Europeiska unionens råd

Bryssel den 14 september 2017
(OR. en)

12183/17

Interinstitutionellt ärende:
2017/0225 (COD)

CYBER 127
TELECOM 207
ENFOPOL 410
CODEC 1397
JAI 785
MI 627
IA 139

FÖRSLAG

från:	Jordi AYET PUIGARNAU, direktör, för Europeiska kommissionens generalsekreterare
till:	Jeppe TRANHOLM-MIKKELSEN, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	COM(2017) 477 final
Ärende:	Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”)

För delegationerna bifogas dokument – COM(2017) 477 final.

Bilaga: COM(2017) 477 final

EUROPEISKA
KOMMISSIONEN

Bryssel den 4.10.2017
COM(2017) 477 final

2017/0225 (COD)

NOTE
This language version reflects the corrections done to the original EN version transmitted under COM(2017) 477 final of 13.9.2017 and retransmitted (with corrections) under COM(2017) 477 final/2 of 4.10.2017

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”)

(Text av betydelse för EES)

{SWD(2017) 500 final}
{SWD(2017) 501 final}
{SWD(2017) 502 final}

MOTIVERING

1. BAKGRUND TILL FÖRSLAGET

• Motiv och syfte med förslaget

Europeiska unionen har vidtagit en rad åtgärder på cybersäkerhetsområdet för att öka resiliensen och beredskapen. Den första EU-strategin för cybersäkerhet[1] antogs 2013. I den fastställs strategiska mål och konkreta åtgärder för att uppnå resiliens, minska cyberbrottsligheten, utveckla politiken och kapaciteteten på cyberförsvarsområdet, utveckla industriresurser och teknologiska resurser, och upprätta en sammanhängande internationell policy för cybersäkerhet för EU. Sedan dess har det skett viktiga förändringar på området, särskilt inledningen av det andra mandatet för Europeiska unionens byrå för nät- och informationssäkerhet (Enisa)[2], och antagandet av **direktivet om säkerhet i nätverks- och informationssystem**[3] (nedan kallat *it-säkerhetsdirektivet*), som ligger till grund för det här förslaget.

Dessutom **antog Europeiska kommissionen under 2016 meddelandet Stärka Europas system för cyberresiliens och främja en konkurrenskraftig och innovativ cybersäkerhetsbransch**[4], där den tillkännager ytterligare åtgärder för att intensifiera samarbetet och informations- och kunskapsutbytet och öka EU:s resiliens och beredskap, även med hänsyn tagen till möjligheten av storskaliga incidenter och en eventuell europaomfattande cyberkris. I samband med det lät kommissionen meddela att den skulle tidigarelägga **utvärderingen** och **översynen** av Europaparlamentets och rådets förordning (EU) nr 526/2013 om Enisa och om upphävande av förordning (EG) nr 460/2004 (nedan kallad *Enisa-förordningen*). Utvärderingen kan leda till en reform av Enisa och en ökning av Enisas förmåga att stödja medlemsstaterna på ett hållbart sätt. Enisa skulle därför ges en mer operativ och central roll i arbetet med att skapa cyberresiliens, och de nya ansvarsområdena enligt it-säkerhetsdirektivet skulle bekräftas i det nya mandatet.

It-säkerhetsdirektivet var ett första viktigt steg för att främja en riskhanteringskultur genom att det inför säkerhetskrav som utgör rättsliga skyldigheter för de centrala ekonomiska aktörerna, särskilt de operatörer som tillhandahåller samhällsviktiga tjänster (nedan kallade *leverantörer av samhällsviktiga tjänster*) och de operatörer som tillhandahåller vissa viktiga digitala tjänster (nedan kallade *leverantörer av digitala tjänster*). Med tanke på att säkerhetskraven anses vara viktiga för att slå vakt om fördelarna med den växande digitaliseringen av samhället, och med tanke på den snabba spridningen av enheter med internetuppkoppling (sakernas internet), föreslog man i 2016 års meddelande att det ska upprättas en ram för säkerhetscertifiering av IKT-produkter och IKT-tjänster i syfte att öka förtroendet och säkerheten på den digitala inre marknaden. IKT-cybersäkerhetscertifiering framstår som särskilt relevant mot bakgrund av den ökade användningen av teknik som kräver en hög nivå av cybersäkerhet, såsom uppkopplade och automatiserade bilar och industriella automatiseringskontrollsystem (IACS).

---

1 Gemensamt meddelande från Europeiska kommissionen och Europeiska avdelningen för yttre åtgärder: EU:s strategi för cybersäkerhet: En öppen, säker och trygg cyberrymd (JOIN(2013).

2 Förordning (EU) nr 526/2013 om Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) och om upphävande av förordning (EG) nr 460/2004.

3 Direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

4 Meddelande från kommissionen: Stärka Europas system för cyberresiliens och främja en konkurrenskraftig och innovativ cybersäkerhetsbransch, COM(2016) 0410 slutlig.

Dessa politiska åtgärder och tillkännagivanden gavs ytterligare tyngd genom **rådets slutsatser** från 2016 där det konstaterades att ”de cyberrelaterade hoten och sårbarheterna fortsätter att utvecklas och blir intensivare, vilket kräver ett fortsatt och närmare samarbete, särskilt vad gäller att hantera gränsöverskridande storskaliga cybersäkerhetsincidenter”. I slutsatserna bekräftas att ”Enisa-förordningen utgör en av de centrala delarna av en EU-ram för cyberresiliens”[5], och kommissionen uppmanas att vidta ytterligare åtgärder för att ta itu med frågan om certifiering på EU-nivå.

Inrättandet av ett certifieringssystem skulle kräva att det även inrättas ett lämpligt styrningssystem på EU-nivå, inklusive tillhandahållande av djupgående sakkunskap från ett oberoende EU-organ. I det hänseendet fastställs i det här förslaget att Enisa är det EU-organ med behörighet i cybersäkerhetsfrågor som är bäst lämpat att ikläda sig rollen att sammanföra och samordna arbetet inom de nationella behöriga organen på certifieringsområdet.

Dessutom angav kommissionen i sitt **meddelande från maj 2017 om halvtidsöversynen av strategin för den digitala inre marknaden** att den senast i september 2017 ska se över Enisas mandat för att definiera dess roll i det förändrade cybersäkerhetslandskapet och ta fram förslag på standarder, certifiering och märkning på cybersäkerhetsområdet i syfte att göra IKT-baserade system, inklusive uppkopplade föremål, cybersäkrare[6]. I **slutsatserna från Europeiska rådets möte** i juni 2017[7] välkomnades kommissionens avsikt att se över EU:s strategi för cybersäkerhet i september och att föreslå ytterligare riktade åtgärder före utgången av 2017.

I förslaget till förordning fastställs en omfattande uppsättning åtgärder som bygger på tidigare åtgärder och främjar specifika ömsesidigt förstärkande mål:

- Öka medlemsstaternas och företagens **kapacitet och beredskap**.
- Förbättra **samarbetet och samordningen** mellan medlemsstaterna och EU:s institutioner, byråer och organ.
- Öka **EU:s förmåga att komplettera medlemsstaternas åtgärder**, i synnerhet när det gäller gränsöverskridande cyberkriser.
- Öka allmänhetens och företagens **medvetenhet** om cybersäkerhetsfrågor.
- Öka den övergripande **transparensen i fråga om assuransnivån för cybersäkerhet**[8] hos IKT-produkter och IKT-tjänster i syfte att stärka förtroendet för den digitala inre marknaden och för digital innovation. och
- Undvika en **uppsplittring av certifieringssystemen** i EU och av de tillhörande säkerhetskraven och utvärderingskriterierna i de olika medlemsstaterna och sektorerna.

---

5 Rådets slutsatser om att stärka Europas system för cyberresiliens och främja en konkurrenskraftig och innovativ cybersäkerhetsbransch – 15 november 2016.

6 Meddelande från kommission om halvtidsöversynen av genomförandet av strategin för den digitala inre marknaden, COM(2017) 228.

7 Europeiska rådets möte (22–23 juni 2017) – slutsatser, EUCO 8/17.

8 Med transparens i fråga om assuransnivån för cybersäkerhet avses att ge användarna tillräcklig information om cybersäkerhetsegenskaperna hos en viss IKT-produkt, IKT-tjänst eller IKT-process, så att de objektivt kan fastställa cybersäkerhetsnivån hos denna IKT-produkt, IKT-tjänst eller IKT-process.

I följande del av motiveringen lämnas en mer detaljerad redogörelse för skälen bakom initiativet när det gäller de föreslagna åtgärderna rörande Enisa och cybersäkerhetscertifiering.

Enisa

Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) agerar expertcentrum med uppgift att förbättra nät- och informationssäkerheten inom unionen och stödja kapacitetsuppbyggnaden i medlemsstaterna.

Den inrättades 2004[9] med syftet att bidra till målet att säkerställa en hög nivå på nät- och informationssäkerheten i EU. Genom förordning (EU) nr 526/2013 fastställdes under 2013 Enisas nya mandat för en period av sju år, fram till 2020. Enisa har sitt säte i Grekland, med förvaltningen i Heraklion (Kreta) och kärnverksamheten i Aten.

Enisa är en liten byrå med begränsad budget och personalstyrka jämfört med övriga EU-organ. Den har ett tidsbegränsat mandat.

Enisa stöder de europeiska institutionerna, medlemsstaterna och näringslivet i arbetet med att **lösa, åtgärda och i synnerhet förebygga nät- och informationssäkerhetsproblem**. Den gör detta genom en rad åtgärder inom fem områden som fastställs i dess strategi[10]:

- Sakkunskap: Tillhandahålla information och sakkunskap om viktiga nät- och informationssäkerhetsfrågor.
- Politik: Bistå vid beslutsfattande och genomförande av politiken i unionen.
- Kapacitet: Stödja kapacitetsuppbyggnaden i hela unionen (genom t.ex. utbildning, rekommendationer och informationskampanjer).
- Gemenskapsbyggande: Bygga gemenskap inom området nät- och informationssäkerhet (t.ex. stöd till incidenthanteringsorganisationerna (CERT) och samordning av paneuropeiska cyberövningar).
- Möjliggörande (t.ex. samarbete med intressenterna och internationella förbindelser).

I samband med förhandlingarna om it-säkerhetsdirektivet beslutade EU:s medlagstiftare att Enisa skulle ges en viktig roll vid genomförandet av det här direktivet. I synnerhet tillhandahåller Enisa sekretariatstjänster för CSIRT-nätverket (som inrättats för att främja snabbt och effektivt operativt samarbete mellan medlemsstaterna kring specifika cybersäkerhetsincidenter och spridning av information om risker), och den ska också bistå samarbetsgruppen i utförandet av dess uppgifter. I direktivet föreskrivs också att Enisa ska bistå medlemsstaterna och kommissionen genom att tillhandahålla sakkunskap och rådgivning och genom att underlätta utbyte av bästa praxis.

I enlighet med Enisa-förordningen har kommissionen genomfört en utvärdering av Enisa som omfattar en oberoende undersökning och ett offentligt samråd. Vid utvärderingen bedömdes Enisas relevans, genomslagskraft, ändamålsenlighet, effektivitet, samstämmighet och europeiska mervärde med avseende på dess resultat, styrning, interna organisation och arbetsmetoder under perioden 2013–2016.

En majoritet av de svarande[11] i det offentliga samrådet (74 %) gav en positiv bedömning av Enisas övergripande resultatet. En majoritet av de svarande ansåg dessutom att Enisa uppnår

---

9 Europaparlamentets och rådets förordning (EG) nr 460/2004 av den 10 mars 2004 om inrättandet av den europeiska byrån för nät- och informationssäkerhet (EUT L 77, 13.3.2004, s. 1).

10 https://www.enisa.europa.eu/publications/corporate/enisa-strategy

sina olika mål (minst 63 % för vart och ett av målen). Enisas tjänster och produkter används regelbundet (varje månad eller oftare) av nästan hälften av de svarande (46 %), som uppskattar det faktum att de härrör från ett organ på EU-nivå (83 %) och är av god kvalitet (62 %).

En stor majoritet (88 %) av de svarande ansåg att den nuvarande instrumentet och mekanismerna på EU-nivå är otillräckliga eller endast delvis ändamålsenliga när det gäller att lösa de nuvarande cybersäkerhetsutmaningarna. En stor majoritet av de svarande (98 %) angav att ett EU-organ bör tillgodose dessa behov, och av dessa ansåg 99 % att Enisa utgör det rätta organet. Dessutom ansåg 67,5 % av de svarande att Enisa skulle kunna hjälpa till att skapa en harmoniserad ram för säkerhetscertifiering av it-produkter och it-tjänster.

I den övergripande utvärderingen (som inte endast bygger på det offentliga samrådet, utan även på ett antal enskilda intervjuer, kompletterande riktade enkäter och workshopar) drogs följande slutsatser:

- Enisas mål är fortfarande relevanta i dag. Mot bakgrund av den snabba tekniska utvecklingen, de framväxande hoten och de växande globala cybersäkerhetsriskerna finns ett klart behov i EU av att främja och ytterligare stärka den tekniska sakkunskapen på hög nivå om cybersäkerhetfrågor. Medlemsstaterna behöver öka sin förmåga att förstå och bemöta hot, och intressenterna måste samarbeta inom olika tematiska områden och institutionerna emellan.
- Trots en begränsad budget har Enisa varit operativt effektiv i att utnyttja sina resurser och genomföra sina uppgifter. Uppdelningen av Enisa mellan Aten och Heraklion har emellertid medfört extra administrativa kostnader.
- När det gäller ändamålsenligheten har Enisa delvis nått målen. Byrån bidrog framgångsrikt till att förbättra nät- och informationssäkerheten i Europa genom att erbjuda kapacitetsuppbyggnad i 28 medlemsstater[12], fördjupa samarbetet mellan medlemsstaterna och intressenterna inom området nät- och informationssäkerhet, och genom att bidra med sakkunskap, göra gemenskapsbyggande insatser och ge stöd till utvecklingen av politiken. Överlag lade Enisa stort fokus vid att genomföra sitt arbetsprogram och var en tillförlitlig partner för sina intressenter, inom ett område vars stora gränsöverskridande betydelse först nyligen har erkänts.
- Enisas arbete har fått genomslag, åtminstone i viss utsträckning, inom det vidsträckta området nät- och informationssäkerhet, men byrån har ännu inte lyckats utveckla ett tillräckligt starkt varumärke och få tillräcklig synlighet för att bli erkänd som det ”officiella” expertcentrumet på området i Europa. Förklaringen till detta ligger i

---

11 I samrådet deltog 90 berörda parter från 19 medlemsstater (88 svar och 2 ståndpunktsdokument), varav nationella myndigheter från 15 medlemsstater och 8 paraplyorganisationer som företräder ett stort antal europeiska företag.

12 Deltagarna i det offentliga samrådet ombads lämna en kommentar till vad de ansåg vara det viktigaste Enisa åstadkommit under perioden 2013–2016. De svarande från alla grupper (sammanlagt 55, varav 13 från nationella myndigheter, 20 från den privata sektorn och 22 från ”övriga”) ansåg att Enisas viktigaste resultat utgjordes av följande: 1) Samordning av Cyber Europe-insatserna. 2) Stöd till CERT/CSIRT-enheter genom utbildning och workshoppar för att främja samordning och utbyte. 3) Enisas publikationer (riktlinjer, rekommendationer, rapporter om hotbild, strategier för incidentrapportering och krishantering m.m.), som ansågs användbara för att skapa och uppdatera nationella säkerhetsramar och som referens för beslutsfattare och yrkesverksamma på cyberområdet. 4) Hjälp med att främja it-säkerhetsdirektivet. 5) Insatser för att öka medvetenheten om cybersäkerhet genom Europeiska månaden för cybersäkerhet.

Enisas breda mandat, som inte står i proportion till de tilldelade medlen. Dessutom är Enisa den enda EU-byrån med ett tidsbegränsat mandat, vilket begränsar dess förmåga att utveckla en långsiktig vision och stödja sina intressenter på ett hållbart sätt. Detta står också i skarp motsats till bestämmelserna i it-säkerhetsdirektivet, där byrån tilldelas uppgifter som inte är tidsbegränsade. Slutligen konstaterades det i bedömningen att denna begränsade ändamålsenlighet delvis kan förklaras med det stora beroendet av extern sakkunskap relativt intern sakkunskap och att det är svårt att rekrytera och behålla specialiserad personal.

- Sist med inte minst konstaterades det i utvärderingen att Enisas mervärde särskilt ligger i dess förmåga att stärka samarbetet mellan främst medlemsstaterna och i synnerhet med de berörda nät- och informationssäkerhetsorganen (speciellt mellan olika CSIRT-enheter). Det finns ingen annan aktör på EU-nivå som stöder så många typer av intressenter på området nät- och informationssäkerhet. På grund av behovet av en noggrann prioritering av Enisas verksamhet styrs Enisas arbetsprogram främst av medlemsstaternas behov. Som en följd av detta tillgodoses inte intressenters behov i tillräcklig hög grad, i synnerhet näringslivets. Det har också medfört att byrån är inriktad mot att tillgodose de viktigaste intressenternas behov, vilket hindrar den från att få större genomslag. Därför varierade byråns tillförda mervärde i förhållande till de olika intressenternas behov och till i vilken utsträckning som byrån hade möjlighet att reagera på dem (t.ex. stora kontra små medlemsstater och medlemsstater kontra näringsliv).

Sammanfattningsvis antydde resultaten av samrådet med intressenterna och utvärderingen att Enisas resurser och mandat måste anpassas så att de på ett adekvat sätt kan bidra till att möta nuvarande och framtida utmaningar.

Med beaktande av ovanstående rymmer det här förslaget en översyn av Enisas nuvarande mandat och en ny uppsättning uppgifter och funktioner med målet att på ett verksamt och effektivt sätt stödja medlemsstaternas, EU-institutionernas och andra intressenters ansträngningar att säkerställa en trygg cyberrymd i Europeiska unionen. Syftet med det nya mandatet är att ge byrån en tydligare och mer central roll, särskilt genom att det föreslås att den även stödjer medlemsstaterna när det gäller genomförandet av it-säkerhetsdirektivet och bemöter specifika hot mer aktivt (operativ kapacitet) och att den blir ett expertcentrum som bistår medlemsstaterna och kommissionen vid cybersäkerhetscertifiering. Förslaget innehåller bland annat följande:

- Enisa beviljas ett permanent mandat och får därigenom en stabil grund att stå på inför framtiden. Mandatet, målen och uppgifterna ska dock fortfarande regelbundet ses över.
- Det föreslagna mandatet förtydligar ytterligare Enisas roll, att vara EU:s cybersäkerhetsbyrå och referenspunkt i EU:s cybersäkerhetslandskap och verka i nära samarbete med alla andra relevanta organ i cybersäkerhetslandskapet.
- Byråns organisation och styrning, som gavs ett positivt omdöme vid utvärderingen, blir föremål för en måttlig översyn, i synnerhet för att se till att behoven hos intressenterna i stort bättre återspeglas i byråns arbete.
- Räckvidden hos det föreslagna mandatet är avgränsad. De områden där byrån har visat ett tydligt mervärde stärks, och tillägg görs av nya områden där stöd fordras med anledning av nya politiska prioriteringar och instrument, särskilt it-säkerhetsdirektivet, översynen av EU:s strategi för cybersäkerhet, EU:s kommande cybersäkerhetsplan för samarbete vid cyberkriser och IKT-säkerhetscertifiering:

- **Utvecklingen och genomförandet av EU:s politik:** Byrån får till uppgift att aktivt bidra till utvecklingen av politiken på området nät- och informationssäkerhet samt utvecklingen av politiska initiativ med cybersäkerhetsinslag i diverse andra sektorer (t.ex. energi-, transport- och finanssektorn). För att åstadkomma detta får den en viktig rådgivande roll genom att den kan avge oberoende yttranden och delta i utvecklingen och uppdateringen av politik och lagstiftning. Enisa kommer också att bistå EU i politiken och lagstiftningen på områdena elektronisk kommunikation, elektronisk identifiering och betrodda tjänster, i syfte att främja en ökad nivå av cybersäkerhet. Enisa hjälper medlemsstaterna under genomförandefasen, särskilt inom ramen för den samarbetsgrupp som inrättades genom it-säkerhetsdirektivet, att tillämpa en enhetlig strategi när det gäller it-säkerhetsdirektivets genomförande över gränser och mellan sektorer, samt när det gäller övrig relevant politik och lagstiftning. För att hjälpa till vid den regelbundna översynen av politiken och lagstiftningen på cybersäkerhetsområdet kommer Enisa tillhandahålla regelbundna rapporter om hur genomförandet av den EU-rättsliga ramen fortskrider.

- **Kapacitetsuppbyggnad:** Enisa bidrar till att förbättra EU:s och nationella myndigheters kapacitet och sakkunskap, bland annat i fråga om hantering av incidenter och övervakning av cybersäkerhetsrelaterad lagstiftning. Byrån ska också bidra till upprättandet av centrum för informationsutbyte och analys (Isac) i olika sektorer genom att tillhandahålla bästa praxis och vägledning om tillgängliga verktyg och förfaranden samt genom att på lämpligt sätt hantera regelfrågor rörande informationsutbyte.

- **Kunskap och information, öka medvetenheten:** Enisa blir EU:s informationsnav. Detta inbegriper att främja och utbyta bästa metoder och initiativ i hela EU genom att samla den information om cybersäkerhet som kommer från EU:s och medlemsstaternas institutioner, organ och byråer. Byrån kommer också att göra rådgivning, vägledning och bästa praxis i fråga om säkerheten för kritiska infrastrukturer tillgängliga. Vid en allvarlig gränsöverskridande cybersäkerhetsincident kommer Enisa dessutom att sammanställa rapporter i syfte att ge företagen och allmänheten i hela EU vägledning i efterdyningarna av incidenten. Detta arbete omfattar även att regelbundet organisera medvetandehöjande aktiviteter i samordning med medlemsstaternas myndigheter.

- **Marknadsrelaterade uppgifter (standardisering, cybersäkerhetscertifiering):** Enisa skulle utföra ett antal uppgifter till specifikt stöd för den inre marknaden och utgöra ett ”marknadsobservatorium” inom cybersäkerhet, genom att analysera relevanta trender på cybersäkerhetsmarknaden för att bättre matcha utbud och efterfråga, och genom att stödja utvecklingen av EU-politiken på områdena IKT-standardisering och IKT-cybersäkerhetscertifiering. Särskilt när det gäller standardisering skulle Enisa göra det lättare att skapa cybersäkerhetsstandarder och främja användningen av dem . Enisa skulle också utföra de uppgifter som föreskrivs i den kommande certifieringsramen (se nedanstående avsnitt).

- **Forskning och innovation:** Enisa skulle ge expertrådgivning till EU och de nationella myndigheterna rörande prioritering inom forskning och utveckling, inbegripet det avtalsbaserade offentlig-privata partnerskapet om cybersäkerhet

(cPPP). Enisas forskningsråd skulle tas med i det nya europeiska forsknings- och kompetenscentrumet för cybersäkerhet i nästa fleråriga budgetram. Enisa skulle också, på begäran av kommission, delta i genomförandet av EU:s finansieringsprogram för forskning och innovation.

