifter skulle omfattas av Enisas mandat, men de kommer att leda till ytterligare arbetsbelastning för byrån. Närmare bestämt skulle Enisa enligt kommissionens förslag till ett reviderat NIS-direktiv få i uppgift att bland annat i) utveckla och underhålla ett europeiskt sårbarhetsregister (artikel 6.2), ii) tillhandahålla sekretariatet för Europeiska kontaktnätverket för cyberkriser (EU-CyCLONe), (artikel 14), utfärda en årlig rapport om cybersäkerhetssituationen i unionen (artikel 15), iii) stödja anordnandet av sakkunnigbedömningar mellan medlemsstaterna (artikel 16), iv) samla in aggregerade uppgifter om incidenter från medlemsstaterna och utfärda teknisk vägledning (artikel 20.9), v) skapa och upprätthålla ett register över entiteter som tillhandahåller gränsöverskridande tjänster (artikel 25).

Därför kommer en begäran om ytterligare fem heltidsekvivalenter att göras från och med 2022 med motsvarande budget för att täcka dessa nya poster.

- ☐ Förslaget/initiativet kräver inte att anslag av administrativ natur tas i anspråk
- ☒ Förslaget/initiativet kräver att anslag av administrativ natur tas i anspråk enligt följande:

Miljoner euro (avrundat till tre decimaler)

	År N ⁶⁵ 2022	År N+1 2023	År N+2 2024	År N+3 2025	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)		TOTALT
	2026	2027					

Tillfälligt anställda (AD-tjänster)	0,450	0,450	0,450	0,450	0,450	0,450		2,7
Tillfälligt anställda (AST-tjänster)								
Kontraktsanställda	0,160	0,160	0,160	0,160	0,160	0,160		0,96
Nationella experter								

TOTALT	0,61	0,61	0,61	0,61	0,61	0,61		3,66
---------------	-------------	-------------	-------------	-------------	-------------	-------------	--	-------------

Personalbehov (i heltidsekvivalenter):

⁶⁵

Med år N avses det år då förslaget eller initiativet ska börja genomföras. Ersätt "N" med det förväntade första genomförandeåret (till exempel 2021). Detsamma för följande år.

	År N ⁶⁶ 2022	År N+1 2023	År N+2 2024	År N+3 2025	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)		TOTALT
					2026	2027	

Tillfälligt anställda (AD-tjänster)	3	3	3	3	3	3	18
Tillfälligt anställda (AST-tjänster)							
Kontraktсанställda	2	2	2	2	2	2	12
Nationella experter							

TOTALT	5	5	5	5	5	5	30
--------	---	---	---	---	---	---	----

3.2.3.2. Beräknat personalbehov för det ansvariga generaldirektoratet

- ☐ Förslaget/initiativet kräver inte att personalresurser tas i anspråk
- ☐ Förslaget/initiativet kräver att personalresurser tas i anspråk enligt följande:

Beräkningarna ska anges i heltal (eller med högst en decimal)

	År N	År N+1	År N+2	År N+3	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)		
• Tjänster som tas upp i tjänsteförteckningen (tjänstemän och tillfälligt anställda)							
XX 01 01 01 (vid huvudkontoret eller vid kommissionens kontor i medlemsstaterna)							
XX 01 01 02 (vid delegationer)							
XX 01 05 01 (indirekta forskningsåtgärder)							
10 01 05 01 (direkta forskningsåtgärder)							

⁶⁶

Med år N avses det år då förslaget eller initiativet ska börja genomföras. Ersätt ”N” med det förväntade första genomförandeåret (till exempel 2021). Detsamma för följande år.

• Extern personal (i heltidsekvivalenter)⁶⁷								
XX 01 02 01 (kontraktsanställda, nationella experter och vikarier finansierade genom ramanslaget)								
XX 01 02 02 (kontraktsanställda, lokalanställda, nationella experter, vikarier och unga experter som tjänstgör vid delegationerna)								
XX 01 04 yy⁶⁸	- vid huvudkontoret ⁶⁹							
	- vid delegationer							
XX 01 05 02 (kontraktsanställda, nationella experter och vikarier som arbetar med indirekta forskningsåtgärder)								
10 01 05 02 (kontraktsanställda, vikarier och nationella experter som arbetar med direkta forskningsåtgärder)								
Annan budgetrubrik (ange vilken)								
TOTALT								

XX motsvarar det politikområde eller den avdelning i budgeten som avses.