- **Operativt samarbete och krishantering:** Enisa bör bygga vidare på arbetet med att stärka den befintliga operativa förebyggandekapaciteten, särskilt de paneuropeiska cybersäkerhetsövningarna (Cyber Europe) genom att genomföra dem varje år, och i egenskap av sekretariatet för CSIRT-nätverket (enligt bestämmelserna i it-säkerhetsdirektivet) spela en stödjande roll i det operativa samarbetet, bl.a. genom att säkerställa att CSIRT-nätverkets it-infrastruktur och kommunikationskanaler fungerar väl. För att åstadkomma detta krävs ett strukturerat samarbete med CERT-EU, Europeiska it-brottscentrumet (EC3) och andra berörda EU-organ. Vidare bör Enisa ha ett strukturerat och fysiskt nära samarbete med CERT-EU som resulterar i att Enisa fyller en funktion att ge tekniskt stöd i händelse av betydande incidenter och att stödja incidentanalyser. Medlemsstater skulle på begäran få hjälp med att hantera incidenter och utföra analyser av sårbarheter, artefakter och incidenter i syfte att stärka sin egen kapacitet att förebygga och hantera incidenter.
- Enisa kommer också att spela en roll i **EU:s cybersäkerhetsplan** som läggs fram som en del av det här paketet och som fastställer kommissionens rekommendation till medlemsstaterna om ett samordnat svar på storskaliga gränsöverskridande cybersäkerhetsincidenter och cybersäkerhetskriser på EU-nivå[13]. Enisa skulle underlätta enskilda medlemsstaters samarbete kring hantering av nödsituationer genom att analysera och sammanställa nationella lägesrapporter på grundval av uppgifter som ställs till byråns förfogande på frivillig basis av medlemsstaterna och andra parter.

- **Cybersäkerhetscertifiering av IKT-produkter och IKT-tjänster**

För att skapa och bibehålla förtroendet och säkerheten måste säkerhetsdetaljer införlivas direkt i ett tidigt skede av den tekniska utformningen och utvecklingen av IKT-produkter och IKT-tjänster (inbyggd säkerhet). Dessutom måste kunder och användare kunna förvissa sig om vilken säkerhetsnivå de produkter och tjänster som de förmedlar eller köper har.

Certifiering, som utgörs av en formell utvärdering av produkter, tjänster och processer av ett oberoende och ackrediterat organ med utgångspunkt i ett antal fastställda kriterier eller standarder samt utfärdande av ett certifikat om överensstämmelse, är mycket viktig för att öka förtroendet för varor och tjänster och göra dem säkrare. Säkerhetsutvärdering är ett mycket tekniskt område, medan certifiering har till syfte att informera och försäkra köparna och användarna om säkerhetsegenskaperna hos de IKT-produkter och IKT-tjänster som de köper eller använder. Såsom nämnts ovan är detta särskilt relevant för nya system som i hög grad bygger på digital teknik och som fordrar en hög säkerhetsnivå, såsom uppkopplade och

[13] Planen kommer att gälla cybersäkerhetsincidenter vars störning är mer omfattande än medlemsstaten kan hantera på egen hand eller påverkar två eller flera medlemsstater genom så vidsträckta och betydande konsekvenser eller så allvarlig politisk inverkan att det krävs snabb samordning och respons på unionspolitisk nivå.

automatiserade bilar, elektronisk hälsovård, industriella automatiseringskontrollsystem (IACS)[14] eller smarta elnät.

För närvarande är cybersäkerhetscertifieringen av IKT-produkter och IKT-tjänster i EU högst splittrad. Det finns ett antal internationella initiativ, bland annat de s.k. gemensamma kriterierna (*Common Criteria*, CC) för it-säkerhetsutvärdering (ISO 15408), som är en internationell standard för säkerhetsutvärdering av IKT-produkter och IKT-tjänster. Det baseras på oberoende utvärdering och omfattar sju assuransnivåer (*Evaluation Assurance Levels*, EAL). De gemensamma kriterierna och den åtföljande gemensamma metoden för it-säkerhetsutvärdering, *Common Methodology for Information Technology Security Evaluation* (CEM), utgör teknisk grund för ett internationellt avtal, *Common Criteria Recognition Arrangement* (CCRA), vilket säkerställer att CC-certifieringar erkänns av alla som har undertecknat CCRA. Men enligt den nuvarande versionen av CCRA sker ömsesidigt erkännande endast av utvärderingar upp till assuransnivå 2. Dessutom har bara 13 medlemsstater undertecknat överenskommelsen.

Certifieringsmyndigheterna i tolv medlemsstater har ingått ett avtal om ömsesidigt erkännande av certifikat som utfärdas i enlighet med överenskommelsen på grundval av de gemensamma kriterierna[15]. Dessutom finns det ett antal IKT-certifieringsinitiativ som redan införts eller håller på att införas i medlemsstaterna. De är visserligen viktiga men riskerar att ge upphov till marknadsfragmentering och interoperabilitetsproblem. Till följd av detta kan ett företag blir tvunget genomgå flera certifieringar i olika medlemsstater för att kunna sälja sina produkter på flera olika marknader. Som exempel på detta kan tas en tillverkare av smarta mätare som vill sälja sina produkter i tre medlemsstater, t.ex. Tyskland, Frankrike och Storbritannien. Den tillverkaren måste i dag måste uppfylla kraven i tre olika certifieringssystem: *Commercial Product Assurance* (CPA) i Förenade kungariket, *Certification de Sécurité de Premier Niveau* (CPA) i Frankrike och en specifik CC-skyddsprofil som bygger på de gemensamma kriterierna i Tyskland.

Denna situation leder till högre kostnader och utgör en betydande administrativ börda för företag som bedriver verksamhet i flera medlemsstater. Eftersom kostnaderna för certifiering kan variera avsevärt beroende på vilken produkt/tjänst som avses, vilken assuransnivå som eftersträvas och/eller andra komponenter, tenderar i allmänhet dessa kostnader att vara betydande för företagen. Kostnaden för BSI:s ”Smart Meter Gateway”-certifikat, till exempel, är över en miljon euro (högsta nivå på test och assurans, och certifikatet gäller inte endast en produkt, utan hela den omgärdande infrastrukturen). Kostnaden för certifiering av smarta mätare i Förenade kungariket är nästan 150 000 euro. I Frankrike är kostnaden snarlik den i Förenade kungariket, cirka 150 000 euro eller något högre.

Viktiga offentliga och privata intressenter har konstaterat att företagen i många fall måste certifieras separat i varje medlemsstat om det saknas ett EU-omfattande system för cybersäkerhetscertifiering, vilket leder till en fragmentering av marknaden. I synnerhet skulle

---

[14] Generaldirektoratet Gemensamma forskningscentrumet har publicerat en rapport där man föreslår en första uppsättning gemensamma europeiska krav och allmänna riktlinjer som rör cybersäkerhetscertifiering av IACS-beståndsdelar. Tillgänglig på följande länk: https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf

[15] Gruppen av höga tjänstemän på informationssäkerhetsområdet (SOG-IS) består av tolv medlemsstater plus Norge och har utvecklat ett antal skyddsprofiler för ett begränsat antal produkter, t.ex. digitala signaturer, digitala färdskrivare och smartkort. Medlemmarna arbetar tillsammans för att samordna standardiseringen av CC-skyddsprofiler och samordna utvecklingen av skyddsprofiler. Medlemsstaterna begär ofta SOG-IS-certifiering vid nationella offentliga upphandlingar.

skillnaderna i standard och praxis för cybersäkerhetscertifiering i de olika medlemsstaterna i avsaknad av en harmoniseringslagstiftning på EU-nivå för IKT-produkter och IKT-tjänster sannolikt ge upphov till 28 separata säkerhetsmarknader inom EU i praktiken, var och en med egna tekniska krav, testningsmetoder och förfaranden för cybersäkerhetscertifiering. Om inte lämpliga åtgärder vidtas på EU-nivå, kommer skillnaderna i strategierna på nationell nivå sannolikt att orsaka ett stort bakslag för förverkligandet av den digitala inre marknaden och fördröja eller förhindra de därmed sammanhängande positiva effekterna i form av tillväxt och sysselsättning.

Med utgångspunkt i ovanstående utveckling föreskriver den föreslagna förordningen att det inrättas en EU-ram för cybersäkerhetscertifiering av IKT-produkter och IKT-tjänster (nedan kallad *ramen*), och anger i detalj Enisas väsentliga funktioner och uppgifter på cybersäkerhetscertifieringsområdet. I detta förslag fastställs ett övergripande regelverk för europeiska system för cybersäkerhetscertifiering. Genom förslaget införs inte direkt tillämpliga certifieringssystem, utan det skapas ett system (en ram) för fastställandet av specifika certifieringssystem för specifika IKT-produkter och IKT-tjänster (de ”europeiska systemen för cybersäkerhetscertifiering”). Genom att europeiska system för cybersäkerhetscertifiering inrättas i enlighet med ramavtalet kommer de certifikat som utfärdats enligt dessa system att kunna vara giltiga och erkännas i alla medlemsstater, och det kommer att bli möjligt att ta itu med den nuvarande marknadsfragmenteringen.

Det allmänna syftet med ett europeiskt system för cybersäkerhetscertifiering är att intyga att de IKT-produkter och IKT-tjänster som har certifierats i enlighet med ett sådant system uppfyller de angivna kraven på cybersäkerhet. Detta skulle till exempel inbegripa deras förmåga att skydda uppgifter (oavsett om de lagras, överförs eller på annat sätt behandlas) mot oavsiktlig eller obehörig lagring, behandling, tillgång, utlämnande, förstörelse, oavsiktlig förlust eller ändring. I EU:s system för cybersäkerhetscertifiering skulle befintliga standarder användas i samband med de tekniska krav och utvärderingsförfaranden som produkterna måste uppfylla. Inga egna tekniska standarder skulle utvecklas[16]. För att till exempel skapa en EU-omfattande certifiering av produkter såsom smartkort, som för närvarande testas mot den internationella CC-standarden inom ramen för det multilaterala SOG-IS-systemet (som beskrivs ovan), skulle SOGI-IS-systemet göras giltigt i hela EU.

Förutom en särskild uppsättning säkerhetsmål som ska beaktas vid utformningen av varje specifikt europeiskt system för cybersäkerhetscertifiering fastställs i förslaget dessutom vad systemen åtminstone bör rymma. I sådana system måste det fastställas bland annat ett antal specifika uppgifter om omfattningen av och syftet med cybersäkerhetscertifieringen. Detta inbegriper identifiering av de kategorier av varor och tjänster som avses. den detaljerade specifikationen av cybersäkerhetskrav (t.ex. genom hänvisning till relevanta standarder eller tekniska specifikationer), särskilda utvärderingskriterier och metoder, och den nivå av säkerhet som de är avsedda att garantera (grundläggande, betydande eller hög).

Europeiska system för cybersäkerhetscertifiering kommer att utarbetas av Enisa med bistånd och expertråd från och i nära samarbete med europeiska gruppen för cybersäkerhetscertifiering (se nedan) och antas av kommissionen genom genomförandeakter. När behovet av ett system för cybersäkerhetscertifiering har konstaterats kommer kommissionen att be Enisa att utarbeta ett system för specifika IKT-produkter eller IKT-tjänster. Enisa kommer att arbeta med systemet i nära samarbete med de nationella

[16] När det gäller europeiska standarder ombesörjs detta av de europeiska standardiseringsorganisationerna, och det godkänns av Europeiska kommissionen genom offentliggörande i *Europeiska unionens officiella tidning* (se förordning (EU) nr 1025/2012).

tillsynsmyndigheter för certifiering som företräds i gruppen. Medlemsstaterna och gruppen får föreslå att kommissionen ber Enisa att utarbeta ett särskilt system.

Certifiering kan vara en mycket kostsam process, vilket i sin tur kan leda till högre priser för kunder och konsumenter. Behovet av certifiering kan också variera kraftigt beroende på det specifika användningssammanhanget för produkterna och tjänsterna och den snabba tekniska förändringen. Det bör därför även fortsättningsvis vara frivilligt att anlita en europeisk cybersäkerhetscertifiering, om inte annat föreskrivs i unionslagstiftningen om säkerhetskrav för IKT-produkter och IKT-tjänster.

För att säkerställa en harmonisering och undvika fragmentering kommer de nationella system eller förfaranden för certifiering av IKT-produkter och IKT-tjänster som omfattas av ett europeiskt system för cybersäkerhetscertifiering upphöra att gälla från och med den dag som fastställs i genomförandeakten om antagande av systemet. Vidare bör medlemsstaterna inte införa nya nationella system för certifiering av de IKT-produkter och IKT-tjänster som omfattas av ett befintligt europeiskt certifieringssystem.

När ett europeiskt system för cybersäkerhetscertifiering har antagits kommer tillverkarna av IKT-produkter och leverantörerna av IKT-tjänster att kunna lämna in en ansökan om certifiering av sina produkter och tjänster till valfritt organ för bedömning av överensstämmelse. Organen för bedömning av överensstämmelse bör ackrediteras av ett ackrediteringsorgan, om de uppfyller vissa fastställda krav. Ackrediteringen ska utfärdas för en period på högst fem år och får förnyas på samma villkor under förutsättning att organet för bedömning av överensstämmelse uppfyller kraven. Ackrediteringsorganet ska återkalla ackrediteringen av ett organ för bedömning av överensstämmelse om villkoren för ackrediteringen inte, eller inte längre, uppfylls eller om åtgärder som vidtagits av organet för bedömning av överensstämmelse strider mot denna förordning.

Enligt förslaget ansvarar medlemsstaterna för övervakning, tillsyn och verkställighet. Medlemsstaterna ska tillhandahålla en tillsynsmyndighet för certifiering. Denna myndighet ska ges i uppgift att övervaka att organen för bedömning av överensstämmelse och de certifikat som utfärdats av organen för bedömning av överensstämmelse etablerade på deras territorium uppfyller kraven i denna förordning och i de relevanta europeiska systemen för cybersäkerhetscertifiering. De nationella tillsynsmyndigheterna för certifiering kommer att vara behöriga att handlägga klagomål från fysiska eller juridiska personer rörande certifikat som utfärdats av de organ för bedömning av överensstämmelse som är etablerade på deras territorier. I lämplig omfattning kommer de att undersöka det ärende som klagomålet gäller och underrätta anmälaren om hur ärendet framskrider och om resultatet av utredningen inom rimlig tid. De kommer dessutom att samarbeta med andra tillsynsmyndigheter för certifiering eller andra offentliga myndigheter, t.ex. genom att utbyta information om IKT-produkter och IKT-tjänster som eventuellt avviker från kraven i denna förordning eller de särskilda europeiska system för cybersäkerhetscertifiering.

Genom förslaget inrättas dessutom den europeiska gruppen för cybersäkerhetscertifiering (nedan kallad *gruppen*), bestående av nationella certifieringstillsynsmyndigheter från samtliga medlemsstater. Gruppens huvuduppgift är att bistå kommissionen med råd i frågor som rör politiken på området cybersäkerhetscertifiering och att arbeta tillsammans med Enisa med att utforma förslag till europeiska system för cybersäkerhetscertifiering. Enisa kommer att bistå kommissionen genom att tillhandahålla gruppens sekretariat och föra ett uppdaterat offentligt register över de system som godkänts enligt EU-ramen för cybersäkerhetscertifiering. Enisa skulle dessutom samarbeta med standardiseringsorganen för att garantera lämpligheten hos de standarder som används i godkända system och att fastställa vilka områden som är i behov av cybersäkerhetsstandarder.

Den europeiska ramen för cybersäkerhetscertifiering (nedan kallad *ramen*) kommer att ge flera fördelar för medborgare och företag. I synnerhet gäller följande:

- Genom inrättandet av EU-omfattande system för certifiering av specifika produkters eller tjänsters cybersäkerhet får företagen en enda kontaktpunkt för cybersäkerhetscertifiering inom EU. De företagen behöver bara certifiera produkten en gång, och certifikatet gäller i alla medlemsstater. De är inte skyldiga att certifiera sina produkter hos varje nationellt certifieringsorgan. Det kommer att väsentligt minska företagens kostnader, underlätta gränsöverskridande verksamhet och i slutändan minska och undvika en fragmentering av den inre marknaden för de berörda produkterna.
- I ramen fastställs att de europeiska systemen för cybersäkerhetscertifiering har företräde framför de nationella systemen: Enligt denna bestämmelse kommer ett europeiskt system för cybersäkerhetscertifiering när det antas att ersätta alla befintliga parallella nationella system avseende samma IKT-produkter eller IKT-tjänster på en given tillförlitlighetsnivå. Detta kommer att leda till större tydlighet genom att det minskar den nuvarande spridningen av överlappande och kanske motstridiga nationella certifieringssystem.
- Förslaget stöder och kompletterar genomförandet av it-säkerhetsdirektivet genom att förse de företag som omfattas av direktivet med ett mycket användbart verktyg för att visa att nät- och informationssäkerhetskraven uppfylls i hela unionen. När kommissionen och Enisa utvecklar nya system för cybersäkerhetscertifiering kommer de att rikta särskild uppmärksamhet mot behovet att säkerställa att nät- och informationssäkerhetskraven återspeglas i systemen för cybersäkerhetscertifiering.
- Förslaget kommer att stödja och underlätta utvecklingen av en europeisk politik cybersäkerhet genom att harmonisera villkoren och de materiella kraven för cybersäkerhetscertifiering av IKT-produkter och IKT-tjänster i EU. Europas system för cybersäkerhetscertifiering kommer att hänvisa till gemensamma standarder eller kriterier för utvärderings- och testmetoder. Detta kommer att bidra avsevärt, om än indirekt, till användningen av gemensamma säkerhetslösningar i EU, och därmed också att undanröja hinder för den inre marknaden.
- Ramen är utformad på ett sådant sätt att den nödvändiga flexibilitet som krävs för systemen för cybersäkerhetscertifiering säkerställs. Beroende på vilka särskilda cybersäkerhetsbehov som föreligger kan en produkt eller tjänst certifieras enligt en högre eller lägre nivå av säkerhet. De europeiska systemen för cybersäkerhetscertifiering kommer att utformas med denna flexibilitet i åtanke och kommer därför att föreskriva olika tillförlitlighetsnivåer (grundläggande, betydande eller hög), så att de kan användas för olika ändamål eller i olika sammanhang.
- Alla ovanstående beståndsdelar kommer att göra cybersäkerhetscertifiering mer attraktiv för företag som ett effektivt sätt att kommunicera nivån av cybersäkerhet hos IKT-produkter eller IKT-tjänster. I takt med att cybersäkerhetscertifiering blir billigare, effektivare och mer ekonomiskt attraktiv kommer företag att ha större incitament att certifiera sina produkter mot cybersäkerhetsrisker, och därigenom bidra till spridning av bättre praxis inom cybersäkerhet vid utformningen av IKT-produkter och IKT-tjänster (man tar hänsyn till cybersäkerhet vid produktens utformning, *cybersecurity by design*).

- **Förenlighet med befintliga bestämmelser inom området**

Enligt it-säkerhetsdirektivet är aktörerna inom de sektorer som är av avgörande betydelse för vår ekonomi och vårt samhälle, såsom vatten, energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård samt digital infrastruktur, och leverantörerna av digitala tjänster (t.ex. sökmotorer, molntjänster och internetbaserade marknadsplatser) skyldiga att vidta åtgärder för att på ett lämpligt sätt hantera säkerhetsrisker. De nya bestämmelserna i detta förslag kompletterar och säkerställer förenlighet med bestämmelserna i it-säkerhetsdirektivet, i syfte att ytterligare öka cyberresiliensen i EU genom att utöka kapaciteten, samarbetet, riskhanteringen och cybermedvetenheten.

Vidare är bestämmelserna om cybersäkerhetcertifiering ett viktigt redskap för de företag som omfattas av it-säkerhetsdirektivet, eftersom de kommer att kunna certifiera sina IKT-produkter och IKT-tjänster mot cybersäkerhetsrisker på grundval av system för cybersäkerhetscertifiering som är giltiga och godtas i hela EU. Bestämmelserna kommer också att vara ett komplement till de säkerhetskrav som anges i eIDA-förordningen[17] och direktivet om radioutrustning[18].

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

I förordning (EU) 2016/679 (den allmänna uppgiftsskyddsförordningen)[19] fastställs bestämmelser som gör det möjligt att upprätta certifieringsmekanismer, dataskyddsförseglingar och dataskyddsmärkningar för att visa att denna förordning följs när personuppgiftsansvariga eller registerförare behandlar uppgifter. Den här förordningen påverkar inte certifiering av uppgiftsbehandling enligt den allmänna dataskyddsförordningen, även i de fall då en sådan behandling ingår i produkter och tjänster.

Den föreslagna förordningen kommer att säkerställa överensstämmelse med förordning 765/2008 om krav för ackreditering och marknadskontroll[20] genom att hänvisa till dess bestämmelser om nationella ackrediteringsorganen och organ för bedömning av överensstämmelse. När det gäller tillsynsmyndigheter föreskrivs i förslaget till förordning att medlemsstaterna ska utse nationella certifieringstillsynsmyndigheter med ansvar för tillsyn, övervakning och efterlevnad av bestämmelserna. Dessa organ kommer att vara separata från organen för bedömning av överensstämmelse, i enlighet med förordning 765/2008.

---

17 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.

18 Europaparlamentets och rådets direktiv 2014/53/EU av den 16 april 2014 om harmonisering av medlemsstaternas lagstiftning om tillhandahållande på marknaden av radioutrustning och om upphävande av direktiv 1999/5/EG

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 Förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93.

2. RÄTTSLIG GRUND, SUBSIDIARITETSPRINCIPEN OCH PROPORTIONALITETSPRINCIPEN

- **Rättslig grund**

Den rättsliga grunden för EU:s insatser är artikel 114 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget), som behandlar tillnärmning av medlemsstaternas lagstiftning för att uppnå de mål som anges i artikel 26 i EUF-fördraget, nämligen en väl fungerande inre marknad.

Den inremarknadsrättsliga grunden för att inrätta Enisa har fastställts av domstolen (dom i mål C-217/04, *Förenade kungariket mot Europaparlamentet och rådet*) och åter bekräftats i 2013 års förordning som fastställer byråns nuvarande mandat. Dessutom skulle verksamhet som återspeglar målen att öka samarbetet och samordningen mellan medlemsstaterna, eller som förbättrar förmågan på EU-nivå att komplettera medlemsstaternas åtgärder, ingå i kategorin ”operativt samarbete”. Operativt samarbete identifieras särskilt i it-säkerhetsdirektivet (vars rättsliga grund är artikel 114 i EUF-fördraget) som ett mål som bör eftersträvas inom ramen för CSIRT-nätverket, där ”Enisa ska tillhandahålla sekretariatet och aktivt stödja samarbetet” (artikel 12.2). I synnerhet anges i artikel 12.3 f identifiering av ytterligare former av operativt samarbete som en uppgift för CSIRT-nätverket, inklusive med avseende på i) kategorier av risker och incidenter, ii) tidiga varningar, iii) ömsesidigt bistånd, och iv) principer och metoder för samordning, när medlemsstaterna vidtar åtgärder mot gränsöverskridande risker och incidenter.