Personalbehoven ska täckas med personal inom generaldirektoratet vilka redan har avdelats för förvaltningen av åtgärden i fråga, eller genom en omfördelning av personal inom generaldirektoratet, om så krävs kompletterad med ytterligare resurser som kan tilldelas det förvaltande generaldirektoratet som ett led i det årliga förfarandet för tilldelning av anslag och med hänsyn tagen till begränsningar i fråga om budgetmedel.

Beskrivning av arbetsuppgifter:

Tjänstemän och tillfälligt anställda	
Extern personal	

En beskrivning av beräkningen av kostnaden för heltidsekvivalenterna bör införas i avsnitt 3 i bilaga V.

⁶⁷ [I denna fotnot förklaras vissa initialförkortningar som inte används i den svenska versionen]
⁶⁸ Särskilt tak för finansiering av extern personal genom driftsanslag (tidigare s.k. BA-poster).
⁶⁹ Huvudsakligen för strukturfonderna, Europeiska jordbruksfonden för landsbygdsutveckling (Ejflu), och Europeiska fiskerifonden (EFF).

3.2.4. Förenlighet med den gällande fleråriga budgetramen

- ☒ Förslaget/initiativet är förenligt med den gällande fleråriga budgetramen.
- ☐ Förslaget/initiativet kräver omfördelningar under den berörda rubriken i den fleråriga budgetramen.

Förklara i förekommande fall vilka omfördelningar som krävs, och ange berörda budgetrubriker och motsvarande belopp.

Förslaget är förenligt med den fleråriga budgetramen 2021–2027.

Kompensationen av den budget som begärs för att täcka Enisas ökade personalresurser kommer att göras genom att budgeten för programmet för ett digitalt Europa minskas med samma belopp under samma rubrik.

- ☐ Förslaget/initiativet kräver tillämpning av flexibilitetsinstrumentet eller revidering av den fleråriga budgetramen⁷⁰.

Beskriv behovet av sådana åtgärder, och ange berörda rubriker i budgetramen, budgetrubriker i den årliga budgeten samt de motsvarande beloppen.

3.2.5. Bidrag från tredje part

- Det ingår inga bidrag från tredje parter i det aktuella förslaget eller initiativet
- Förslaget eller initiativet kommer att medfinansieras enligt följande:

Miljoner euro (avrundat till tre decimaler)

	År N	År N+1	År N+2	År N+3	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)			Totalt
Ange vilket organ som deltar i samfinansieringen								
TOTALA anslag som tillförs genom samfinansiering								

⁷⁰

Se artiklarna 11 och 17 i rådets förordning (EU, Euratom) nr 1311/2013 om den fleråriga budgetramen för 2014–2020

3.3. Beräknad inverkan på inkomsterna

- ☐ Förslaget/initiativet påverkar inte budgetens inkomstsida.
- ☐ Förslaget/initiativet påverkar inkomsterna på följande sätt:
 - ☐ påverkan på egna medel
 - ☐ påverkan på andra inkomster
 - ☐ ange om inkomsterna har avsatts för utgiftsposter

Miljoner euro (avrundat till tre decimaler)

Budgetrubrik i den årliga budgetens inkomstsidan:	Belopp som förts in för det innevarande budgetåret	Förslaget/initiativets inverkan på inkomsterna ⁷¹						
		År N	År N+1	År N+2	År N+3	För in så många år som behövs för att redovisa varaktigheten för inverkan på resursanvändningen (jfr punkt 1.6)		
Artikel								

Ange vilka budgetrubriker i utgiftsdelen som berörs i de fall där inkomster i diversekategorin kommer att avsättas för särskilda ändamål.

--

Ange med vilken metod inverkan på inkomsterna har beräknats.

--

⁷¹

Vad gäller traditionella egna medel (tullar, sockeravgifter) ska nettobeloppen anges, dvs. bruttobeloppen minus 20 % avdrag för uppbördskostnader.