- Den nuvarande fragmenteringen av system för certifiering av IKT-produkter och IKT-tjänster är också en följd av det saknas ett gemensamt rättsligt bindande och effektivt ramförfarande som gäller i medlemsstaterna. Detta hindrar skapandet av en inre marknad för IKT-produkter och IKT-tjänster och hämmar de europeiska företagens konkurrenskraft inom denna sektor. Syftet med det här förslaget är att komma till rätta med den nuvarande fragmenteringen och de därmed sammanhängande hindren på den inre marknaden genom att tillhandahålla en gemensam ram för inrättandet av europeiska system för cybersäkerhetscertifiering som ska gälla i hela EU.

Subsidiaritetsprincipen (för icke-exklusiv befogenhet)

Subsidiaritetsprincipen kräver att det görs en bedömning av nödvändigheten och mervärdet av en åtgärd på EU-nivå. Att åtgärder på det här området måste vara förenliga med subsidiaritetsprincipen fastställdes redan när den nuvarande Enisa-förordningen antogs[21].

Cybersäkerhet är en fråga av gemensamt intresse för unionen. Det ömsesidiga beroendet mellan nät- och informationssystem är så stort att enskilda aktörer (offentliga och privata, inklusive allmänheten) ofta inte isolerade kan möta hot och hantera riskerna och de möjliga effekterna av cyberincidenter. Å ena sidan gör det ömsesidiga beroendet mellan medlemsstaterna, bland annat när det gäller driften av kritisk infrastruktur (energi, transport, vatten, för att bara nämna några) att offentliga insatser på EU-nivå inte bara är något positivt, utan även nödvändigt. Å andra sidan kan EU-insatserna ge positiva ”spridningseffekter” till

[21] Europaparlamentets och rådets förordning (EU) nr 526/2013 av den 21 maj 2013 om Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) och om upphävande av förordning (EG) nr 460/2004.

följd av att god praxis sprids mellan medlemsstaterna, vilket kan leda till ökad cybersäkerhet i unionen.

Sammanfattningsvis, i den rådande kontexten och i betraktande av framtida scenarier, verkar det som att **enskilda åtgärder från EU:s medlemsstaterna och en fragmenterad strategi för cybersäkerhet** inte kommer att räcka för att **öka unionens kollektiva cyberresiliens**.

EU-åtgärder bedöms även vara nödvändiga för att motverka fragmenteringen av de nuvarande systemen för cybersäkerhetscertifiering. Det skulle göra det möjligt för tillverkarna att fullt ut dra nytta av en inre marknad med betydande besparingar när det gäller provning och kostnader för omkonstruktion. Medan den aktuella gruppen av höga tjänstemän på informationssäkerhetsområdet (SOG-IS) avtalet om ömsesidigt erkännande exempelvis har uppnått goda resultat i detta avseende, har den också visat viktiga begränsningar som står i vägen för dess lämplighet att ge långsiktigt hållbara lösningar när det gäller att ta tillvara den inre marknadens fulla potential.

Mervärdet av att vidta åtgärder på EU-nivå, särskilt i syfte att stärka samarbetet mellan medlemsstaterna, men också mellan nät- och informationssäkerhetsaktörerna, har konstaterats i rådets slutsatser från 2016[22] det framgår också klart av utvärderingen av Enisa.

- **Proportionalitetsprincipen**

De föreslagna åtgärderna går inte utöver vad som är nödvändigt för att uppnå de politiska målen. Vidare bör räckvidden hos EU-insatserna inte hindra ytterligare nationella åtgärder med avseende på den nationella säkerheten. Insatser på EU-nivå är därför motiverat av subsidiaritetsskäl och proportionalitetsskäl.

- **Val av instrument**

Detta förslag innehåller en översyn över förordning (EU) nr 526/2013 som fastställer Enisas nuvarande mandat och uppgifter. Med beaktande av Enisas betydelsefulla roll vid inrättandet och förvaltningen av EU:s ram för cybersäkerhetscertifiering, vore det bäst om Enisas nya mandat och den ramen fastställdes genom ett enda rättsligt instrument som har formen av en förordning.

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

Efterhandsutvärderingar/kontroller av ändamålsenligheten med befintlig lagstiftning

Enligt utvärderingsfärdplanen[23] bedömde kommissionen byråns **relevans, genomslagskraft, ändamålsenlighet, effektivitet, samstämmighet och mervärde** med avseende på dess resultat, styrning, interna organisation och arbetsmetoder under perioden 2013–2016. De viktigaste resultaten kan sammanfattas enligt följande (mer information finns i arbetsdokumentet från kommissionens avdelningar som åtföljer konsekvensanalysen):

- **Relevans:** Mot bakgrund av den tekniska utvecklingen och de nya hoten och med tanke på det stora behovet av att öka cybersäkerheten i EU har Enisas mål visat sig

[22] Rådets slutsatser om att stärka Europas system för cyberresiliens och främja en konkurrenskraftig och innovativ cybersäkerhetsbransch – 15 november 2016.

[23] http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf

vara relevanta. Medlemsstaterna och EU:s organ är beroende av Enisas betydande sakkunskap på området cybersäkerhet. Medlemsstaterna behöver dessutom öka sin förmåga att bättre förstå och bemöta hot, och intressenterna behöver samarbeta inom olika tematiska områden och institutioner emellan. Cybersäkerhet fortsätter att vara en viktig politisk prioritering för EU som Enisa förväntas hantera; men Enisas utformning som EU-byrå med ett tidsbegränsat mandat i) möjliggör inte långsiktig planering och hållbart stöd till medlemsstaterna och EU:s institutionerna, ii) kan leda till ett rättsligt vakuum, eftersom de uppgifter som Enisa anförtros enligt bestämmelserna i it-säkerhetsdirektivet är av permanent karaktär[24], iii) saknar samstämmighet med en vision som kopplar samman Enisa med ett stärkt EU-cybersäkerhetslandskap.

- **Ändamålsenlighet**: Enisa uppnådde generellt sina mål och genomförde sina uppgifter. Den bidrog till att öka nät- och informationssäkerheten i Europa genom sin huvudsakliga verksamhet (kapacitetsuppbyggnad, tillhandahållande av sakkunskap, gemenskapsbyggande insatser, och stöd till politik). Den visade emellertid att den har potential att uppnå bättre resultat inom samtliga dessa områden. I utvärderingen konstaterades att Enisa har skapat starka och förtroendefulla relationer med vissa av sina intressenter, bl.a. med medlemsstaterna och de olika CSIRT. Insatserna inom kapacitetsuppbyggnad uppfattades som ändamålsenliga, särskilt de som riktades till medlemsstaterna med mindre resurser. Att främja ett brett samarbete har varit en av de viktigaste insatserna, och intressenterna är eniga om Enisas positiva roll när det gäller att föra samman människor. Enisa har dock haft svårt att åstadkomma mycket inom det stora området nät- och informationssäkerhet. Detta berodde också på att Enisa hade relativt begränsade mänskliga och finansiella resurser till genomförandet av det mycket breda mandatet. I utvärderingen konstaterades det även att Enisa delvis uppfyllt målet att tillhandahålla sakkunskap, vilket sammanhängde med svårigheterna att rekrytera experter (se även avsnittet Effektivitet nedan).
- **Effektivitet**: Trots sin begränsade budget – bland de lägsta jämfört med andra EU-byråer – har byrån kunnat bidra till de uppsatta målen och sammantaget visat att den effektivt använt sina resurser. Utvärderingen visade att processerna i allmänhet var effektiva och att en tydlig uppdelning av ansvaret inom organisationen ledde till att uppgifterna utfördes väl. En av de största utmaningarna när det gäller Enisas effektivitet är dess svårigheter med att rekrytera och behålla högt kvalificerade experter. Resultaten av utvärderingen visar att detta kan förklaras av en kombination av faktorer, bland annat de allmänna svårigheterna inom hela den offentliga sektorn att konkurrera med den privata sektorn när det gäller att anställa högt specialiserade experter, typen av kontrakt (visstid) som Enisa erbjuder och den tämligen låga attraktionskraften hos Enisas geografiska läge, t.ex. kopplade till svårigheter för makar att hitta arbete. Uppdelningen av byråerna mellan Aten och Heraklion krävde ytterligare samordningsinsatser och skapade merkostnader, men flytten av den centrala operativa avdelningen till Aten 2013 ökade byråns operativa effektivitet.
- **Samstämmighet**: Enisas verksamhet har generellt sett varit samstämmig med dess intressenters politik och verksamhet, både på nationell nivå och EU-nivå, men det behövs en mer samordnad strategi för cybersäkerhet på EU-nivå. Möjligheterna till samarbete mellan Enisa och andra EU-organ har inte utnyttjats till fullo.

[24] Hänvisning till artiklarna 7, 9, 11, 12, 19 i it-säkerhetsdirektivet.

Utvecklingen av EU:s rättsliga och politiska landskap gör det nuvarande mandatet mindre sammanhängande i dag.

- **EU-mervärde**: Enisas mervärde ligger främst i dess förmåga att förbättra samarbetet i synnerhet mellan medlemsstaterna men även med de relaterade nät- och informationssäkerhetsorganen. Det finns ingen annan aktör på EU-nivå som stöder så många typer av intressenter på området nät- och informationssäkerhet. Det mervärde som byrån kan variera i förhållande till de olika behov och resurser av berörda parter (t.ex. stora kontra små medlemsstater. Medlemsstaterna och industrin) och behovet att prioritera sin verksamhet enligt arbetsprogrammet. I utvärderingen konstaterades att om Enisa lades ner skulle det innebära att en möjlighet gick förlorad för alla medlemsstater. Det skulle inte vara möjligt att säkerställa samma grad av gemenskapsbyggande och samarbete mellan alla medlemsstaterna på området cybersäkerhet. I avsaknad av ett mer centraliserat EU-organ skulle det ske en ökad uppsplittring, där bilateralt och regionalt samarbete skulle fylla tomrum efter Enisa.

När det gäller Enisas tidigare och framtida resultat, är de viktigaste trender som kan utläsas ur 2017 års samråd följande[25]:

- Enisas allmänna resultat under perioden 2013–2016 bedömdes vara positivt av en majoritet av de svarande (74 %). En majoritet av de svarande ansåg dessutom att Enisa uppnår sina olika mål (minst 63 % för vart och ett av målen). Enisas tjänster och produkter används regelbundet (varje månad eller oftare) av nästan hälften av de svarande (46 %), som uppskattar det faktum att de härrör från ett organ på EU-nivå (83 %) och är av god kvalitet (62 %).
- De svarande pekade på ett antal brister och utmaningar för cybersäkerheten i EU i framtiden, där de fem viktigaste (i en förteckning över 16) var samarbete mellan medlemsstaterna, kapacitet att förebygga, upptäcka och lösa storskaliga cyberattacker, samarbete mellan medlemsstaterna i frågor som rör cybersäkerhet, samarbete och informationsutbyte mellan olika intressenter, inbegripet mellan offentlig och privat sektor, och skydd av kritisk infrastruktur mot cyberattacker.
- En stor majoritet (88 %) av de svarande ansåg emellertid att den nuvarande instrumentet och mekanismerna på EU-nivå är otillräckliga eller endast delvis ändamålsenliga när det gäller dessa punkter. En stor majoritet av de svarande (98 %) ansåg att ett EU-organ bör tillgodose dessa behov, och av dessa ansåg 99 % att Enisa är det rätta organet att göra detta.

Samråd med berörda parter

- Kommissionen anordnade ett offentligt samråd om översynen av Enisa mellan den 12 april och den 5 juli 2016 och fick 421 svar[26]. Enligt resultaten från samrådet ansåg

[25] 90 intressenter från 19 medlemsstater deltog i samrådet (88 svar och 2 ståndpunktsdokument), inbegripet nationella myndigheter från 15 medlemsstater, bland annat Frankrike, Italien, Irland och Grekland, och 8 paraplyorganisationer som företräder ett stort antal europeiska organisationer, till exempel Europeiska bankförbundet, Digital Europe (företräder den digitala teknikbranschen i Europa) och ETNO (den europeiska sammanslutningen för publika telenätoperatörer). Det offentliga samrådet om Enisa kompletterades av flera andra källor, bland annat i) intervjuer med cirka 50 viktiga aktörer inom cybersäkerhetssektorn, ii) enkät till CSIRT-nätverket, iii) enkät till Enisas styrelse, Enisas direktion och Enisas ständiga intressentgrupp.

67,5 % av de svarande att Enisa skulle kunna hjälpa till att skapa en harmoniserad ram för säkerhetscertifiering av it-produkter och it-tjänster.

Av avsnittet rörande certifiering i samrådet från 2016 om avtalsbaserade offentlig-privata partnerskap (cPPP) om cybersäkerhet[27] framgår följande:

- 50,4 % (121 av 240 svarande) visste inte om de nationella certifieringssystemen erkänns ömsesidigt i alla EU:s medlemsstater eller inte. 25,8 % (62 av 240) svarade ”nej”, medan 23,8 % (57 av 240) svarade ”ja”.
- 37,9 % (91 av 240) ansåg att de nuvarande certifieringssystemen inte stöder de europeiska företagens behov. Å andra sidan uttryckte 17, 5 % (42 av 240) – huvudsakligen internationella företag verksamma på den europeiska marknaden – motsatsen.
- 49,6 % (119 av 240) av de svarande ansåg att det inte är lätt att påvisa likvärdighet mellan standarder, certifieringssystem och märkningar. 37,9 % (91 av 240) svarade ”vet inte”, medan endast 12,5 % (30 av 240) svarade ”ja”.

Insamling och användning av sakkunnigutlåtanden

Kommissionen förlitade sig på följande externa sakkunskap:

- Study on the Evaluation of ENISA (Ramboll/Carsa 2017. Smart no. 2016/0077).
- Study on ICT Security Certification and Labelling – Evidence gathering and impact assessment (PriceWaterhouseCoopers 2017, Smart nr 2016/0029).

Konsekvensbedömning

- I konsekvensbedömningen om detta initiativ identifierades följande huvudsakliga problem som behöver åtgärdas:
- Fragmentering av politiken och strategierna på området cybersäkerhet i alla medlemsstater.
- Utspridning av resurser och fragmentering av strategier på området cybersäkerhet bland EU:s institutioner, organ och byråer. och
- Bristande medvetenhet hos och information till medborgarna och företagen kombinerat med ett växande antal olika nationella och sektorsvisa certifieringssystem.

I rapporten bedömdes följande möjliga alternativ när det gäller Enisas mandat:

- Bevarande av status quo, vilket innebär ett utvidgat mandat som fortfarande är begränsat i tiden (grundalternativ).
- Enisas nuvarande mandat löper ut utan förlängning samt avslutande av Enisa (inga åtgärder).

---

[26] 162 bidrag från medborgare, 33 från det civila samhället och konsumentorganisationer, 186 från branschen och 40 från offentliga organ, inklusive de behöriga myndigheter som kontrollerar att direktivet om integritet och elektronisk kommunikation efterlevs.

[27] 240 intressenter från nationella offentliga myndigheter, stora företag, små och medelstora företag, mikroföretag och forskningsorgan svarade på avsnittet om certifiering.

- En reform av Enisa.
- En EU-cybersäkerhetsbyrå med full operativ kapacitet.

I rapporten bedömdes följande möjliga alternativ när det gäller cybersäkerhetscertifiering:

- Inga åtgärder (grundalternativ).
- Andra åtgärder än lagstiftning (”icke-bindande instrument”).
- EU-rättsakt för att skapa ett obligatoriskt system för samtliga medlemsstater på grundval av SOG-IS.
- Allmän EU-ram för IKT-cybersäkerhetscertifiering.

Analysen ledde till slutsatsen att en ”reform av Enisa” i kombination med en allmän EU-ram för IKT-cybersäkerhetscertifiering är att rekommendera.

Det rekommenderade alternativet har bedömts vara de mest effektiva för att EU ska uppnå de fastställda målen att Öka kapaciteten, beredskapen, samarbetet, medvetenheten och insynen på området cybersäkerhet och undvika en fragmentering av marknaden. Det alternativet har också bedömts vara det som bäst överensstämmer med de politiska prioriteringarna i EU:s strategi för cybersäkerhet och den därmed sammanhängande politiken (t.ex. it-säkerhetsdirektivet) och strategin för den digitala inre marknaden. Det framgick också det av samrådsförfarandet att det rekommenderade alternativet stöds av de flesta intressenter. Dessutom visade den analys som gjordes inom ramen för konsekvensbedömningen att målen skulle nås med rimligt utnyttjande av resurser om det rekommenderade alternativet valdes.

Kommissionens nämnd för lagstiftningskontroll avgav ett negativt yttrande den 24 juli och ett positivt yttrande den 25 augusti 2017 efter att konsekvensbedömningen lagts fram på nytt. Den ändrade konsekvensbedömningen rymde ytterligare styrkande dokumentation, de slutgiltiga slutsatserna från utvärderingen av Enisa samt ytterligare förklaringar rörande de olika policy-alternativen och deras konsekvenser. I bilaga 1 till slutversionen av konsekvensbedömningen sammanfattas hur nämndens kommentarer i det andra yttrandet har beaktats. Konsekvensanalysen uppdaterades för att mer i detalj redogöra för cybersäkerhetskontexten i EU, inbegripet de åtgärder som ingår i det gemensamma meddelandet till Europaparlamentet och rådet: Resiliens, avskräckning och försvar: ett starkt cyberförsvar för EU (JOIN(2017) 450) och är av särskild relevans för Enisa, nämligen EU:s cybersäkerhetsplan och det europeiska forsknings- och kompetenscentrumet för cybersäkerhet, till vilka byrån skulle koppla sin rådgivning om EU:s forskningsbehov.

I konsekvensanalysen beskrivs hur reformen av Enisa, inbegripet nya uppgifter, bättre anställningsvillkor och strukturellt samarbete med EU:s organ på området, skulle öka Enisas attraktionskraft som arbetsgivare och bidra till att ta itu med problem i samband med rekrytering av experter. Bilaga 6 till konsekvensanalysen innehåller också en reviderad uppskattning av kostnaderna för de olika alternativen för Enisa. När det gäller certifiering har konsekvensanalysen reviderats för att ge en mer utförlig förklaring, inklusive en grafisk presentation av det rekommenderade alternativet, och för att göra uppskattningar av kostnaderna för medlemsstaterna och kommissionen kopplade till den nya certifieringsramen. En närmare förklaring har getts till valet av Enisa som nyckelaktör i ramen, vilket grundades på Enisas expertkunskap på området och det faktum att det är den enda byrån på EU-nivå på området cybersäkerhet. Slutligen reviderades avsnitten om certifiering för att klargöra aspekterna rörande skillnaden jämfört med det nuvarande SOG-IS-systemet och fördelarna med de olika alternativen, och förklara det faktum att typen av IKT-produkter och IKT-tjänster som omfattas av ett europeiskt certifieringssystem kommer att fastställas i det godkända systemet i fråga.

Lagstiftningens ändamålsenlighet och förenkling

Ej tillämpligt

Konsekvenser för de grundläggande rättigheterna

Cybersäkerhet spelar en viktig roll för att skydda enskilda personers privatliv och personuppgifter i enlighet med artiklarna 7 och 8 i EU:s stadga om de grundläggande rättigheterna. Vid cyberincidenter är skyddet för privatlivet och personuppgifterna tydligt utsatta för risker. Cybersäkerhet är således en nödvändig förutsättning för respekten för privatlivet och konfidentialiteten när det gäller personuppgifter. Enligt detta synsätt utgör förslaget, som syftar till att stärka cybersäkerheten i Europa, ett viktigt komplement till den befintliga lagstiftningen om skydd av den grundläggande rätten till privatlivet och skydd av personuppgifter. Cybersäkerhet är också viktigt för att skydda konfidentialiteten vid elektroniska kommunikationer och därmed för utövandet av yttrande- och informationsfriheten och andra närliggande rättigheter, såsom tankefrihet, samvetsfrihet och religionsfrihet.

4. BUDGETKONSEKVENSER

Se finansieringsöversikten

5. ÖVRIGA INSLAG

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

Kommissionen kommer att övervaka tillämpningen av denna förordning och lämna en rapport om sin utvärdering till Europaparlamentet och rådet och Europeiska ekonomiska sociala kommittén vart femte år. Dessa rapporter kommer att vara offentliga och redogöra för den praktiska tillämpningen och kontrollen av efterlevnaden när det gäller denna förordning.

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

Avdelning I i förordningen innehåller de allmänna bestämmelserna: syfte (artikel 1), definitioner (artikel 2), inklusive hänvisningar till relevanta definitioner från andra EU-instrument, såsom Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (it-säkerhetsdirektivet), Europaparlamentets och rådets förordning (EG) nr 765/2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 och av Europaparlamentets och rådets förordning (EU) nr 1025/2012 om europeisk standardisering.

Avdelning II i förordningen innehåller de viktigaste bestämmelserna om Enisa, EU:s cybersäkerhetsbyrå.

I kapitel I i denna avdelning anges byråns mandat (artikel 3), mål (artikel 4) och uppgifter (artiklarna 5–11).

I kapitel II beskrivs Enisas organisation och ryms viktiga bestämmelser om dess struktur (artikel 12). Kapitlet behandlar styrelsens sammansättning, omröstningsförfaranden och uppgifter (avsnitt 1, artiklarna 13–17), direktionen (avsnitt 2, artikel 18) och verkställande

direktören (avsnitt 3, artikel 19). Det innehåller också bestämmelser om den ständiga intressentgruppens sammansättning och roll (avsnitt 4, artikel 20). Sist men inte minst innehåller avsnitt 5 byråns verksamhetsregler rörande bland annat programplanering, intressekonflikter, öppenhet, konfidentialitet och tillgång till handlingar (artiklarna 21–25).

Kapitel III rör inrättandet av byråns budget och budgetens struktur (artiklarna 26 och 27), liksom bestämmelserna om dess genomförande (artiklarna 28 och 29). Det rymmer även bestämmelser som underlättar kampen mot bedrägerier, korruption och annan olaglig verksamhet (artikel 30).

Kapitel IV avser byråns personalstyrka. Det innehåller allmänna bestämmelser om tjänsteföreskrifterna och anställningsvillkoren och om immunitet och privilegier (artiklarna 31 och 32). Det rymmer även detaljerade bestämmelser om hur den verkställande direktören ska anställas och utses (artikel 33). Avslutningsvis innehåller det bestämmelser om användningen av nationella experter och annan personal som inte är anställd av byrån (artikel 34).

Kapitel V avslutningsvis innehåller allmänna bestämmelser rörande byrån. Det beskriver den rättsliga ställningen (artikel 35) och innehåller bestämmelser som reglerar ansvar, språkanvändning och skydd av personuppgifter (artiklarna 36–38) samt säkerhetsbestämmelser om skydd av säkerhetsskyddsklassificerade uppgifter och känsliga icke-säkerhetsskyddsklassificerade uppgifter (artikel 40). Reglerna som styr byråns samarbete med tredjeländer och internationella organisationer beskrivs också (artikel 39). Sist men inte minst innehåller det bestämmelser om byråns säte och villkor för verksamheten samt administrativ kontroll av ombudsmannen (artiklarna 41 och 42).

Genom avdelning III inrättas EU-ramen för cybersäkerhetscertifiering av IKT-produkter och IKT-tjänster (nedan kallad ***ramen***) som allmän rättslig ram (artikel 1). I denna avdelning definieras det allmänna syftet med EU:s system för cybersäkerhetscertifiering, nämligen att säkerställa att IKT-produkter och IKT-tjänster uppfyller de angivna kraven för cybersäkerhet vad gäller deras förmåga att, vid en viss tillförlitlighetsnivå, tåla handlingar som äventyrar tillgängligheten, autenticiteten, integriteten eller konfidentialiteten hos lagrade, överförda eller behandlade data eller tjänster, eller därmed sammanhängande funktioner (artikel 43). I denna avdelning förtecknas dessutom de säkerhetsmål som EU:s system för cybersäkerhetscertifiering ska försöka nå (artikel 45), bland annat förmågan att skydda uppgifter mot oavsiktlig eller obehörig åtkomst, eller röjande, förstöring eller ändring, och innehållet (det vill säga delarna) av EU:s system för cybersäkerhetscertifiering, såsom den detaljerade beskrivningen av deras tillämpningsområde, säkerhetsmålen, utvärderingskriterierna och så vidare. (artikel 47).

Dessutom fastställs i avdelning III de viktigaste rättsliga följderna av EU:s system för cybersäkerhetscertifiering, nämligen i) skyldigheten att genomföra systemet på nationell nivå och den frivilliga karaktären hos certifieringen, ii) den ogiltigförklarande inverkan som de europeiska systemen för certifiering av sybersäkerhet har på de nationella systemen för samma produkter eller tjänster (artiklarna 48 och 49).

I denna avdelning fastställs vidare förfarandet för antagande av EU:s system för cybersäkerhetscertifiering samt de respektive roller som kommissionen, Enisa och den europeiska gruppen för cybersäkerhet – nedan kallad *gruppen* – ska ha (artikel 44). Avdelning III rymmer dessutom bestämmelserna om organen för bedömning av överensstämmelse, inklusive krav, befogenheter och uppgifter, om de nationella tillsynsmyndigheterna för certifiering samt om sanktioner.

Gruppen inrättas även i denna avdelning som ett viktigt organ bestående av företrädare för de nationella certifieringstillsynsmyndigheterna vars främsta funktion är att tillsammans med

Enisa utarbeta förslag till europeiska system för cybersäkerhetscertifiering och bistå kommissionen med råd i allmänna eller särskilda frågor rörande politiken på området cybersäkerhetscertifiering.

Avdelning IV i förordningen innehåller slutbestämmelserna, som beskriver utövande av delegering, utvärderingskrav, upphävande och succession samt ikraftträdandet.

2017/0225 (COD)

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013, och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”)

(Text av betydelse för EES)

EUROPAPARLAMENTET OCH EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

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

med beaktande av Europeiska kommissionens förslag,

efter översändande av utkastet till lagstiftningsakt till de nationella parlamenten,

med beaktande av Europeiska ekonomiska och sociala kommitténs yttrande[28],

med beaktande av Regionkommitténs yttrande[29],

i enlighet med det ordinarie lagstiftningsförfarandet, och

av följande skäl:

(1) Nät- och informationssystem samt telekommunikationsnät och -tjänster har en avgörande betydelse för samhället och har blivit själva ryggraden för ekonomisk tillväxt. Informations- och kommunikationsteknik är grunden för komplexa system som stöder samhälleliga verksamheter, håller våra ekonomier igång inom viktiga sektorer som hälso- och sjukvård, energi, finans och transporter, och framför allt bidrar till den inre marknadens funktion.

(2) Användningen av nät- och informationssystem bland allmänheten, företag och regeringar i hela unionen genomsyrar nu hela samhället. Digitalisering och konnektivitet är på väg att bli centrala inslag i ett allt större antal produkter och tjänster, och med tillkomsten av sakernas internet väntas miljoner eller rentav miljarder uppkopplade digitala enheter tas i bruk inom EU under det kommande årtiondet. Trots att allt fler enheter är uppkopplade till internet, är säkerhet och resiliens inte tillräckligt integrerade i konstruktionen, vilket leder till otillräcklig cybersäkerhet. I detta sammanhang leder den begränsade användningen av certifiering till att organisationer och enskilda användare har otillräcklig information om cybersäkerheten hos IKT-produkter och IKT-tjänster, vilket undergräver förtroendet för digitala lösningar.

(3) Ökad digitalisering och konnektivitet leder till ökade cybersäkerhetsrisker, vilket gör samhället som helhet mer sårbart för cyberhot och ökar farorna för enskilda individer,

[28] EUT C , , s. .
[29] EUT C , , s. .

inbegripet sårbara grupper som barn. För att minska denna risk för samhället måste alla nödvändiga åtgärder vidtas för att stärka cybersäkerheten i EU i syfte att bättre skydda nät- och informationssystem, telekommunikationsnät, digitala produkter, tjänster och enheter som används av privatpersoner, myndigheter och företag – från små och medelstora företag till operatörer av kritisk infrastruktur – mot cyberhot.

(4) Cyberangreppen ökar och en uppkopplad ekonomi och ett uppkopplat samhälle som är mer utsatta för cyberhot och -angrepp kräver starkare skydd. Även om cyberangrepp ofta är gränsöverskridande, är dock de politiska insatserna från cybersäkerhetsmyndigheter och brottsbekämpande organ till övervägande del nationella. Storskaliga cyberincidenter kan störa tillhandahållandet av grundläggande tjänster i hela EU. Detta kräver en effektiv respons och krishantering på EU-nivå som bygger på särskilt utformade strategier och bredare instrument för europeisk solidaritet och ömsesidigt stöd. För beslutsfattare, näringsliv och användare är det också viktigt att det görs regelbundna bedömningar av situationen när det gäller cybersäkerhet och resiliens i unionen, på grundval av tillförlitliga unionsdata, samt systematiska prognoser för framtida utveckling, utmaningar och hot på både unionsnivå och global nivå.

(5) Mot bakgrund av de allt större cybersäkerhetsutmaningar som unionen står inför behövs en omfattande uppsättning åtgärder som bygger vidare på tidigare unionsåtgärder och främjar mål som stärker varandra inbördes. Dessa innefattar behovet av att ytterligare öka medlemsstaternas och företagens kapacitet och beredskap samt att förbättra samarbete och samordning mellan medlemsstaterna och EU:s institutioner, byråer och organ. Med tanke på cyberhotens gränsöverskridande karaktär finns det ett behov av att öka kapaciteten på unionsnivå som ett komplement till medlemsstaternas insatser, särskilt när det gäller storskaliga gränsöverskridande cyberincidenter och -kriser. Ytterligare insatser behövs också för att öka allmänhetens och företagens medvetenhet om cybersäkerhetsfrågor. Dessutom bör förtroendet för den digitala inre marknaden stärkas ytterligare genom att transparent information tillhandahålls om säkerhetsnivån för IKT-produkter och IKT-tjänster. Detta kan underlättas genom EU-omfattande certifiering som erbjuder gemensamma cybersäkerhetskrav och utvärderingskriterier för olika nationella marknader och sektorer.

(6) Europaparlamentet och rådet antog 2004 förordning (EG) nr 460/2004[30] om inrättandet av Enisa med syftet att bidra till målet att säkerställa en hög nivå på nät- och informationssäkerheten i unionen och utveckla en kultur av nät- och informationssäkerhet till förmån för medborgarna, konsumenterna, företagen och den offentliga administrationen. Europaparlamentet och rådet antog år 2008 förordning (EG) nr 1007/2008[31] som förlängde byråns mandat till mars 2012. Genom förordning (EU) nr 580/2011[32] förlängdes byråns mandat ytterligare till den 13 september 2013.

---

30 Europaparlamentets och rådets förordning (EG) nr 460/2004 av den 10 mars 2004 om inrättandet av den europeiska byrån för nät- och informationssäkerhet (EUT L 77, 13.3.2004, s. 1).

31 Europaparlamentets och rådets förordning (EG) nr 1007/2008 av den 24 september 2008 om ändring av förordning (EG) nr 460/2004 om inrättandet av den europeiska byrån för nät- och informationssäkerhet i fråga om dess mandatperiod (EUT L 293, 31.10.2008, s. 1).

32 Europaparlamentets och rådets förordning (EU) nr 580/2011 av den 8 juni 2011 om ändring av förordning (EG) nr 460/2004 om inrättandet av den europeiska byrån för nät- och informationssäkerhet vad gäller dess varaktighet (EUT L 165, 24.6.2011, s. 3).

Europaparlamentet och rådet antog år 2013 förordning (EU) nr 526/2013[33] om Enisa och om upphävande av förordning (EG) nr 460/2004, som förlängde byråns mandat till juni 2020.

(7) Unionen har redan vidtagit viktiga åtgärder för att säkerställa cybersäkerhet och öka förtroendet för digital teknik. År 2013 antogs EU:s strategi för cybersäkerhet för att vägleda EU:s politiska åtgärder för cybersäkerhetshot och -risker. I sin satsning för att bättre skydda invånarna på nätet antog unionen 2016 den första rättsakten på området cybersäkerhet, direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (nedan kallat *it-säkerhetsdirektivet*). It-säkerhetsdirektivet införde krav om nationell kapacitet på cybersäkerhetsområdet, inrättade de första mekanismerna för att stärka det strategiska och operativa samarbetet mellan medlemsstaterna och införde skyldigheter avseende säkerhetsåtgärder och incidentrapportering inom sektorer som är centrala för ekonomin och samhället, såsom energi, transporter, vatten, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, digital infrastruktur samt leverantörer av viktiga digitala tjänster (sökmotorer, molntjänster och elektroniska marknadsplatser). Enisa fick en viktig roll när det gällde att stödja genomförandet av direktivet. Dessutom är en effektiv kamp mot it-brottslighet en viktig prioritering i den europeiska säkerhetsagendan, som bidrar till det övergripande målet att uppnå en hög nivå av cybersäkerhet.

(8) Det är allmänt erkänt att den övergripande politiska ramen har förändrats avsevärt sedan antagandet av EU:s strategi för cybersäkerhet 2013 och den senaste översynen av byråns uppdrag, även i förhållande till en mer oviss och mindre säker global miljö. Mot denna bakgrund och inom ramen för unionens nya cybersäkerhetsstrategi är det nödvändigt att se över Enisas mandat för att definiera dess roll i det förändrade cybersäkerhetsekosystemet och säkerställa att byrån bidrar effektivt till unionens reaktion på cybersäkerhetsutmaningar som härrör från detta radikalt förändrade hotlandskap, för vilket det nuvarande mandatet är inte tillräckligt, vilket också medges i utvärderingen av byrån.

(9) Den byrå som inrättas genom denna förordning bör efterträda Enisa, som inrättades genom förordning (EG) nr 526/2013. Byrån bör utföra de uppgifter som den tilldelas genom denna förordning och unionens rättsakter på cybersäkerhetsområdet genom att bland annat tillhandahålla expertis och rådgivning och fungera som unionens informations- och kunskapscentrum. Kommissionen bör främja utbyte av bästa praxis mellan medlemsstaterna och privata aktörer, lägga fram strategiförslag för Europeiska kommissionen och medlemsstaterna som kan användas som utgångspunkt för unionens sektorsvisa politiska initiativ när det gäller cybersäkerhet, för att främja praktiskt samarbete både medlemsstaterna emellan och mellan medlemsstaterna och EU:s institutioner, byråer och organ.

(10) Inom ramen för beslut 2004/97/EG, Euratom, som antogs vid Europeiska rådets möte den 13 december 2003, beslutade medlemsstaternas företrädare att Enisa skulle ha sitt säte i en stad i Grekland som skulle fastställas av den grekiska regeringen. Byråns värdmedlemsstat bör säkerställa bästa möjliga förutsättningar för en smidig och effektiv drift av byrån. Det är mycket viktigt att byrån är förlagd till en lämplig plats,

[33] Europaparlamentets och rådets förordning (EU) nr 526/2013 av den 21 maj 2013 om Europeiska unionens byrå för nät- och informationssäkerhet (Enisa) och om upphävande av förordning (EG) nr 460/2004 (EUT L 165, 18.6.2013, s. 41).

där det bland annat finns lämpliga transportförbindelser och faciliteter för makar och barn som medföljer byråns personal, för att byrån ska kunna utföra sina uppgifter väl och effektivt samt för möjligheterna att rekrytera och behålla personal och för en effektivare nätverksverksamhet. De nödvändiga arrangemangen bör efter godkännande av byråns styrelse fastställas i ett avtal mellan byrån och värdmedlemsstaten.

(11) Med tanke på de ökande cybersäkerhetsutmaningar som unionen står inför bör de ekonomiska och personella resurser som anslagits för byrån ökas för att återspegla dess förstärkta roll och arbetsuppgifter och dess centrala position i ekosystemet av organisationer som försvarar det europeiska digitala ekosystemet.

(12) Byrån bör utveckla och upprätthålla en hög nivå av expertis och fungera som en referenspunkt och skapa förtroende och tillit för den inre marknaden genom sin opartiskhet, kvaliteten på de råd och den information den tillhandahåller, öppenheten i dess förfaranden och arbetssätt samt genom ett kompetent utförande av sina uppgifter. Byrån bör aktivt bidra till nationella insatser och unionsinsatser och utföra sina uppgifter i fullt samarbete med unionens institutioner, organ, kontor och byråer samt medlemsstaterna. Byrån bör också stödja sig på synpunkter från och samarbete med den privata sektorn och andra berörda aktörer. Genom en uppsättning uppgifter bör det fastställas hur byrån ska uppnå sina mål samtidigt som flexibilitet i verksamheten möjliggörs.

(13) Byrån bör bistå kommissionen med råd, yttranden och analyser i alla unionsfrågor som rör utveckling, uppdatering och översyn av politik och lagstiftning på cybersäkerhetsområdet, inbegripet skydd av kritisk infrastruktur och cyberresiliens. Byrån bör fungera som en referenspunkt för rådgivning och expertis för unionens sektorsspecifika politik och lagstiftningsinitiativ i frågor som rör cybersäkerhet.

(14) De underliggande uppgiften för byrån är att främja ett konsekvent genomförande av den gällande rättsliga ramen, i synnerhet ett effektivt genomförande av it-säkerhetsdirektivet, vilket är viktigt för att öka cyberresiliensen. Mot bakgrund av det snabbt föränderliga hotlandskapet på cybersäkerhetsområdet är det uppenbart att medlemsstaterna måste stödjas genom en mer omfattande tvärpolitisk strategi för att bygga upp cyberresiliens.

(15) Byrån bör bistå medlemsstaterna och unionens institutioner, organ, kontor och byråer i deras arbete för att bygga upp och förbättra kapacitet och beredskap för att förebygga, spåra och reagera på cybersäkerhetsproblem och -incidenter samt i fråga om säkerhet i nät- och informationssystem. Byrån bör särskilt stödja utvecklingen och stärkandet av nationella CSIRT-enheter, i syfte att uppnå en hög gemensam mognadsnivå för dem i unionen. Byrån bör också bistå med utveckling och uppdatering av unionens och medlemsstaternas strategier för säkerhet i nät- och informationssystem, särskilt för cybersäkerhet, främja deras spridning och följa upp hur de genomförs. Byrån bör också erbjuda utbildning och utbildningsmaterial till offentliga organ, och vid behov ”utbilda utbildarna”, för att bistå medlemsstaterna när de utvecklar sin egen utbildningskapacitet.

(16) Byrån bör bistå den samarbetsgrupp som inrättas genom it-säkerhetsdirektivet vid utförandet av dess uppgifter, särskilt genom att tillhandahålla expertis och rådgivning och underlätta utbytet av bästa praxis, särskilt i fråga om identifiering av leverantörer av samhällsviktiga tjänster, även i samband med gränsöverskridande beroenden, vad gäller risker och incidenter.

(17) I syfte att stimulera samarbete mellan offentlig och privat sektor och inom den privata sektorn, särskilt för att stödja skyddet av kritisk infrastruktur, bör byrån underlätta inrättandet av sektorsvisa centrum för informationsutbyte och analys (ISAC) genom att tillhandahålla bästa praxis och vägledning om tillgängliga verktyg och förfaranden samt ge vägledning om hantering av regleringsfrågor som rör informationsutbyte.

(18) Byrån bör sammanställa och analysera nationella rapporter från CSIRT-enheter och CERT-EU samt upprätta gemensamma regler, gemensamt språk och gemensam terminologi för utbyte av information. Byrån bör även engagera den privata sektorn, inom ramen för it-säkerhetsdirektivet som lade grunden för frivilligt utbyte av teknisk information på operativ nivå med inrättandet av CSIRT-nätverket.

(19) Byrån bör bidra till insatser på EU-nivå i samband med storskaliga gränsöverskridande cybersäkerhetsincidenter och -kriser. Denna funktion bör omfatta insamling av relevant information och att fungera som kontaktpunkt mellan CSIRT-nätverket och såväl tekniska aktörer som beslutsfattare med ansvar för krishantering. Vidare skulle byrån kunna stödja hanteringen av incidenter ur ett tekniskt perspektiv genom att underlätta utbyte av relevanta tekniska lösningar mellan medlemsstaterna och genom att ge input till kommunikation med allmänheten. Byrån bör stödja processen genom att granska formerna för sådant samarbete genom årliga cybersäkerhetsövningar.

(20) För att utföra sina operativa uppgifter bör byrån använda tillgänglig expertis från CERT-EU genom ett strukturerat och fysiskt mycket nära samarbete. Det strukturerade samarbetet kommer att underlätta synergier och uppbyggnad av Enisas expertis. Vid behov bör särskilda arrangemang mellan de båda organisationerna inrättas för att definiera det praktiska genomförandet av detta samarbete.

(21) I överensstämmelse med sina operativa uppgifter bör byrån kunna tillhandahålla stöd till medlemsstaterna, till exempel genom att ge råd eller tekniskt bistånd, eller säkerställa analyser av hot och incidenter. I kommissionens rekommendation om samordnade insatser vid storskaliga cybersäkerhetsincidenter och cyberkriser rekommenderas medlemsstaterna att samarbeta i god tro och utbyta information sinsemellan och med Enisa om storskaliga cyberinsäkerhetsincidenter och cyberkriser utan onödigt dröjsmål. Sådan information bör hjälpa Enisa att utföra sina operativa uppgifter.

(22) Som en del av det löpande samarbetet på teknisk nivå för att stödja en gemensam situationsmedvetenhet i unionen bör byrån regelbundet ta fram tekniska EU-lägesrapporter om cyberincidenter och cyberhot, baserade på allmänt tillgänglig information, sin egen analys och rapporter som den får från medlemsstaternas CSIRT-enheter (på frivillig basis) eller de gemensamma kontaktpunkterna enligt direktivet om nät- och informationssäkerhet, det Europeiska it-brottscentrumet (EC3) vid Europol, CERT-EU och, i tillämpliga fall, Europeiska unionens underrättelseanalyscentrum (Intcen) vid Europeiska utrikestjänsten (EEAS). Rapporten bör göras tillgänglig för berörda enheter inom rådet, kommissionen, unionens höga representant för utrikes frågor och säkerhetspolitik samt CSIRT-nätverket.

(23) Tekniska utredningar efter incidenter med betydande konsekvenser i fler än en medlemsstat, som stöds eller genomförs av byrån på begäran av eller efter överenskommelse med de berörda medlemsstaterna, bör inriktas på att förhindra framtida incidenter och utföras utan att det påverkar rättsliga eller administrativa förfaranden för fördelning av skuld eller ansvar.

(24) De berörda medlemsstaterna bör tillhandahålla nödvändig information och assistans till byrån för genomförandet av utredningen, utan att det påverkar tillämpningen av artikel 346 i fördraget om Europeiska unionens funktionssätt, eller av andra skäl som rör allmän ordning.

(25) Medlemsstaterna kan uppmana företag som berörs av incidenten att samarbeta genom att tillhandahålla nödvändig information och assistans till byrån utan att det påverkar deras rätt att skydda kommersiellt känslig information,

(26) För att bättre förstå utmaningarna inom cybersäkerhetsområdet, och i syfte att tillhandahålla strategisk långsiktig rådgivning till medlemsstaterna och unionens institutioner, behöver byrån analysera nuvarande och framväxande risker. För detta ändamål bör byrån i samarbete med medlemsstaterna och, om lämpligt, med statistikorgan och andra samla in relevant information och utföra analyser av framväxande teknik och tillhandahålla ämnesspecifika bedömningar om förväntade samhälleliga, rättsliga, ekonomiska och regleringsmässiga konsekvenser av tekniska innovationer inom området nät- och informationssäkerhet, i synnerhet cybersäkerhet. Byrån bör också hjälpa medlemsstaterna och unionens institutioner, byråer och organ att identifiera framväxande trender och förebygga problem som rör cybersäkerhet, genom att utföra analyser av hot och incidenter.

(27) För att stärka unionens resiliens bör byrån utveckla spetskompetens i fråga om säkerhet för internetinfrastruktur och för de kritiska infrastrukturerna, genom att tillhandahålla rådgivning, vägledning och bästa praxis. För att säkerställa enklare tillgång till bättre strukturerad information om cybersäkerhetsrisker och möjliga motåtgärder bör byrån utarbeta och upprätthålla unionens ”informationsnav”, en gemensam webbportal som förser allmänheten med information om cybersäkerhet från EU:s och medlemsstaternas institutioner, organ och byråer.

(28) Byrån bör bidra till att öka allmänhetens medvetenhet om cybersäkerhetsrisker och ge vägledning om god praxis för enskilda användare riktad till privatpersoner och organisationer. Byrån bör även bidra till att främja bästa praxis och lösningar för enskilda och organisationer genom att samla in och analysera offentligt tillgänglig information om betydande incidenter och genom att sammanställa rapporter i syfte att ge vägledning till företag och privatpersoner och att höja den allmänna beredskaps- och resiliensnivån. Byrån bör vidare, i samarbete med medlemsstaterna och unionens institutioner, organ, kontor och byråer, organisera informations- och folkbildningskampanjer riktade till slutanvändare, i syfte att främja ett säkrare beteende bland enskilda internetanvändare och höja medvetenheten om de potentiella hoten i cyberrymden, bland annat it-brottslighet såsom phishingattacker, botnät, ekonomiska bedrägerier och bankbedrägerier, samt främja grundläggande rådgivning om autentisering och dataskydd. Byrån bör spela en central roll när det gäller att höja slutanvändarnas medvetenhet om enheters säkerhet.

(29) För att stödja både de företag som verkar inom den europeiska cybersäkerhetssektorn och användarna av cybersäkerhetslösningar bör byrån utveckla och upprätthålla ett ”marknadsobservatorium” genom att utföra regelbundna analyser och spridning av de viktigaste trenderna på cybersäkerhetsmarknaden, både på tillgångs- och efterfrågesidan.

(30) För att se till att byrån fullt ut uppnår sina mål bör den samarbeta med berörda institutioner, byråer och organ, däribland CERT-EU, Europeiska it-brottscentrumet (EC3) vid Europol, Europeiska försvarsbyrån (EDA), Europeiska byrån för den operativa förvaltningen av stora it-system (eu-LISA), Europeiska byrån för

luftfartssäkerhet (Easa) och andra EU-organ som arbetar med cybersäkerhet. Byrån bör också samverka med myndigheter som hanterar dataskydd för att utbyta sakkunskap och bästa praxis samt ge råd om cybersäkerhetsaspekter som kan påverka deras arbete. Företrädare för medlemsstaternas och unionens rättsvårdande myndigheter och dataskyddsmyndigheter bör ha rätt att företrädas i byråns ständiga intressentgrupp. I samarbetet med rättsvårdande organ om nät- och informationssäkerhetsaspekter som kan påverka deras arbete bör byrån använda existerande informationskanaler och etablerade nätverk.

(31) Byrån, som en medlem i CSIRT-nätverket som dessutom tillhandahåller dess sekretariat, bör stödja medlemsstaternas CSIRT-enheter och CERT-EU i det operativa samarbetet med alla relevanta uppgifter för CSIRT-nätverket som fastställs i it-säkerhetsdirektivet. Byrån bör dessutom främja och stödja samarbete mellan de berörda CSIRT-enheterna i händelse av incidenter, attacker mot eller störningar i de nät eller den infrastruktur som förvaltas eller skyddas av dem och som berör eller potentiellt kan beröra minst två CERT, och därvid beakta CSIRT-nätverkets operationella standardförfaranden.

(32) För att öka unionens beredskap att hantera cybersäkerhetsincidenter bör byrån organisera årliga cybersäkerhetsövningar på unionsnivå och, på deras begäran, bistå medlemsstaterna och EU:s institutioner, byråer och organ med att organisera övningar.

(33) Byrån bör vidareutveckla och upprätthålla sina kunskaper om cybersäkerhetscertifiering för att stödja unionens politik på detta område. Byrån bör främja spridningen av cybersäkerhetscertifiering i unionen, bland annat genom att bidra till inrättandet och upprätthållandet av en ram för cybersäkerhetscertifiering på unionsnivå, i syfte att öka öppenheten i fråga om assuransnivån för cybersäkerhet hos IKT-produkter och IKT-tjänster och därigenom stärka förtroendet för den digitala inre marknaden.

(34) Effektiva cybersäkerhetsstrategier bör bygga på välutvecklade metoder för riskbedömning, både inom den offentliga och den privata sektorn. Riskbedömningsmetoder används på olika nivåer, men det saknas gemensam praxis för hur de ska tillämpas på ett effektivt sätt. Främjande och utveckling av bästa praxis för riskbedömning och för interoperabla lösningar för riskhantering inom organisationer i den offentliga och privata sektorn kommer att höja cybersäkerhetsnivån i unionen. Därför bör byrån stödja samarbete mellan intressenter på unionsnivå och främja deras insatser för upprättande och tillämpning av europeiska och internationella standarder för riskhantering och mätbar säkerhet för elektroniska produkter, system, nät och tjänster som tillsammans med programvara utgör nät- och informationssystemen.

(35) Byrån bör uppmuntra medlemsstaterna och tjänsteleverantörerna att höja sina allmänna säkerhetsstandarder så att alla internetanvändare kan vidta de åtgärder som krävs för att trygga sin egen cybersäkerhet. I synnerhet bör tjänsteleverantörer och produkttillverkare återkalla eller återvinna produkter och tjänster som inte uppfyller cybersäkerhetsstandarderna. I samarbete med de behöriga myndigheterna kan Enisa sprida uppgifter om cybersäkerhetsnivån för de produkter och tjänster som erbjuds på den inre marknaden, och utfärda varningar riktade till leverantörer och tillverkare och ålägga dem att förbättra sina produkters och tjänsters säkerhet, inbegripet cybersäkerhet.

(36) Byrån bör i sitt arbete fullt ut beakta pågående forskning, utveckling och tekniska bedömningar, i synnerhet sådan verksamhet som bedrivs inom unionens olika

forskningsinitiativ för att ge råd till unionens institutioner, organ, kontor och byråer och, i tillämpliga fall, till medlemsstaterna på deras begäran om forskningsbehoven på området nät- och informationssäkerhet, särskilt cybersäkerhet.

(37) Cybersäkerhetsproblem är globala frågor. Det behövs ett tätare internationellt samarbete för att förbättra säkerhetsstandarder, bland annat genom att fastställa gemensamma beteendenormer, och informationsutbyte, och på så vis främja snabbare internationellt samarbete som svar på, och en gemensam global syn på, nät- och informationssäkerhetsproblem. Därför bör byrån stödja ett starkare unionsdeltagande och samarbete med tredjeländer och internationella organisationer genom att, när så är lämpligt, tillhandahålla nödvändig expertis och nödvändiga analyser till berörda unionsinstitutioner, -organ, -kontor och -byråer.

(38) Byrån bör kunna besvara ad hoc-förfrågningar om råd och bistånd från medlemsstaterna och EU:s institutioner, byråer och organ som omfattas av byråns mål.

(39) Vissa principer för byråns förvaltning behöver genomföras för att den ska vara förenlig med det gemensamma uttalande och den gemensamma ansats som den interinstitutionella arbetsgruppen för EU:s decentraliserade byråer enades om i juli 2012 och vars syfte är att effektivisera byråernas verksamhet och förbättra deras resultat. Det gemensamma uttalandet och den gemensamma ansatsen bör också på lämpligt sätt återspeglas i byråns arbetsprogram, i utvärderingar av byrån och i byråns rapportering och administration.

(40) Styrelsen, som består av företrädare för medlemsstaterna och kommissionen, bör fastställa den allmänna inriktningen för byråns verksamhet och se till att den utför sina uppgifter i enlighet med denna förordning. Styrelsen bör ha de nödvändiga befogenheterna för att fastställa budgeten och kontrollera att den genomförs, anta lämpliga finansiella bestämmelser, utarbeta klara och tydliga förfaranden för byråns beslutsfattande, anta byråns samlade programdokument, anta sin egen arbetsordning, utse den verkställande direktören, besluta om förlängning av hans eller hennes mandat och om avslutande av mandatet.

(41) För att byrån ska fungera väl och effektivt bör kommissionen och medlemsstaterna säkerställa att personer som utses till styrelseledamöter har lämplig yrkesmässig expertis och erfarenhet inom funktionella områden. Medlemsstaterna och kommissionen bör även eftersträva att begränsa omsättningen av deras respektive företrädare i styrelsen i syfte att skapa kontinuitet i dess arbete.

(42) För att byrån ska fungera väl bör den verkställande direktören utses på grundval av meriter, dokumenterad skicklighet i förvaltning och ledarskap samt kompetens och erfarenheter som rör cybersäkerhet, och den verkställande direktörens uppgifter bör utföras med fullständigt oberoende. Den verkställande direktören bör utarbeta ett förslag till arbetsprogram för byrån, efter samråd med kommissionen, och vidta alla åtgärder som är nödvändiga för att säkerställa att byråns arbetsprogram genomförs på rätt sätt. Den verkställande direktören bör utarbeta en årsrapport som föreläggs styrelsen och upprätta en preliminär beräkning av byråns inkomster och utgifter samt genomföra budgeten. Den verkställande direktören bör också ha möjlighet att inrätta tillfälliga arbetsgrupper som i synnerhet ska behandla vetenskapliga, tekniska, rättsliga eller socioekonomiska frågor. Den verkställande direktören bör se till att de tillfälliga arbetsgruppernas medlemmar väljs med utgångspunkt i högsta möjliga standard när det gäller expertkunskaper, med beaktande av att det, utifrån de specifika frågor som berörs, ska finnas en representativ balans mellan medlemsstaternas förvaltningar,

unionens institutioner och den privata sektorn, inklusive branschen, användare och akademiska experter på nät- och informationssäkerhet.

(43) Direktionen bör bidra till att styrelsen fungerar på ett effektivt sätt. Som ett led i det förberedande arbetet i samband med styrelsens beslut bör den i detalj granska relevant information och utforska tillgängliga alternativ och ge råd och lösningar för att utarbeta relevanta beslut av styrelsen.

(44) Byrån bör ha en ständig intressentgrupp som rådgivande organ, för att säkerställa en regelbunden dialog med den privata sektorn, konsumentorganisationer och andra berörda intressenter. Den ständiga intressentgruppen, som inrättas av styrelsen på förslag av den verkställande direktören, bör koncentrera sig på frågor som är relevanta för intressenter och uppmärksamma byrån på dem. Den ständiga intressentgruppens sammansättning och de uppgifter som anförtrotts denna grupp, som särskilt rådfrågas om utkastet till arbetsprogram, bör säkerställa en tillräcklig representation av intressenter i byråns arbete.

(45) Byrån bör ha regler för förebyggande och hantering av intressekonflikter. Byrån bör också tillämpa relevanta unionsbestämmelser om allmänhetens tillgång till handlingar enligt Europaparlamentets och rådets förordning (EG) nr 1049/2001[34]. Byråns behandling av personuppgifter bör ske i enlighet med Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter[35]. Byrån bör efterleva de bestämmelser som gäller för unionens institutioner och den nationella lagstiftning som rör hantering av information, i synnerhet känsliga icke-säkerhetsskyddsklassificerade uppgifter och säkerhetsskyddsklassificerade EU-uppgifter.

(46) För att garantera byråns autonomi och oberoende och ge den möjlighet att utföra kompletterande och nya uppgifter, också oförutsedda uppgifter i en krissituation, bör den ges en tillräcklig egen budget där intäkterna främst består av ett bidrag från unionen och bidrag från tredjeländer som deltar i byråns arbete. Huvuddelen av byråns personal bör vara direkt delaktig i det operativa genomförandet av byråns mandat. Värdmedlemsstaten, eller varje annan medlemsstat, bör ha rätt att lämna frivilliga bidrag till byråns intäkter. Unionens budgetförfarande bör även i fortsättningen tillämpas på de bidrag som belastar unionens allmänna budget. Dessutom bör revisionsrätten granska byråns räkenskaper för att säkerställa insyn och ansvarighet.

(47) Bedömning av överensstämmelse är den process där det visas om specificerade krav avseende en produkt, en process, en tjänst, ett system, en person eller ett organ har uppfyllts. I denna förordning bör certifiering betraktas som en typ av bedömning av överensstämmelse när det gäller cybersäkerhetsegenskaperna hos en produkt, en process, en tjänst, ett system eller en kombination av dessa (”IKT-produkter och IKT-tjänster”) som utförs av en oberoende tredje part, annan än produkttillverkaren eller tjänsteleverantören. Certifiering utgör inte i sig någon garanti för att certifierade IKT-produkter och IKT-tjänster är cybersäkra. Den är snarare ett förfarande och en teknisk metod för att intyga att IKT-produkter och IKT-tjänster har testats och att de uppfyller vissa cybersäkerhetskrav som fastställs på annan plats, till exempel i tekniska standarder.

---

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

[35] EGT L 8, 12.1.2001, s. 1.

(48) Cybersäkerhetscertifiering har stor betydelse för att öka förtroendet för och säkerheten hos IKT-produkter och IKT-tjänster. Den digitala inre marknaden, och särskilt den datadrivna ekonomin och sakernas internet, kan utvecklas framgångsrikt endast om allmänheten litar på att sådana produkter och tjänster har en viss assuransnivå i fråga om cybersäkerhet. Uppkopplade och automatiserade bilar, elektroniska medicintekniska produkter, styrsystem för industriell automation eller smarta elnät är bara några exempel på sektorer inom vilka certifiering redan används eller kan komma att användas i en nära framtid. De sektorer som regleras av it-säkerhetsdirektivet är också sektorer där cybersäkerhetscertifiering är av yttersta vikt.

(49) I sitt meddelande från 2016 *Stärka Europas system för cyberresiliens och främja en konkurrenskraftig och innovativ cybersäkerhetsbransch* tog kommissionen upp behovet av billiga och interoperabla cybersäkerhetsprodukter och cybersäkerhetslösningar av hög kvalitet. Utbudet av IKT-produkter och IKT-tjänster på den inre marknaden är fortfarande i hög grad geografiskt fragmenterat. Cybersäkerhetsbranschen i Europa har till stor del utvecklats med stöd av nationell statlig efterfrågan. Bristen på interoperabla lösningar (tekniska standarder), förfaranden och EU-mekanismer för certifiering är några av de andra faktorer som påverkar den inre marknaden för cybersäkerhet. Detta gör det svårt för de europeiska företagen att konkurrera på nationell, europeisk och global nivå. Det minskar också utbudet av livskraftig och användbar cybersäkerhetsteknik som enskilda och företag har tillgång till. Även i halvtidsöversynen av genomförandet av strategin för den digitala inre marknaden underströk kommissionen behovet av säkra uppkopplade produkter och system, och framhöll att skapandet av en europeisk IKT-säkerhetsram med regler om hur IKT-säkerhetscertifiering ska organiseras i unionen kan bevara förtroendet för internet och samtidigt motverka den nuvarande fragmenteringen av marknaden för cybersäkerhet.

(50) För närvarande används cybersäkerhetscertifiering av IKT-produkter och IKT-tjänster endast i begränsad omfattning. I de fall det förekommer är det oftast på medlemsstatsnivå eller inom ramen för industridrivna system. Ett certifikat utfärdat av en nationell cybersäkerhetsmyndighet i ett sådant sammanhang erkänns i princip inte av andra medlemsstater. Företag kan därför behöva certifiera sina produkter och tjänster i flera medlemsstater där de bedriver verksamhet, exempelvis för att kunna delta i nationella upphandlingsförfaranden. Även om nya system utvecklas, tycks det inte finnas någon samlad helhetssyn på övergripande cybersäkerhetsfrågor, exempelvis inom området sakernas internet. Befintliga system uppvisar allvarliga brister och skillnader i fråga om produkttäckning, assuransnivå, grundläggande kriterier och faktisk användning.

(51) Vissa ansträngningar har gjorts tidigare för att få till stånd ett ömsesidigt erkännande av certifikat i Europa. De har dock endast delvis varit framgångsrika. Det främsta exemplet är det avtal om ömsesidigt erkännande (MRA) som ingåtts inom gruppen av höga tjänstemän på informationssäkerhetsområdet (SOG-IS). Även om det är den viktigaste modellen för samarbete och ömsesidigt erkännande av säkerhetscertifiering uppvisar SOG-IS-avtalet vissa betydande brister i form av höga kostnader och begränsat tillämpningsområde. Hittills har bara ett fåtal skyddsprofiler för digitala produkter utvecklats, t.ex. digitala signaturer, digitala färdskrivare och smartkort. Viktigast av allt är att SOG-IS endast omfattar vissa av unionens medlemsstater. Detta har begränsat SOG-IS-avtalets effektivitet för den inre marknaden.

(52) Mot bakgrund av ovanstående är det nödvändigt att inrätta en europeisk ram för cybersäkerhetscertifiering som fastställer de viktigaste övergripande kraven för

europeiska system för cybersäkerhetscertifiering som ska utvecklas, och som gör att certifikat för IKT-produkter och IKT-tjänster kan erkännas och användas i samtliga medlemsstater. Den europeiska ramen bör ha ett dubbelt syfte: Å ena sidan bör den bidra till att öka förtroendet för IKT-produkter och IKT-tjänster som har certifierats enligt sådana system. Å andra sidan bör den undvika att det uppstår flera olika motstridiga eller överlappande nationella cybersäkerhetscertifieringar och därmed minska kostnaderna för företag som är verksamma på den digitala inre marknaden. Systemen bör vara icke-diskriminerande och grundas på internationella och/eller unionens standarder såvida inte dessa standarder är ineffektiva eller olämpliga för att förverkliga EU:s legitima mål i detta avseende.

(53) Kommissionen bör ges befogenhet att anta europeiska system för cybersäkerhetscertifiering för särskilda grupper av IKT-produkter och IKT-tjänster. Dessa system bör genomföras och övervakas av nationella tillsynsmyndigheter för certifiering, och certifikat utfärdade enligt dessa system bör vara giltiga och erkännas i hela unionen. Certifieringssystem som drivs av industrin eller andra privata organisationer bör inte ingå i förordningens tillämpningsområde. De organ som handhar sådana system kan dock föreslå kommissionen att överväga sådana system som en grund för att godkänna dem som ett europeiskt system.

(54) Bestämmelserna i denna förordning bör inte påverka tillämpningen av unionslagstiftning som innehåller särskilda bestämmelser om certifiering av IKT-produkter och IKT-tjänster. Särskilt den allmänna dataskyddsförordningen innehåller bestämmelser för införandet av certifieringsmekanismer samt sigill och märkningar för dataskydd för att visa att personuppgiftsansvarigas eller personuppgiftsbiträdens uppgiftsbehandling är förenlig med den förordningen. Dessa certifieringsmekanismer samt sigill och märkningar för dataskydd bör göra det möjligt för de registrerade att snabbt bedöma dataskyddsnivån för relevanta produkter och tjänster. Den här förordningen påverkar inte certifieringen av uppgiftsbehandling, inte heller om denna verksamhet ingår i produkter och tjänster, enligt den allmänna dataskyddsförordningen.

(55) Syftet med europeiska system för cybersäkerhetscertifiering bör vara att se till att IKT-produkter och IKT-tjänster som certifierats enligt ett sådant system uppfyller de angivna kraven. Dessa krav gäller förmågan att, vid en viss assuransnivå, stå emot åtgärder som syftar till att äventyra tillgängligheten, autenticiteten, integriteten och konfidentialiteten hos lagrade eller överförda eller behandlade uppgifter eller de därmed sammanhängande funktioner eller tjänster som tillhandahålls av eller är tillgängliga via dessa produkter, processer, tjänster och system i den mening som avses i denna förordning. Det är inte möjligt att i denna förordning i detalj fastställa cybersäkerhetskraven för alla IKT-produkter och IKT-tjänster. IKT-produkter och IKT-tjänster och relaterade cybersäkerhetsbehov är så olikartade att det är mycket svårt att ta fram allmänna cybersäkerhetskrav som är giltiga över hela linjen. Det är därför nödvändigt att anta ett brett och allmänt cybersäkerhetsbegrepp när det gäller certifieringsändamål, kompletterat med en uppsättning specifika cybersäkerhetmål som måste beaktas vid utformningen av europeiska system för cybersäkerhetscertifiering. Formerna för att uppnå dessa mål i specifika IKT-produkter och IKT-tjänster bör sedan fastställas i detalj för det enskilda certifieringssystem som antas av kommissionen, till exempel genom hänvisningar till standarder eller tekniska specifikationer.

(56) Kommissionen bör ges befogenhet att begära att Enisa förbereder förslag till system för särskilda IKT-produkter eller IKT-tjänster. Kommissionen bör, på grundval av

Enisas förslag till system, ges befogenhet att anta det europeiska certifieringssystemet genom genomförandeakter. Med beaktande av det allmänna syfte och de säkerhetsmål som fastställs i denna förordning bör det i europeiska certifieringssystem som antas av kommissionen specificeras en minimiuppsättning komponenter avseende det enskilda systemets föremål, tillämpningsområde och funktionssätt. Dessa bör bland annat omfatta cybersäkerhetscertifieringens tillämpningsområde och föremål, inklusive de kategorier av IKT-produkter och IKT-tjänster som omfattas, den detaljerade specifikationen av cybersäkerhetskraven, exempelvis genom hänvisning till standarder eller tekniska specifikationer, de särskilda utvärderingskriterierna och utvärderingsmetoderna samt den avsedda assuransnivån: grundläggande, betydande och/eller hög.

(57) Användningen av europeisk cybersäkerhetscertifiering bör vara frivillig, om inte annat föreskrivs i unionslagstiftning eller nationell lagstiftning. I syfte att uppnå målen för denna förordning och undvika en fragmentering av den inre marknaden, bör dock nationella system eller förfaranden för cybersäkerhetscertifiering av IKT-produkter och IKT-tjänster som omfattas av ett europeiskt system för cybersäkerhetscertifiering upphöra att ha verkan från och med den dag som fastställs av kommissionen genom en genomförandeakt. Vidare bör medlemsstaterna inte införa nya nationella certifieringssystem som tillhandahåller cybersäkerhetscertifiering av IKT-produkter och IKT-tjänster som redan omfattas av ett befintligt europeiskt system för cybersäkerhetscertifiering.

(58) När ett europeiskt system för cybersäkerhetscertifiering har antagits bör tillverkarna av IKT-produkter och leverantörerna av IKT-tjänster kunna lämna in en ansökan om certifiering av sina produkter och tjänster till valfritt organ för bedömning av överensstämmelse. Organen för bedömning av överensstämmelse bör ackrediteras av ett ackrediteringsorgan, om de uppfyller vissa krav som fastställs i denna förordning. Ackrediteringen bör utfärdas för en period på högst fem år och kan förnyas på samma villkor under förutsättning att organet för bedömning av överensstämmelse uppfyller kraven. Ackrediteringsorganet bör återkalla ackrediteringen av ett organ för bedömning av överensstämmelse om villkoren för ackrediteringen inte, eller inte längre, uppfylls eller om åtgärder som vidtagits av organet för bedömning av överensstämmelse strider mot denna förordning.

(59) Det är nödvändigt att kräva att alla medlemsstater utser en tillsynsmyndighet för cybersäkerhetscertifiering som övervakar att organen för bedömning av överensstämmelse och de certifikat som utfärdas av organ för bedömning av överensstämmelse som är etablerade på deras territorium uppfyller kraven i denna förordning och de relevanta systemen för cybersäkerhetscertifiering. De nationella tillsynsmyndigheterna för certifiering bör behandla klagomål som lämnas in av fysiska eller juridiska personer avseende certifikat som utfärdats av organ för bedömning av överensstämmelse som är etablerade på deras territorier, i lämplig utsträckning undersöka det ärende som klagomålet gäller och underrätta anmälaren om utvecklingen och resultatet av utredningen inom rimlig tid. De bör dessutom att samarbeta med andra nationella tillsynsmyndigheter för certifiering eller någon annan offentlig myndighet, bland annat genom att utbyta information om IKT-produkter och IKT-tjänster som eventuellt avviker från kraven i denna förordning eller särskilda system för cybersäkerhet.

(60) För att säkerställa en konsekvent tillämpning av den europeiska ramen för cybersäkerhetscertifiering bör det inrättas en europeisk grupp för cybersäkerhetscertifiering (nedan kallad *gruppen*), bestående av nationella

tillsynsmyndigheter. Gruppens främsta uppgifter bör vara att ge kommissionen råd och bistånd i dess arbete för att säkerställa konsekvent genomförande och tillämpning av den europeiska ramen för cybersäkerhetscertifiering, att bistå och ha ett nära samarbete med byrån i utarbetandet av förslag till system för cybersäkerhetscertifiering, att rekommendera kommissionen att uppmana byrån att utarbeta ett förslag till europeiskt system för cybersäkerhetscertifiering samt att anta yttranden till kommissionen rörande underhåll och översyn av befintliga europeiska system för cybersäkerhetscertifiering.

(61) För att öka medvetenheten och underlätta acceptansen för EU:s framtida cybersäkerhetssystem kan Europeiska kommissionen utfärda allmänna eller sektorsspecifika cybersäkerhetsriktlinjer, t.ex. vad gäller god praxis för cybersäkerhet eller ansvarsfullt cybersäkerhetsbeteende som belyser de positiva konsekvenserna av att använda certifierade IKT-produkter och IKT-tjänster.

(62) Byråns stöd till cybersäkerhetscertifiering bör också omfatta samverkan med rådets säkerhetskommitté och det berörda nationella organet, i fråga om kryptografiskt godkännande av produkter som ska användas i sekretessbelagda nätverk.

(63) I syfte att ytterligare specificera kriterierna för ackreditering av organ för bedömning av överensstämmelse bör befogenheten att anta akter i enlighet med artikel 290 i fördraget om Europeiska unionens funktionssätt delegeras till kommissionen. Kommissionen bör genomföra lämpliga samråd under sitt förberedande arbete, inklusive på expertnivå. Dessa samråd bör genomföras i enlighet med principerna i det interinstitutionella avtalet om bättre lagstiftning av den 13 april 2016. För att säkerställa lika stor delaktighet i förberedelsen av delegerade akter bör Europaparlamentet och rådet erhålla alla handlingar samtidigt som medlemsstaternas experter, och deras experter bör systematiskt ges tillträde till möten i kommissionens expertgrupper som arbetar med förberedelse av delegerade akter.

(64) För att säkerställa enhetliga villkor för tillämpningen av denna förordning bör kommissionen ges genomförandebefogenheter i enlighet med denna förordning. Dessa befogenheter bör utövas i enlighet med förordning (EU) nr 182/2011.

(65) Granskningsförfarandet bör användas för antagande av genomförandeakter om europeiska system för cybersäkerhetscertifiering av IKT-produkter och IKT-tjänster, om formerna för att genomföra utredningar av byrån samt om förhållanden, format och förfaranden för anmälningar av ackrediterade organ för bedömning av överensstämmelse från de nationella tillsynsmyndigheterna för certifiering till kommissionen.

(66) Byråns verksamhet bör utvärderas på ett oberoende sätt. Utvärderingen bör beakta byråns måluppfyllelse, dess arbetsmetoder och relevansen i dess uppgifter. Utvärderingen bör även bedöma konsekvenserna, ändamålsenligheten och effektiviteten i fråga om den europeiska ramen för cybersäkerhetscertifiering.

(67) Förordning (EU) nr 526/2013 bör upphävas.

(68) Eftersom målen för denna förordning inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare 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 denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

AVDELNING I
ALLMÄNNA BESTÄMMELSER

Artikel 1
Syfte och tillämpningsområde

I syfte att säkerställa en väl fungerande inre marknad och samtidigt sträva efter en hög nivå i fråga om cybersäkerhet, cyberresiliens och förtroende inom unionen, ska denna förordning

(a) fastställa mål, uppgifter och organisatoriska aspekter för Enisa, ”EU:s cybersäkerhetsbyrå”, nedan kallad *byrån*, och

(b) fastställa en ram för inrättandet av europeiska system för cybersäkerhetscertifiering i syfte att säkerställa en tillfredsställande nivå i fråga om cybersäkerhet för IKT-produkter och IKT-tjänster i unionen. En sådan ram ska användas utan att det påverkar tillämpningen av särskilda bestämmelser om frivillig eller obligatorisk certifiering i andra unionsakter.

Artikel 2
Definitioner

I denna förordning gäller följande definitioner:

(1) *cybersäkerhet*: all verksamhet som är nödvändig för att skydda nät- och informationssystem, deras användare och berörda personer mot cyberhot.

(2) *nät- och informationssystem*: ett system i den mening som avses i artikel 4.1 i direktiv (EU) 2016/1148.

(3) *nationell strategi för säkerheten i nät- och informationssystem*: en ram i den mening som avses i artikel 4.3 i direktiv (EU) 2016/1148.

(4) *leverantör av samhällsviktiga tjänster*: en offentlig eller privat enhet enligt definitionen i artikel 4.4 i direktiv (EU) 2016/1148.

(5) *leverantör av digitala tjänster*: en juridisk person som tillhandahåller en digital tjänst enligt definitionen i artikel 4.6 i direktiv (EU) 2016/1148.

(6) *incident*: en händelse enligt definitionen i artikel 4.7 i direktiv (EU) 2016/1148.

(7) *incidenthantering*: ett förfarande enligt definitionen i artikel 4.8 i direktiv (EU) 2016/1148.

(8) *cyberhot*: en potentiell omständighet eller händelse som på ett negativt sätt kan påverka nät- och informationssystem, deras användare och berörda personer.

(9) *europeiskt system för cybersäkerhetscertifiering*: den vittomfattande uppsättning regler, tekniska krav, standarder och förfaranden som fastställs på unionsnivå och som tillämpas på certifiering av informations- och kommunikationstekniska (IKT) produkter och tjänster som omfattas av tillämpningsområdet för det systemet.

(10) *europeiskt cybersäkerhetscertifikat*: en handling utfärdad av ett organ för bedömning av överensstämmelse som intygar att en viss IKT-produkt eller IKT-tjänst uppfyller de specifika krav som fastställs i ett europeiskt system för cybersäkerhetscertifiering.

(11) *IKT-produkt och IKT-tjänst*: en del, eller grupp av delar, i nät- och informationssystem.

(12) *ackreditering*: ackreditering enligt definitionen i artikel 2.10 i förordning (EG) nr 765/2008.

(13) *nationellt ackrediteringsorgan*: ett nationellt ackrediteringsorgan enligt definitionen i artikel 2.11 i förordning (EG) nr 765/2008.

(14) *bedömning av överensstämmelse*: bedömning av överensstämmelse enligt definitionen i artikel 2.12 i förordning (EG) nr 765/2008.

(15) *organ för bedömning av överensstämmelse*: organ för bedömning av överensstämmelse enligt definitionen i artikel 2.13 i förordning (EG) nr 765/2008.

(16) *standard*: en standard enligt definitionen i artikel 2.1 i förordning (EU) nr 1025/2012.

AVDELNING II
Enisa – ”EU:s cybersäkerhetsbyrå”

KAPITEL I
MANDAT, MÅL OCH UPPGIFTER

Artikel 3
Mandat

1. Byrån ska utföra de uppgifter som den tilldelas genom denna förordning i syfte att bidra till en hög nivå i fråga om cybersäkerhet inom unionen.
2. Byrån ska utföra uppgifter som den tilldelas genom unionsakter som fastställer åtgärder för tillnärmning av de bestämmelser i medlemsstaternas lagar och andra författningar som rör cybersäkerhet.
3. Byråns mål och uppgifter ska inte påverka medlemsstaternas befogenheter i fråga om cybersäkerhet, särskilt inte verksamhet som berör allmän säkerhet, försvar, nationell säkerhet och statens verksamhet på strafflagstiftningens område.

Artikel 4
Mål

1. Byrån ska vara ett expertcentrum inom området cybersäkerhet genom sitt oberoende, den vetenskapliga och tekniska kvaliteten på de råd, den assistans och den information den tillhandahåller, öppenheten i dess operativa förfaranden och arbetssätt samt genom ett kompetent utförande av sina uppgifter.
2. Byrån ska bistå unionens institutioner, byråer och organ, samt medlemsstaterna, med utarbetande och genomförande av politiska åtgärder som rör cybersäkerhet.
3. Byrån ska stödja kapacitetsuppbyggnad och beredskap i hela unionen genom att bistå unionen, medlemsstaterna och offentliga och privata intressenter i syfte att öka skyddet av deras nät- och informationssystem, utveckla färdigheter och kompetens inom området cybersäkerhet och uppnå cyberresiliens.
4. Byrån ska främja samarbete och samordning på unionsnivå mellan medlemsstater, unionens institutioner, byråer och organ samt berörda intressenter, inbegripet den privata sektorn, i frågor som rör cybersäkerhet.
5. Byrån ska öka cybersäkerhetskapaciteten på unionsnivå i syfte att komplettera medlemsstaternas åtgärder för att förebygga och vidta åtgärder mot cyberhot, särskilt vid gränsöverskridande incidenter.
6. Byrån ska främja användningen av certifiering, bland annat genom att bidra till inrättandet och upprätthållandet av en ram för cybersäkerhetscertifiering på unionsnivå i enlighet med avdelning III i denna förordning, i syfte att öka transparensen i fråga om assuransnivån för cybersäkerhet hos IKT-produkter och IKT-tjänster och därigenom stärka förtroendet för den digitala inre marknaden.
7. Byrån ska främja en hög medvetenhet hos allmänheten och företagen i frågor som rör cybersäkerhet.

Artikel 5

Uppgifter som rör utarbetande och genomförande av unionens politik och lagstiftning

Byrån ska bidra till utarbetandet och genomförandet av unionens politik och lagstiftning genom att

1. bistå och ge råd, särskilt genom att tillhandahålla oberoende yttranden och förberedande arbete, i fråga om utarbetande och översyn av unionens politik och lagstiftning inom området cybersäkerhet samt sektorsspecifika strategier och lagförslag där frågor som rör cybersäkerhet ingår,
2. hjälpa medlemsstaterna att på ett konsekvent sätt genomföra unionens politik och lagstiftning som rör cybersäkerhet, i synnerhet vad gäller direktiv (EU) 2016/1148, bland annat genom yttranden, riktlinjer, råd och bästa praxis i frågor såsom riskhantering, incidentrapportering och informationsutbyte, samt underlätta utbytet av bästa praxis mellan behöriga myndigheter i detta avseende,
3. bidra till arbetet i samarbetsgruppen enligt artikel 11 i direktiv (EU) 2016/1148 genom att tillhandahålla expertis och bistånd,
4. stödja
    (1) utarbetandet och genomförandet av unionens politik inom området elektronisk identitet och betrodda tjänster, i synnerhet genom att tillhandahålla råd och tekniska riktlinjer, samt underlätta utbytet av bästa praxis mellan behöriga myndigheter,
    (2) främjandet av en högre säkerhetsnivå för elektronisk kommunikation, bland annat genom att tillhandahålla expertis och råd, samt underlätta utbytet av bästa praxis mellan behöriga myndigheter,
5. stödja den regelbundna översynen av unionens politiska verksamhet genom att lägga fram en årlig rapport om hur genomförandet av respektive rättsliga ramar framskrider avseende
    (a) medlemstaternas incidentrapporter som överlämnas av de gemensamma kontaktpunkterna till samarbetsgruppen enligt artikel 10.3 i direktiv (EU) 2016/1148,
    (b) anmälningar om säkerhetsöverträdelser och integritetsförlust vad gäller leverantörerna av betrodda tjänster, som överlämnas av tillsynsorganen till byrån, enligt artikel 19.3 i förordning (EU) nr 910/2014,
    (c) anmälningar om säkerhetsöverträdelser som överlämnats av de företag som tillhandahåller allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster, som överlämnas av de behöriga myndigheterna till byrån, enligt artikel 40 i [direktivet om inrättandet av en europeisk kodex för elektronisk kommunikation].

Artikel 6

Uppgifter som rör kapacitetsuppbyggnad

1. Byrån ska bistå

(a) medlemsstaterna i deras ansträngningar för att förbättra förebyggandet, spårandet och analysen av, samt kapaciteten att reagera på, problem och incidenter inom området cybersäkerhet genom att förse dem med nödvändiga kunskaper och nödvändig expertis,

(b) unionens organ, kontor och byråer i deras ansträngningar för att förbättra förebyggandet, spårandet och analysen av, samt kapaciteten att reagera på, problem och incidenter inom området cybersäkerhet genom lämpligt stöd för CERT för unionens institutioner, byråer och organ (CERT-EU),

(c) medlemsstater, på deras begäran, med inrättandet av nationella enheter för hantering av it-säkerhetsincidenter (Computer Security Incident Response Teams, nedan kallade *CSIRT-enheter*) enligt artikel 9.5 i direktiv (EU) 2016/1148,

(d) medlemsstater, på deras begäran, med utarbetandet av nationella strategier för säkerhet i nät- och informationssystem, enligt artikel 7.2 i direktiv (EU) 2016/1148; byrån ska också främja spridning och övervaka framstegen i genomförandet av dessa strategier i hela unionen i syfte att främja bästa praxis,

(e) unionens institutioner med utarbetandet och översynen av unionens strategier avseende cybersäkerhet och därvid främja deras spridning och övervaka framstegen i genomförandet av dem,

(f) nationella CSIRT-enheter och CSIRT-enheter på unionsnivå i deras arbete för att öka sin kapacitet, bland annat genom att främja dialog och informationsutbyte, för att säkerställa att alla CSIRT-enheter när det gäller den tekniska nivån uppfyller gemensamma minimikrav för kapaciteten och att deras verksamhet följer bästa praxis,

(g) medlemsstaterna genom att organisera årliga storskaliga cybersäkerhetsövningar på unionsnivå enligt artikel 7.6 och genom att avge policyrekommendationer som grundar sig på utvärderingar av övningarna och på lärdomar som dragits av dem,

(h) relevanta offentliga organ genom att erbjuda utbildning om cybersäkerhet, om lämpligt i samarbete med intressenter,

(i) samarbetsgruppen genom att utbyta bästa praxis, i synnerhet för medlemsstaternas identifiering av leverantörer av samhällsviktiga tjänster, inklusive vid gränsöverskridande beroenden, vad gäller risker och incidenter, enligt artikel 11.3 l i direktiv (EU) 2016/1148.

2. Byrån ska underlätta inrättandet av och kontinuerligt stödja sektorsvisa centrum för informationsutbyte och analys (Information Sharing and Analysis Centres, ISAC), i synnerhet i de sektorer som förtecknas i bilaga II till direktiv (EU) 2016/1148, genom att tillhandahålla bästa praxis och vägledning i fråga om tillgängliga verktyg, om förfaranden samt om hur regleringsfrågor som rör informationsutbyte ska hanteras.

Artikel 7

Uppgifter som rör operativt samarbete på unionsnivå

1. Byrån ska stödja operativt samarbete mellan behöriga offentliga organ och mellan intressenter.

2. Byrån ska samarbeta på operativ nivå och skapa synergier med unionens institutioner, organ, kontor och byråer, inbegripet CERT-EU, de enheter som arbetar med it-brottslighet och tillsynsmyndigheter som arbetar med integritets- och personuppgiftsskydd, i syfte att ta itu med frågor av gemensamt intresse, inbegripet

   (a) utbyte av sakkunskap och bästa praxis,

   (b) tillhandahållande av råd och riktlinjer om relevanta frågor som rör cybersäkerhet,

   (c) inrättande, efter samråd med kommissionen, av praktiska arrangemang för utförande av särskilda uppgifter.

3. Byrån ska tillhandahålla sekretariatet för CSIRT-nätverket enligt artikel 12.2 i direktiv (EU) 2016/1148 och ska aktivt underlätta informationsutbytet och samarbetet mellan nätverkets medlemmar.

4. Byrån ska bidra till det operativa samarbetet inom CSIRT-nätverket och stödja medlemsstater genom att

   (a) ge råd om hur de kan förbättra sin kapacitet att förebygga, upptäcka och reagera på incidenter,

   (b) på deras begäran tillhandahålla tekniskt stöd i samband med incidenter som har en betydande eller avsevärd inverkan,

   (c) analysera sårbarheter, artefakter och incidenter.

Vid fullgörandet av dessa uppgifter ska byrån och CERT-EU samarbeta på ett strukturerat sätt för att dra nytta av synergier, särskilt när det gäller operativa aspekter.

5. På begäran av två eller flera berörda medlemsstater, och med det enda syftet att tillhandahålla råd för att förebygga framtida incidenter, ska byrån stödja eller genomföra en teknisk efterhandsundersökning som svar på rapporter från berörda företag om incidenter som har en betydande eller avsevärd inverkan enligt direktiv (EU) 2016/1148. Byrån ska också genomföra en sådan undersökning efter en vederbörligen motiverad begäran från kommissionen, i samförstånd med de berörda medlemsstaterna, om sådana incidenter berör fler än två medlemsstater.

   Omfattningen av undersökningen och det förfarande som ska följas vid genomförandet av en sådan undersökning, ska överenskommas av de berörda medlemsstaterna och byrån och ska inte påverka eventuella pågående brottsutredningar om samma incident. Undersökningen ska avslutas med en slutlig teknisk rapport som sammanställs av byrån, i synnerhet på grundval av information och synpunkter från de berörda medlemsstaterna och företagen, och fastställs tillsammans med de berörda medlemsstaterna. En sammanfattning av rapporten, med fokusering på rekommendationer för att förebygga framtida incidenter, kommer att distribueras till CSIRT-nätverket.

6. Byrån ska organisera årliga cybersäkerhetsövningar på unionsnivå och bistå medlemsstater och EU:s institutioner, byråer och organ med att organisera övningar på deras begäran. Årliga övningar på unionsnivå ska innehålla tekniska, operativa

och strategiska element och ska bidra till att förbereda den samarbetsinriktade responsen på unionsnivå för att hantera storskaliga gränsöverskridande cybersäkerhetsincidenter. Byrån ska också bidra till och hjälpa till att organisera, när det är lämpligt, sektorsvisa cybersäkerhetsövningar tillsammans med berörda ISAC och tillåta ISAC att delta även i cybersäkerhetsövningar på unionsnivå.

7. Byrån ska regelbundet utarbeta en teknisk lägesrapport om cybersäkerheten i EU om incidenter och hot på grundval av information från öppna källor, egna analyser och rapporter som den får från bland andra följande: medlemsstaternas CSIRT-enheter (på frivillig basis) eller de gemensamma kontaktpunkterna enligt it-säkerhetsdirektivet (i enlighet med artikel 14.5 i it-säkerhetsdirektivet); Europeiska it-brottscentrumet (EC3) vid Europol, CERT-EU.

8. Byrån ska bidra till att utveckla en samarbetsinriktad respons, på unions- och medlemsstatsnivå, för att hantera storskaliga gränsöverskridande incidenter eller kriser som rör cybersäkerhet, främst genom att

   (a) sammanställa rapporter från nationella källor i syfte att bidra till att skapa en gemensam situationsmedvetenhet,

   (b) säkerställa ett effektivt informationsflöde och tillhandahålla mekanismer för eskalering mellan CSIRT-nätverket och de tekniska och politiska beslutsfattarna på unionsnivå,

   (c) stödja den tekniska hanteringen av incidenter eller kriser, bland annat genom att underlätta utbytet av tekniska lösningar mellan medlemsstater,

   (d) stödja offentlig kommunikation om incidenter eller kriser,

   (e) testa samarbetsplanerna för hantering av sådana incidenter eller kriser.

Artikel 8

Uppgifter som rör marknaden, cybersäkerhetscertifiering samt standardisering

Byrån ska

(a) stödja och främja utvecklingen och genomförandet av unionens politik för cybersäkerhetscertifiering av IKT-produkter och IKT-tjänster, enligt avdelning III i denna förordning, genom att

   (1) utarbeta förslag till europeiska system för cybersäkerhetscertifiering för IKT-produkter och IKT-tjänster i enlighet med artikel 44 i denna förordning,

   (2) bistå kommissionen med att tillhandahålla sekretariatet för europeiska gruppen för cybersäkerhetscertifiering i enlighet med artikel 53 i denna förordning,

   (3) sammanställa och offentliggöra riktlinjer och utveckla god praxis när det gäller cybersäkerhetskraven för IKT-produkter och IKT-tjänster, i samarbete med nationella tillsynsmyndigheter för certifiering och branschen,

(b) underlätta upprättandet och tillämpningen av europeiska och internationella standarder för riskhantering och för säkerheten hos IKT-produkter och IKT-tjänster samt utarbeta, i samarbete med medlemsstater, råd och riktlinjer avseende de tekniska områden som har en koppling till säkerhetskraven för leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster, samt avseende redan

befintliga standarder, inbegripet medlemsstaternas nationella standarder, i enlighet med artikel 19.2 i direktiv (EU) 2016/1148,

(c) genomföra och sprida regelbundna analyser av de viktigaste trenderna på marknaden för cybersäkerhet på både efterfråge- och utbudssidan, i syfte att främja marknaden för cybersäkerhet i unionen.

Artikel 9

Uppgifter som rör kunskap, information och medvetandehöjande åtgärder

Byrån ska

(a) genomföra analyser av framväxande teknik och tillhandahålla ämnesspecifika bedömningar om tekniska innovationers förväntade samhälleliga, rättsliga, ekonomiska och regleringsrelaterade konsekvenser för cybersäkerhet,

(b) genomföra långsiktiga strategiska analyser av cybersäkerhetshot och cybersäkerhetsincidenter i syfte att identifiera framväxande trender och bidra till att förebygga problem som rör cybersäkerhet,

(c) i samarbete med experter från medlemsstaternas myndigheter tillhandahålla råd, vägledning och bästa praxis avseende säkerheten i nät- och informationssystem, i synnerhet avseende säkerheten hos internetinfrastrukturen och de infrastrukturer som understödjer de sektorer som förtecknas i bilaga II till direktiv (EU) 2016/1148,

(d) via en särskild portal samla, organisera och för allmänheten tillgängliggöra information om cybersäkerhet som tillhandahålls av unionens institutioner, byråer och organ,

(e) öka allmänhetens medvetenhet om cybersäkerhetsrisker och ge vägledning, som är inriktad på privatpersoner och organisationer, om god praxis för enskilda användare,

(f) samla in och analysera allmänt tillgänglig information om betydande incidenter och sammanställa rapporter i syfte att ge vägledning till företag och allmänheten i hela unionen,

(g) i samarbete med medlemsstaterna och unionens institutioner, organ, kontor och byråer organisera regelbundna informationskampanjer för att öka cybersäkerheten och dess synlighet i unionen.

Artikel 10

Uppgifter som rör forskning och innovation

När det gäller forskning och innovation ska byrån

(a) ge råd till unionen och medlemsstaterna om forskningsbehov och forskningsprioriteringar inom området cybersäkerhet, för att möjliggöra ett effektivt svar på befintliga och nya risker och hot, bland annat när det gäller ny och framväxande informations- och kommunikationsteknik, och för att säkerställa en effektiv användning av riskförebyggande teknik,

(b) delta, om kommissionen har delegerat relevanta befogenheter till den, i genomförandefasen av finansieringsprogram för forskning och innovation, eller som stödmottagare.

Artikel 11

Uppgifter som rör internationellt samarbete

Byrån ska bidra till unionens insatser för att samarbeta med tredjeländer och internationella organisationer för att främja internationellt samarbete i frågor som rör cybersäkerhet, genom att

(a) om lämpligt delta som observatör i anordnandet av internationella övningar samt analysera och rapportera till styrelsen om resultaten av sådana övningar,

(b) på begäran av kommissionen underlätta utbytet av bästa praxis mellan relevanta internationella organisationer,

(c) på begäran tillhandahålla kommissionen expertis.

KAPITEL II
BYRÅNS ORGANISATION

Artikel 12

Struktur

Byråns förvaltnings- och ledningsstruktur ska bestå av

(a) en styrelse, som ska utföra de uppgifter som anges i artikel 14,

(b) en direktion, som ska utföra de uppgifter som anges i artikel 18,

(c) en verkställande direktör med det ansvar som anges i artikel 19, och

(d) en ständig intressentgrupp, som ska utföra de uppgifter som anges i artikel 20.

AVSNITT 1
STYRELSE

Artikel 13

Styrelsens sammansättning

1. Styrelsen ska bestå av en företrädare för varje medlemsstat och två företrädare som utses av kommissionen. Samtliga företrädare ska ha rösträtt.

2. Varje ledamot av styrelsen ska ha en suppleant som företräder ledamoten i hans eller hennes frånvaro.

3. Styrelseledamöterna och deras suppleanter ska utses mot bakgrund av deras kunskaper inom området cybersäkerhet, med hänsyn till relevanta kunskaper i fråga om ledarskap, administration och budget. Kommissionen och medlemsstaterna ska bemöda sig om att begränsa omsättningen av sina företrädare i styrelsen för att säkerställa kontinuitet i styrelsens arbete. Kommissionen och medlemsstaterna ska sträva efter att uppnå en jämn könsfördelning i styrelsen.

4. Mandatperioden för styrelsens ledamöter och deras suppleanter ska vara fyra år. Mandatperioden får förnyas.

Artikel 14
Styrelsens uppgifter

1. Styrelsen ska göra följande:

   (a) Fastställa de allmänna riktlinjerna för byråns arbete och även se till att byrån agerar i enlighet med de regler och principer som fastställs i denna förordning. Den ska även se till att byråns arbete överensstämmer med det arbete som utförs av medlemsstaterna och på unionsnivå.

   (b) Anta byråns utkast till samlat programdokument som avses i artikel 21 innan det överlämnas till kommissionen för yttrande.

   (c) Med beaktande av kommissionens yttrande anta byråns samlade programdokument med två tredjedelars majoritet av ledamöterna och i enlighet med artikel 17.

   (d) Anta byråns årsbudget med två tredjedelars majoritet av ledamöterna och utföra andra uppgifter rörande byråns budget i enlighet med kapitel III.

   (e) Bedöma och anta den konsoliderade årliga rapporten om byråns verksamhet och senast den 1 juli följande år sända både rapporten och bedömningen till Europaparlamentet, rådet, kommissionen och revisionsrätten. Den årliga rapporten ska innehålla räkenskaperna och beskriva hur byrån har uppnått sina resultatindikatorer. Den årliga rapporten ska offentliggöras.

   (f) Anta de finansiella regler som ska tillämpas på byrån i enlighet med artikel 29.

   (g) Anta en bedrägeribekämpningsstrategi som står i proportion till bedrägeririskerna med beaktande av en kostnads–nyttoanalys av de åtgärder som ska genomföras.

   (h) Anta regler för att förebygga och hantera intressekonflikter bland ledamöterna.

   (i) Säkerställa lämplig uppföljning av slutsatserna och rekommendationerna från utredningar som genomförs av Europeiska byrån för bedrägeribekämpning (Olaf) och från olika interna eller externa revisionsrapporter och utvärderingar.

   (j) Anta sin arbetsordning.

   (k) I enlighet med punkt 2, med avseende på byråns personal, utöva de befogenheter som i tjänsteföreskrifterna för tjänstemän tilldelas tillsättningsmyndigheten och i anställningsvillkoren för Europeiska unionens övriga anställda tilldelas den myndighet som är behörig att sluta anställningsavtal (nedan kallade *befogenheter som tillsättningsmyndighet*).

   (l) Anta bestämmelser för att genomföra tjänsteföreskrifterna och anställningsvillkoren för övriga anställda i enlighet med förfarandet i artikel 110 i tjänsteföreskrifterna.

(m) Utse den verkställande direktören och i förekommande fall förlänga mandatperioden för eller avsätta honom eller henne i enlighet med artikel 33 i denna förordning.

(n) Utse en räkenskapsförare, som kan vara kommissionens räkenskapsförare, som ska vara helt oberoende i sin tjänsteutövning.

(o) Fatta alla beslut som rör inrättandet av byråns interna strukturer och, vid behov, ändringar av dessa, med beaktande av byråns verksamhetsbehov och en sund budgetförvaltning.

(p) Godkänna ingåendet av samarbetsavtal i enlighet med artiklarna 7 och 39.

2. Styrelsen ska, i enlighet med artikel 110 i tjänsteföreskrifterna, anta ett beslut grundat på artikel 2.1 i tjänsteföreskrifterna och artikel 6 i anställningsvillkoren för övriga anställda om att delegera relevanta befogenheter som tillsättningsmyndighet till den verkställande direktören och fastställa på vilka villkor denna delegering av befogenheter kan dras in. Den verkställande direktören får vidaredelegera dessa befogenheter.

3. Vid exceptionella omständigheter får styrelsen genom ett beslut tillfälligt dra in delegeringen till den verkställande direktören av befogenheterna som tillsättningsmyndighet samt de befogenheter som den verkställande direktören vidaredelegerat, och själv utöva dem eller delegera dem till en av sina ledamöter eller till någon annan anställd än den verkställande direktören.

Artikel 15
Styrelsens ordförande

Styrelsen ska med två tredjedelars majoritet av ledamöterna välja en ordförande och en vice ordförande bland sina ledamöter för en period på fyra år som får förnyas en gång. Om deras uppdrag som styrelseledamot emellertid upphör någon gång under deras mandatperiod, upphör deras mandatperiod automatiskt vid denna tidpunkt. Vice ordföranden ska inträda i ordförandens ställe om ordföranden inte kan fullgöra sina plikter.

Artikel 16
Styrelsens sammanträden

1. Styrelsens sammanträden ska sammankallas av dess ordförande.

2. Styrelsen ska hålla minst två ordinarie sammanträden per år. Den ska också hålla extra sammanträden på begäran av ordföranden, på begäran av kommissionen eller då minst en tredjedel av dess ledamöter så begär.

3. Den verkställande direktören ska delta i styrelsesammanträdena utan rösträtt.

4. Ledamöterna i den ständiga intressentgruppen får delta, efter inbjudan från ordföranden, i styrelsens sammanträden utan rösträtt.

5. Styrelseledamöterna och deras suppleanter får, med förbehåll för styrelsens arbetsordning, låta sig biträdas av rådgivare eller experter vid sammanträdena.

6. Byrån ska tillhandahålla sekretariatet för styrelsen.

Artikel 17

Omröstningsbestämmelser för styrelsen

1. Styrelsen ska fatta beslut med en majoritet av sina ledamöter.
2. Två tredjedelars majoritet av alla styrelseledamöter ska krävas för det samlade programdokumentet, den årliga budgeten samt utnämning av, förlängning av mandatet för eller avsättning av den verkställande direktören.
3. Varje ledamot ska ha en röst. I en ledamots frånvaro ska suppleanten ha rätt att utöva ledamotens rösträtt.
4. Ordföranden ska delta i omröstningen.
5. Den verkställande direktören ska inte delta i omröstningen.
6. Närmare bestämmelser om röstningsförfarandena, i synnerhet på vilka villkor en ledamot får agera på en annan ledamots vägnar, ska fastställas i styrelsens arbetsordning.

AVSNITT 2
DIREKTION

Artikel 18

Direktion

1. Styrelsen ska bistås av en direktion.
2. Direktionen ska
   (a) förbereda beslut som ska antas av styrelsen,
   (b) tillsammans med styrelsen säkerställa lämplig uppföljning av slutsatserna och rekommendationerna från utredningar som utförts av Europeiska byrån för bedrägeribekämpning (Olaf) och från olika interna eller externa revisionsrapporter och utvärderingar,
   (c) utan att det påverkar den verkställande direktörens ansvar enligt artikel 19 bistå och ge råd till den verkställande direktören vid genomförandet av styrelsens beslut i frågor som rör administration och budget enligt artikel 19.
3. Direktionen ska bestå av fem ledamöter utsedda bland styrelsens ledamöter, däribland styrelsens ordförande, som även kan vara direktionens ordförande, samt en av kommissionens företrädare. Den verkställande direktören ska delta i direktionens sammanträden, men ska inte ha rösträtt.
4. Mandatperioden för ledamöterna i direktionen ska vara fyra år. Mandatperioden får förnyas.
5. Direktionen ska sammanträda minst var tredje månad. Ordföranden för direktionen ska sammankalla extra sammanträden på begäran av direktionens ledamöter.
6. Direktionens arbetsordning ska fastställas av styrelsen.
7. Vid behov får direktionen, i brådskande fall, fatta vissa interimistiska beslut på styrelsens vägnar, särskilt i frågor som rör den administrativa ledningen, inklusive om indragning av delegeringen av befogenheterna som tillsättningsmyndighet och budgetfrågor.

AVSNITT 3
VERKSTÄLLANDE DIREKTÖR

Artikel 19

Den verkställande direktörens ansvarsområden

1. Byrån ska ledas av den verkställande direktören, som ska vara oberoende i sin tjänsteutövning. Den verkställande direktören ska vara ansvarig inför styrelsen.

2. Den verkställande direktören ska på begäran rapportera till Europaparlamentet om resultatet av sitt arbete. Rådet får uppmana den verkställande direktören att rapportera om resultatet av sitt arbete.

3. Den verkställande direktören ska ha ansvaret för följande:

   (a) Byråns dagliga förvaltning.

   (b) Genomföra de beslut som antas av styrelsen.

   (c) Utarbeta utkastet till det samlade programdokumentet och lämna det till styrelsen för godkännande innan det lämnas till kommissionen.

   (d) Genomföra det samlade programdokumentet och rapportera till styrelsen om detta.

   (e) Utarbeta den konsoliderade årliga rapporten om byråns verksamhet och framlägga den för styrelsen för bedömning och antagande.

   (f) Utarbeta en handlingsplan för uppföljning av slutsatserna från efterhandsutvärderingarna samt rapportera vartannat år till kommissionen om de framsteg som gjorts.

   (g) Utarbeta en handlingsplan för uppföljning av slutsatserna från interna eller externa revisionsrapporter, liksom utredningar utförda av Europeiska byrån för bedrägeribekämpning (Olaf), samt rapportera om läget två gånger om året till kommissionen och regelbundet till styrelsen.

   (h) Utarbetande av ett utkast till finansiella regler som ska tillämpas på byrån.

   (i) Upprätta byråns preliminära beräkning av inkomster och utgifter och genomföra dess budget.

   (j) Skydda unionens finansiella intressen genom förebyggande åtgärder mot bedrägeri, korruption och annan olaglig verksamhet, genom effektiva kontroller och, om oriktigheter upptäcks, genom återkrav av felaktigt utbetalda belopp samt vid behov genom effektiva, proportionella och avskräckande administrativa och ekonomiska sanktioner.

   (k) Utarbeta en strategi för bedrägeribekämpning för byrån och lägga fram den för styrelsen för godkännande.

(l) Utveckla och upprätthålla kontakter med näringslivet och konsumentorganisationer för att säkerställa en regelbunden dialog med berörda intressenter.

(m) Andra uppgifter som den verkställande direktören tilldelas genom denna förordning.

4. När så är nödvändigt och inom ramen för byråns mandat, och i överensstämmelse med byråns mål och uppgifter, får den verkställande direktören inrätta arbetsgrupper bestående av experter, inbegripet från medlemsstaternas behöriga myndigheter. Styrelsen ska underrättas i förväg. Förfarandena avseende i synnerhet sammansättningen av arbetsgrupperna, den verkställande direktörens tillsättning av arbetsgruppernas experter och arbetsgruppernas arbete ska anges i byråns interna verksamhetsregler.

5. Den verkställande direktören ska besluta om det är nödvändigt att utplacera personal i en eller flera medlemsstater för att byrån ska kunna utföra sina uppgifter på ett effektivt och ändamålsenligt sätt. Innan den verkställande direktören beslutar att inrätta ett lokalt kontor ska han eller hon inhämta förhandsgodkännande från kommissionen, styrelsen samt den eller de medlemsstater som berörs. I beslutet ska man ange omfattningen av den verksamhet som ska bedrivas vid det lokala kontoret på ett sätt som undviker onödiga kostnader och överlappning av byråns administrativa uppgifter. En överenskommelse med de berörda medlemsstaterna ska träffas när det är lämpligt eller nödvändigt.

AVSNITT 4
DEN STÄNDIGA INTRESSENTGRUPPEN

Artikel 20
Den ständiga intressentgruppen

1. Styrelsen ska på förslag av den verkställande direktören inrätta en ständig intressentgrupp bestående av erkända experter som företräder berörda intressenter, exempelvis IKT-branschen, leverantörer av allmänt tillgängliga elektroniska kommunikationsnät eller kommunikationstjänster, konsumentgrupper, experter på cybersäkerhet från den akademiska världen och företrädare för behöriga myndigheter som anmälts i enlighet med [direktivet om inrättandet av en europeisk kodex för elektronisk kommunikation] samt rättsvårdande myndigheter och tillsynsmyndigheter med ansvar för dataskydd.

2. Förfaranden för den ständiga intressentgruppen, i synnerhet avseende gruppens medlemsantal och sammansättning samt styrelsens utnämning av gruppens medlemmar, förslaget från den verkställande direktören och gruppens arbete, ska anges i byråns interna verksamhetsregler och ska offentliggöras.

3. Den verkställande direktören eller en person som han eller hon utser från fall till fall ska vara den ständiga intressentgruppens ordförande.

4. Mandatperioden för den ständiga intressentgruppens medlemmar ska vara två och ett halvt år. Styrelseledamöter får inte vara medlemmar i den ständiga intressentgruppen. Experter från kommissionen och medlemsstaterna får närvara vid den ständiga intressentgruppens möten och delta i dess arbete. Företrädare för andra organ som av den verkställande direktören anses som relevanta, men som inte är

medlemmar av den ständiga intressentgruppen, får bjudas in att närvara vid den ständiga intressentgruppens möten och delta i dess arbete.

5. Den ständiga intressentgruppen ska ge byrån råd med avseende på genomförandet av dess verksamhet. Den ska i synnerhet ge den verkställande direktören råd om utarbetandet av förslaget till byråns arbetsprogram och om kommunikationen med berörda intressenter om alla frågor kopplade till arbetsprogrammet.

AVSNITT 5
VERKSAMHET

Artikel 21
Samlat programdokument

1. Byrån ska genomföra sin verksamhet i enlighet med ett samlat programdokument som innehåller byråns fleråriga och årliga programplanering, vilket ska inbegripa all planerad verksamhet för byrån.

2. Den verkställande direktören ska varje år utarbeta ett utkast till samlat programdokument som innehåller flerårig och årlig programplanering med motsvarande planering av personalresurser och ekonomiska resurser i överensstämmelse med artikel 32 i kommissionens delegerade förordning (EU) nr 1271/2013[36] och som tar hänsyn till riktlinjer som kommissionen fastställt.

3. Senast den 30 november varje år ska styrelsen anta det samlade programdokument som avses i punkt 1 och översända det till Europaparlamentet, rådet och kommissionen senast den 31 januari följande år, liksom eventuella senare uppdaterade versioner av det dokumentet.

4. Det samlade programdokumentet ska anses vara slutgiltigt efter det att unionens allmänna budget slutligen har antagits och ska vid behov anpassas i enlighet därmed.

5. Det årliga arbetsprogrammet ska innehålla detaljerade mål och förväntade resultat, inklusive resultatindikatorer. Det ska också innehålla en beskrivning av de åtgärder som ska finansieras och uppgifter om vilka ekonomiska resurser och personalresurser som anslås till varje åtgärd, i enlighet med principerna om verksamhetsbaserad budgetering och förvaltning. Det årliga arbetsprogrammet ska överensstämma med det fleråriga arbetsprogram som avses i punkt 7. I programmet ska klart anges vilka uppgifter som lagts till, ändrats eller strukits jämfört med föregående räkenskapsår.

6. Styrelsen ska ändra det antagna årliga arbetsprogrammet om byrån får en ny uppgift. Varje betydande ändring av det årliga arbetsprogrammet ska antas enligt samma förfarande som det ursprungliga årliga arbetsprogrammet. Styrelsen får delegera befogenheten att göra icke-väsentliga ändringar i det årliga arbetsprogrammet till den verkställande direktören.

---

[36] Kommissionens delegerade förordning (EU) nr 1271/2013 av den 30 september 2013 med rambudgetförordning för de organ som avses i artikel 208 i Europaparlamentets och rådets förordning (EU, Euratom) nr 966/2012 (EUT L 328, 7.12.2013, s. 42).

7. I det fleråriga arbetsprogrammet ska den övergripande strategiska planeringen, inbegripet mål, förväntade resultat och resultatindikatorer, fastställas. Även resursplanering, inklusive flerårig budget och personal, ska fastställas.

8. Resursplaneringen ska uppdateras årligen. Den strategiska programplaneringen ska uppdateras när det är lämpligt, och i synnerhet när det är nödvändigt för att beakta resultatet av den utvärdering som avses i artikel 56.

Artikel 22
Intresseförklaring

1. Styrelsens ledamöter, den verkställande direktören och tjänstemän som är tillfälligt utstationerade av medlemsstaterna ska var och en göra en åtagandeförklaring och en förklaring som anger om det föreligger eller inte föreligger några direkta eller indirekta intressekonflikter som skulle kunna inverka negativt på deras oberoende. Förklaringarna ska vara tillförlitliga och fullständiga, och de ska göras årligen och skriftligt samt vid behov uppdateras.

2. Styrelsens ledamöter, den verkställande direktören och externa experter som deltar i tillfälliga arbetsgrupper ska var och en senast i inledningen av varje möte exakt och fullständigt redovisa eventuella intressen som kan påverka deras oberoende i förhållande till frågorna på dagordningen och avhålla sig från att delta i diskussioner och omröstningar om sådana frågor.

3. Byrån ska i sina interna verksamhetsregler fastställa hur de regler om intresseförklaringar som avses i punkterna 1 och 2 ska tillämpas praktiskt.

Artikel 23
Öppenhet

1. Byrån ska utföra sitt arbete med en hög grad av öppenhet och i enlighet med artikel 25.

2. Byrån ska säkerställa att allmänheten och eventuella berörda parter får lämplig, objektiv, tillförlitlig och lättillgänglig information, framför allt om resultaten av dess arbete. Den ska också offentliggöra de intresseförklaringar som avges i enlighet med artikel 22.

3. Styrelsen får, på förslag från den verkställande direktören, ge andra berörda parter tillstånd att observera delar av byråns verksamhet.

4. Byrån ska i sina interna verksamhetsregler fastställa hur de regler om öppenhet som avses i punkterna 1 och 2 ska tillämpas praktiskt.

Artikel 24
Konfidentialitet

1. Byrån ska inte för tredje part röja uppgifter som den behandlar eller mottar, om det i en motiverad ansökan har begärts att uppgifterna helt eller delvis ska behandlas konfidentiellt, dock utan att detta påverkar tillämpningen av artikel 25.

2. Ledamöterna i styrelsen, den verkställande direktören, den ständiga intressentgruppen, de externa experter som deltar i olika tillfälliga arbetsgrupper och byråns personal, inbegripet tjänstemän som är tillfälligt utstationerade av

medlemsstaterna, ska omfattas av tystnadsplikt enligt artikel 339 i fördraget om Europeiska unionens funktionssätt (EUF-fördraget), även efter det att deras uppdrag upphört.

3. Byrån ska i sina interna verksamhetsregler fastställa hur de regler om konfidentialitet som avses i punkterna 1 och 2 ska tillämpas praktiskt.

4. Styrelsen ska besluta om att tillåta byrån att hantera säkerhetsskyddsklassificerade uppgifter, om så krävs för att byrån ska kunna utföra sina uppgifter. I sådana fall ska styrelsen efter överenskommelse med kommissionens avdelningar anta interna verksamhetsregler som tillämpar säkerhetsprinciperna i kommissionens beslut (EU, Euratom) 2015/443[37] och 2015/444[38]. Dessa regler ska omfatta bestämmelser om utbyte, behandling och lagring av säkerhetsskyddsklassificerade uppgifter.

Artikel 25
Tillgång till handlingar

1. Förordning (EG) nr 1049/2001 ska tillämpas på de handlingar som finns hos byrån.

2. Styrelsen ska vidta åtgärder för att genomföra förordning (EG) nr 1049/2001 inom sex månader efter det att byrån inrättats.

3. Beslut som fattas av byrån i enlighet med artikel 8 i förordning (EG) nr 1049/2001 får bli föremål för ett klagomål till ombudsmannen enligt artikel 228 i EUF-fördraget eller väckande av talan vid Europeiska unionens domstol i enlighet med artikel 263 i EUF-fördraget.

KAPITEL III
UPPRÄTTANDET AV BUDGETEN OCH BUDGETENS STRUKTUR

Artikel 26
Upprättandet av budgeten

1. Varje år ska den verkställande direktören upprätta en preliminär beräkning av byråns inkomster och utgifter för det därpå följande räkenskapsåret, och ska översända det till styrelsen tillsammans med ett utkast till tjänsteförteckning. Inkomster och utgifter ska vara i balans.

2. Varje år ska styrelsen, på grundval av den preliminära beräkning av inkomster och utgifter som avses i punkt 1, lägga fram en beräkning av byråns inkomster och utgifter för det därpå följande räkenskapsåret.

3. Styrelsen ska senast den 31 januari varje år överlämna den beräkning som avses i punkt 2, som ska vara en del av utkastet till det samlade programdokumentet, till

---

37 Kommissionens beslut (EU, Euratom) 2015/443 av den 13 mars 2015 om säkerhet inom kommissionen (EUT L 72, 17.3.2015, s. 41).

38 Kommissionens beslut (EU, Euratom) 2015/444 av den 13 mars 2015 om säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter (EUT L 72, 17.3.2015, p. 53).

kommissionen och de tredjeländer med vilka unionen har slutit avtal i enlighet med artikel 39.

4. På grundval av den beräkningen ska kommissionen ta upp de medel som den anser vara nödvändiga för tjänsteförteckningen och storleken på det anslag som ska belasta den allmänna budgeten i förslaget till unionens budget, som den ska förelägga Europaparlamentet och rådet i enlighet med artiklarna 313 och 314 i EUF-fördraget.

5. Europaparlamentet och rådet ska bevilja anslagen för bidraget till byrån.

6. Europaparlamentet och rådet ska anta byråns tjänsteförteckning.

7. Styrelsen ska anta byråns budget tillsammans med det samlade programdokumentet. Den blir slutlig när unionens allmänna budget slutgiltigt har antagits. Styrelsen ska vid behov anpassa byråns budget och det samlade programdokumentet till unionens allmänna budget.

Artikel 27
Budgetens struktur

1. Utan att det påverkar andra medel ska byråns inkomster bestå av

   (a) ett bidrag från unionens budget,

   (b) inkomster avsatta för särskilda ändamål i enlighet med byråns finansiella regler som avses i artikel 29,

   (c) unionsfinansiering via delegeringsavtal eller bidrag som beviljas från fall till fall, i enlighet med de finansiella regler som avses i artikel 29 och gällande bestämmelser för de instrument som inrättats till stöd för unionens politik,

   (d) bidrag från tredjeländer som deltar i byråns arbete i enlighet med artikel 39,

   (e) eventuella frivilliga bidrag från medlemsstater i pengar eller in natura. Medlemsstater som ger frivilliga bidrag kan inte göra anspråk på några särskilda rättigheter eller tjänster som en följd av bidragen.

2. Byråns utgifter ska täcka kostnaderna för personal, administrativt och tekniskt stöd, infrastruktur och drift samt utgifter till följd av avtal som ingås med tredje part.

Artikel 28
Budgetgenomförandet

1. Den verkställande direktören ska ansvara för att byråns budget genomförs.

2. Kommissionens internrevisor ska ha samma befogenheter gentemot byrån som gentemot kommissionens avdelningar.

3. Senast den 1 mars efter varje räkenskapsår (den 1 mars år n + 1) ska byråns räkenskapsförare översända de preliminära räkenskaperna till kommissionens räkenskapsförare och till revisionsrätten.

4. Efter mottagandet av revisionsrättens iakttagelser om byråns preliminära räkenskaper ska byråns räkenskapsförare upprätta byråns slutliga räkenskaper på eget ansvar.

5. Den verkställande direktören ska överlämna de slutliga räkenskaperna till styrelsen för yttrande.

6. Den verkställande direktören ska senast den 31 mars år n + 1 översända rapporten om budgetförvaltningen och den ekonomiska förvaltningen till Europaparlamentet, rådet, kommissionen och revisionsrätten.

7. Senast den 1 juli år n + 1 ska räkenskapsföraren överlämna de slutliga räkenskaperna, tillsammans med styrelsens yttrande, till Europaparlamentet, rådet, kommissionens räkenskapsförare och revisionsrätten.

8. Räkenskapsföraren ska, samma dag som hans eller hennes slutliga räkenskaper överlämnas, också till revisionsrätten översända en bekräftelse som omfattar dessa slutliga räkenskaper, med en kopia till kommissionens räkenskapsförare.

9. Den verkställande direktören ska offentliggöra de slutliga räkenskaperna senast den 15 november följande år.

10. Senast den 30 september år n + 1 ska den verkställande direktören till revisionsrätten översända ett svar på dess synpunkter och även sända en kopia av detta svar till styrelsen och till kommissionen.

11. Den verkställande direktören ska på Europaparlamentets begäran, i enlighet med artikel 165.3 i budgetförordningen, för Europaparlamentet lägga fram alla uppgifter som är nödvändiga för att förfarandet för beviljande av ansvarsfrihet för det berörda räkenskapsåret ska kunna tillämpas på ett smidigt sätt.

12. På rekommendation av rådet ska Europaparlamentet före den 15 maj år n + 2 bevilja den verkställande direktören ansvarsfrihet beträffande budgetens genomförande år n.

Artikel 29
Finansiella regler

De finansiella regler som ska tillämpas på byrån ska antas av styrelsen efter samråd med kommissionen. De får inte avvika från förordning (EU) nr 1271/2013 såvida inte en sådan avvikelse är specifikt nödvändig för byråns verksamhet och kommissionen har lämnat sitt samtycke i förväg.

Artikel 30
Bedrägeribekämpning

1. För att underlätta bekämpning av bedrägeri, korruption och andra olagliga handlingar enligt Europaparlamentets och rådets förordning (EU, Euratom) nr 883/2013[39] ska byrån, inom sex månader från den dag då den inleder sin verksamhet, ansluta sig till det interinstitutionella avtalet av den 25 maj 1999 om interna utredningar som utförs av Europeiska byrån för bedrägeribekämpning (Olaf) och anta lämpliga bestämmelser som ska vara tillämpliga på alla anställda vid byrån genom att använda den mall som anges i bilagan till det avtalet.

[39] Europaparlamentets och rådets förordning (EU, Euratom) nr 883/2013 av den 11 september 2013 om utredningar som utförs av Europeiska byrån för bedrägeribekämpning (Olaf) och om upphävande av Europaparlamentets och rådets förordning (EG) nr 1073/1999 och rådets förordning (Euratom) nr 1074/1999 (EUT L 248, 18.9.2013, s. 1).

2. Revisionsrätten ska ha befogenhet att utföra revision, på grundval av handlingar och kontroller på plats, hos alla stödmottagare, uppdragstagare och underleverantörer som erhållit unionsfinansiering från byrån.

3. Olaf får göra utredningar, inbegripet kontroller på plats och inspektioner – i enlighet med bestämmelserna och förfarandena i Europaparlamentets och rådets förordning (EU, Euratom) nr 883/2013 och rådets förordning (Euratom, EG) nr 2185/96[40] av den 11 november 1996 om de kontroller och inspektioner på platsen som kommissionen utför för att skydda unionens finansiella intressen mot bedrägerier och andra oegentligheter – i syfte att fastställa om det har förekommit bedrägeri, korruption eller annan olaglig verksamhet som påverkar unionens ekonomiska intressen i samband med bidrag eller kontrakt som finansierats av byrån.

4. Utan att det påverkar tillämpningen av punkterna 1, 2 och 3 ska samarbetsavtal med tredjeländer och internationella organisationer, kontrakt, bidragsavtal och bidragsbeslut från byrån innehålla bestämmelser som uttryckligen tillerkänner revisionsrätten och Olaf rätten att utföra sådan revision och genomföra sådana utredningar inom ramen för sina respektive befogenheter.

KAPITEL IV
BYRÅNS PERSONAL

Artikel 31
Allmänna bestämmelser

Tjänsteföreskrifterna och anställningsvillkoren för övriga anställda samt de bestämmelser som har antagits gemensamt av unionens institutioner för tillämpningen av dessa tjänsteföreskrifter ska gälla för byråns personal.

Artikel 32
Immunitet och privilegier

Byrån och dess personal ska omfattas av protokoll nr 7 om Europeiska unionens immunitet och privilegier, fogat till fördraget om Europeiska unionen och EUF-fördraget.

Artikel 33
Verkställande direktör

1. Den verkställande direktören ska vara tillfälligt anställd vid byrån i enlighet med artikel 2 a i anställningsvillkoren för övriga anställda.

2. Den verkställande direktören ska utses av styrelsen från en förteckning över kandidater som föreslagits av kommissionen efter ett öppet och transparent urvalsförfarande.

3. I det avtal som sluts med den verkställande direktören ska byrån företrädas av styrelsens ordförande.

---

40 Rådets förordning (Euratom, EG) nr 2185/96 av den 11 november 1996 om de kontroller och inspektioner på platsen som kommissionen utför för att skydda Europeiska gemenskapernas finansiella intressen mot bedrägerier och andra oegentligheter (EGT L 292, 15.11.1996, s. 2).

4. Den kandidat som styrelsen väljer ska före utnämningen ombes att göra ett uttalande inför behörigt utskott i Europaparlamentet och besvara frågor från ledamöterna.

5. Den verkställande direktörens mandatperiod ska vara fem år. I slutet av denna period ska kommissionen genomföra en utvärdering som beaktar den verkställande direktörens arbetsinsats och byråns framtida uppgifter och utmaningar.

6. Styrelsen ska fatta beslut om att utse, förlänga mandatperioden för eller avsätta den verkställande direktören med två tredjedelars majoritet av de röstberättigade ledamöterna.

7. Styrelsen får på förslag av kommissionen, med beaktande av den utvärdering som avses i punkt 5, förlänga den verkställande direktörens mandatperiod en gång med högst fem år.

8. Styrelsen ska underrätta Europaparlamentet om sin avsikt att förlänga den verkställande direktörens mandatperiod. Inom tre månader före en sådan förlängning ska den verkställande direktören på anmodan göra ett uttalande inför behörigt utskott i Europaparlamentet och besvara frågor från ledamöterna.

9. En verkställande direktör vars mandat förlängts får inte delta i något ytterligare urvalsförfarande för samma befattning.

10. Den verkställande direktören får avsättas endast efter ett styrelsebeslut på förslag av kommissionen.

Artikel 34
Utstationerade nationella experter och annan personal

1. Byrån får använda sig av utstationerade nationella experter och annan personal som inte är anställd av byrån. Tjänsteföreskrifterna och anställningsvillkoren för övriga anställda ska inte gälla för sådan personal.

2. Styrelsen ska anta ett beslut om regler för utstationering av nationella experter till byrån.

KAPITEL V
ALLMÄNNA BESTÄMMELSER

Artikel 35
Byråns *rättsliga ställning*

1. Byrån ska vara ett unionsorgan och ska vara en juridisk person.

2. Byrån ska i varje medlemsstat ha den mest vittgående rättskapacitet som tillerkänns juridiska personer enligt den nationella lagstiftningen. Den får särskilt förvärva eller avyttra lös och fast egendom och får föra talan inför domstolar och andra myndigheter, eller båda.

3. Byrån ska företrädas av den verkställande direktören.

Artikel 36

Byråns ansvar

1. Byråns avtalsrättsliga ansvar ska regleras av den lagstiftning som är tillämplig på avtalet i fråga.

2. Europeiska unionens domstol ska vara behörig att träffa avgöranden med stöd av en skiljedomsklausul i ett avtal som byrån ingått.

3. Vad beträffar utomobligatoriskt ansvar ska byrån enligt de allmänna principer som är gemensamma för medlemsstaternas rättsordningar ersätta skada som vållats av byrån själv eller dess personal under tjänsteutövning.

4. Europeiska unionens domstol ska vara behörig att avgöra tvister som rör ersättning för sådana skador.

5. De anställdas personliga ansvar gentemot byrån ska regleras av de relevanta bestämmelser som är tillämpliga på byråns personal.

Artikel 37

Språkordning

1. Rådets förordning nr 1 ska gälla för byrån[41]. Medlemsstaterna och övriga organ som utsetts av dem kan vända sig till byrån och har rätt att få svar på det officiella språk vid unionens institutioner som de själva väljer.

2. De översättningar som krävs för byråns verksamhet ska tillhandahållas av Översättningscentrum för Europeiska unionens organ.

Artikel 38

Skydd av personuppgifter

1. Byrån ska behandla personuppgifter i enlighet med Europaparlamentets och rådets förordning (EG) nr 45/2001[42].

2. Styrelsen ska anta de genomförandebestämmelser som avses i artikel 24.8 i förordning (EG) nr 45/2001. Styrelsen får anta ytterligare åtgärder som behövs för byråns tillämpning av förordning (EG) nr 45/2001.

Artikel 39

Samarbete med tredjeländer och internationella organisationer

1. I den mån det är nödvändigt för att uppnå målen i denna förordning får byrån samarbeta med de behöriga myndigheterna i tredjeländer eller med internationella organisationer, eller båda. För detta ändamål får byrån, efter förhandsgodkännande från kommissionen, upprätta samarbetsavtal med myndigheterna i tredjeländer och med internationella organisationer. Dessa avtal får inte medföra några juridiska förpliktelser för unionen och dess medlemsstater.

---

41 Rådets förordning nr 1 om vilka språk som skall användas i Europeiska atomenergigemenskapen (EGT 17, 6.10.1958, s. 401).

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

2. Byrån ska vara öppen för deltagande av tredjeländer som har ingått avtal med unionen i detta syfte. I enlighet med de relevanta bestämmelserna i dessa avtal ska det utarbetas överenskommelser som särskilt anger karaktären hos, omfattningen av och utformningen av dessa länders deltagande i byråns arbete, inklusive bestämmelser om deltagande i byråns initiativ, finansiella bidrag och personal. När det gäller personalfrågor ska dessa överenskommelser under alla förhållanden vara förenliga med tjänsteföreskrifterna.

3. Styrelsen ska anta en strategi för förbindelserna med tredjeländer eller internationella organisationer i de frågor som byrån har behörighet för. Kommissionen ska säkerställa att byrån arbetar inom ramen för sitt mandat och den befintliga institutionella ramen genom att ingå ett lämpligt samarbetsavtal med byråns verkställande direktör.

Artikel 40

***Säkerhetsbestämmelser* om skydd av säkerhetsskyddsklassificerade uppgifter och känsliga icke-säkerhetsskyddsklassificerade uppgifter**

I samråd med kommissionen ska byrån anta sina säkerhetsbestämmelser som tillämpar säkerhetsprinciperna i kommissionens säkerhetsbestämmelser för skydd av säkerhetsskyddsklassificerade EU-uppgifter och känsliga icke-säkerhetsskyddsklassificerade uppgifter, i enlighet med kommissionens beslut (EU, Euratom) 2015/443 och 2015/444. Det ska bland annat omfatta bestämmelser om utbyte, behandling och lagring av sådana uppgifter.

Artikel 41

Överenskommelse om säte och villkor för verksamheten

1. De nödvändiga bestämmelserna om de lokaler som ska tillhandahållas för byrån i värdmedlemsstaten och de anläggningar som ska ställas till byråns förfogande av den medlemsstaten, tillsammans med de särskilda regler i värdmedlemsstaten som ska tillämpas på den verkställande direktören, styrelseledamöterna, byråns personal och deras familjemedlemmar, ska fastställas i en överenskommelse om säte mellan byrån och den medlemsstat där den har sitt säte, vilken ingås efter att ha godkänts av styrelsen och senast [två år efter ikraftträdandet av denna förordning].

2. Byråns värdmedlemsstat ska tillhandahålla bästa möjliga förutsättningar för att säkerställa en väl fungerande byrå, bland annat när det gäller platsens tillgänglighet, adekvata utbildningsmöjligheter för personalens barn, lämplig tillgång till arbetsmarknad, social trygghet och sjukvård för både barn och makar.

Artikel 42

Administrativ kontroll

Byråns verksamhet ska övervakas av ombudsmannen i enlighet med artikel 228 i EUF-fördraget.

AVDELNING II
I
RAM FÖR CYBERSÄKERHETSCERTIFIERING

Artikel 43

Europeiska system för cybersäkerhetscertifiering

Ett europeiskt system för cybersäkerhetscertifiering ska intyga att de IKT-produkter och IKT-tjänster som har certifierats i enlighet med ett sådant system uppfyller de angivna kraven när det gäller deras förmåga att tåla, vid en viss assuransnivå, åtgärder som syftar till att äventyra tillgängligheten, autenticiteten, integriteten eller konfidentialiteten hos lagrade, överförda eller behandlade data eller de funktioner eller tjänster som tillhandahålls av eller är tillgängliga via dessa produkter, processer, tjänster och system.

Artikel 44

Utarbetande och antagande av ett europeiskt system för cybersäkerhetscertifiering

1. Efter en begäran från kommissionen, ska Enisa utarbeta ett förslag till ett europeiskt system för cybersäkerhetscertifiering som uppfyller kraven i artiklarna 45, 46 och 47 i denna förordning. Medlemsstaterna eller den europeiska gruppen för cybersäkerhetscertifiering (nedan kallad *gruppen*) som inrättats enligt artikel 53 får lämna förslag till kommissionen om utarbetande av ett förslag till ett europeiskt system för cybersäkerhetscertifiering.
2. Vid utarbetandet av förslag till system som avses i punkt 1 i denna artikel ska Enisa samråda med alla berörda intressenter och bedriva ett nära samarbete med gruppen. Gruppen ska ge Enisa det bistånd och de expertråd som Enisa behöver vid utarbetandet av förslaget till system, bland annat genom att avge yttranden om det behövs.
3. Enisa ska till kommissionen översända det förslag till europeiskt system för cybersäkerhetscertifiering som utarbetats i enlighet med punkt 2 i denna artikel.
4. Med utgångspunkt i det förslag till system som Enisa lagt fram, får kommissionen anta genomförandeakter i enlighet med artikel 55.1 för europeiska system för certifiering av IKT-produkter och IKT-tjänster som uppfyller kraven i artiklarna 45, 46 och 47 i denna förordning.
5. Enisa ska upprätthålla en särskild webbplats med information om och offentliggörande av europeiska system för cybersäkerhetscertifiering.

Artikel 45

Säkerhetsmålen för europeiska system för cybersäkerhetscertifiering

Ett europeiskt system för cybersäkerhetscertifiering ska vara utformat så att det, i tillämpliga fall, tar hänsyn till följande säkerhetsmål:

(a) Att skydda data som lagras, överförs eller på andra sätt behandlas, mot oavsiktlig eller otillåten lagring, behandling eller åtkomst eller oavsiktligt eller otillåtet offentliggörande.

(b) Att skydda data som lagras, överförs eller på andra sätt behandlas, mot oavsiktlig eller otillåten förstöring, oavsiktlig förlust eller ändringar.

(c) Att säkerställa att behöriga personer, program eller maskiner kan få åtkomst endast till de data, tjänster eller funktioner som omfattas av deras åtkomsträttigheter.

(d) Att registrera vilka data, funktioner och tjänster som har lämnats ut, vid vilken tidpunkt och av vem.

(e) Att säkerställa att det är möjligt att kontrollera vilka data, tjänster eller funktioner som någon haft åtkomst till eller som använts, vid vilken tidpunkt och vem som haft åtkomst till eller använt dessa.

(f) Att återställa tillgängligheten och tillgången avseende data, tjänster och funktioner i rätt tid vid en fysisk eller teknisk incident.

(g) Att säkerställa att IKT-produkter och IKT-tjänster tillhandahålls med uppdaterad programvara som inte innehåller kända brister, och med mekanismer för säkra uppdateringar av programvaran.

Artikel 46

Assuransnivåer för europeiska system för cybersäkerhetscertifiering

1. Ett europeiskt system för cybersäkerhetscertifiering får innehålla en eller flera av följande assuransnivåer: grundläggande, betydande och/eller hög för IKT-produkter och IKT-tjänster som har utfärdats inom det systemet.

2. Assuransnivåerna grundläggande, betydande och hög ska uppfylla följande kriterier:

(a) Assuransnivån *grundläggande* ska avse ett certifikat som utfärdats inom ramen för ett europeiskt system för cybersäkerhetscertifiering, som ger en begränsad grad av tillförlitlighet i fråga om påstådda eller styrkta cybersäkerhetsegenskaper hos en IKT-produkt eller IKT-tjänst, och som betecknas med hänvisning till tekniska specifikationer, standarder och förfaranden med koppling till detta, inbegripet tekniska kontroller, som ska minska risken för cybersäkerhetsincidenter.

(b) Assuransnivån *betydande* ska avse ett certifikat som utfärdats inom ramen för ett europeiskt system för cybersäkerhetscertifiering, som ger en betydande grad av tillförlitlighet i fråga om påstådda eller styrkta cybersäkerhetsegenskaper hos en IKT-produkt eller IKT-tjänst, och som betecknas med hänvisning till tekniska specifikationer, standarder och förfaranden med koppling till detta, inbegripet tekniska kontroller, som ska minska risken för cybersäkerhetsincidenter.

(c) Assuransnivån *hög* ska avse ett certifikat som utfärdats inom ramen för ett europeiskt system för cybersäkerhetscertifiering, som ger en högre grad av tillförlitlighet i fråga om påstådda eller styrkta cybersäkerhetsegenskaper hos en IKT-produkt eller IKT-tjänst än certifikat med assuransnivån betydande, och som betecknas med hänvisning till tekniska specifikationer, standarder och förfaranden med koppling till detta, inbegripet tekniska kontroller, som ska förhindra cybersäkerhetsincidenter.

Artikel 47

Komponenter i europeiska system för cybersäkerhetscertifiering

1. Ett europeiskt system för cybersäkerhetscertifiering ska innehålla följande komponenter:

   (a) Föremålet och tillämpningsområdet för certifieringen, inbegripet typen eller kategorierna av de IKT-produkter och IKT-tjänster som omfattas av certifieringen.

   (b) Detaljerad specificering av de cybersäkerhetskrav som specifika IKT-produkter och IKT-tjänster bedöms mot, t.ex. genom hänvisning till unionslagstiftning, internationella standarder eller tekniska specifikationer.

   (c) I tillämpliga fall, en eller flera assuransnivåer.

   (d) Särskilda bedömningskriterier och -metoder som använts, inklusive utvärderingstyper, i syfte att visa att de särskilda mål som anges i artikel 45 uppnås.

   (e) Uppgifter som en sökande ska lämna till organ för bedömning av överensstämmelse och som är nödvändiga för certifieringen.

   (f) Om systemet fastställer användning av märken eller etiketter, villkoren för deras användning.

   (g) Om övervakning ingår i systemet, reglerna för övervakning och efterlevnad av certifieringskraven, inklusive mekanismer för att visa fortsatt överensstämmelse med de angivna cybersäkerhetskraven.

   (h) Villkor för beviljande, bibehållande, fortsättande, utvidgning och inskränkning av tillämpningsområdet för certifiering.

   (i) Bestämmelser om följderna om certifierade IKT-produkter och IKT-tjänster inte överensstämmer med certifieringskraven.

   (j) Bestämmelser om hur tidigare oupptäckta sårbarheter i fråga om cybersäkerhet hos IKT-produkter och IKT-tjänster ska rapporteras och utredas.

   (k) Bestämmelser om hur organ för bedömning av överensstämmelse ska bevara sina uppgifter.

   (l) Identifiering av nationella system för cybersäkerhetscertifiering som omfattar samma typ eller kategorier av IKT-produkter och IKT-tjänster.

   (m) Innehållet i det utfärdade certifikatet.

2. De angivna kraven för systemet ska inte strida mot något tillämpligt lagstadgat krav, i synnerhet inte krav som härrör från harmoniserad unionslagstiftning.

3. Om det föreskrivs i en viss unionsakt får certifiering enligt ett europeiskt system för cybersäkerhetscertifiering användas för att påvisa presumtion om överensstämmelse med kraven i den unionsakten.

4. I avsaknad av harmoniserad unionslagstiftning får en medlemsstats lagstiftning också föreskriva att ett europeiskt system för cybersäkerhetscertifiering får användas för fastställande av presumtionen om överensstämmelse med de rättsliga kraven.

Artikel 48

Cybersäkerhetscertifiering

1. IKT-produkter och IKT-tjänster som har certifierats enligt ett europeiskt system för cybersäkerhetscertifiering som antagits enligt artikel 44 ska förutsättas överensstämma med kraven i ett sådant system.

2. Certifieringen ska vara frivillig, om inte annat uttryckligen anges i unionslagstiftningen.

3. Ett europeiskt cybersäkerhetscertifikat i enlighet med denna artikel ska utfärdas av de organ för bedömning av överensstämmelse som avses i artikel 51 på grundval av de kriterier som ingår i det europeiska systemet för cybersäkerhetscertifiering, som antagits i enlighet med artikel 44.

4. Genom undantag från punkt 3, och i vederbörligen motiverade fall, får ett visst europeiskt system för cybersäkerhet föreskriva att ett europeiskt cybersäkerhetscertifikat som är ett resultat av det systemet kan utfärdas endast av ett offentligt organ. Ett sådant offentligt organ ska vara ett av följande:

   (a) En nationell tillsynsmyndighet för certifiering som avses i artikel 50.1.

   (b) Ett organ som är ackrediterat som organ för bedömning av överensstämmelse i enlighet med artikel 51.1.

   (c) Ett organ som inrättats med stöd av lagar, rättsinstrument eller andra administrativa förfaranden i en berörd medlemsstat och som uppfyller kraven för organ som certifierar produkter, processer och tjänster enligt ISO/IEC 17065:2012.

5. Den fysiska eller juridiska person som lämnar in sina IKT- produkter eller IKT-tjänster till certifieringsmekanismen ska till det organ för bedömning av överensstämmelse som avses i artikel 51 lämna all information som krävs för att genomföra certifieringsförfarandet.

6. Certifikat ska utfärdas för en period på högst tre år och får förnyas på samma villkor under förutsättning att de relevanta kraven fortsätter att uppfyllas.

7. Ett europeiskt cybersäkerhetscertifikat som utfärdats i enlighet med denna artikel ska erkännas i alla medlemsstater.

Artikel 49

Nationella system och certifikat för cybersäkerhetscertifiering

1. Utan att det påverkar tillämpningen av punkt 3 ska de nationella systemen för cybersäkerhetscertifiering och därtill hörande förfaranden, för de IKT-produkter och IKT-tjänster som omfattas av ett europeiskt system för cybersäkerhetscertifiering, upphöra att ha verkan från och med den dag som anges i den genomförandeakt som antagits i enlighet med artikel 44.4. Befintliga nationella system för cybersäkerhetscertifiering och därtill hörande förfaranden för IKT-produkter och IKT-tjänster som inte omfattas av ett europeiskt system för cybersäkerhetscertifiering ska fortsätta att existera.

2. Vidare ska medlemsstaterna inte införa nya nationella system för cybersäkerhetscertifiering av de IKT-produkter och IKT-tjänster som omfattas av ett befintligt europeiskt system för cybersäkerhetscertifiering.

3. Befintliga certifikat som utfärdats enligt nationella system för cybersäkerhetscertifiering ska förbli giltiga tills de löper ut.

Artikel 50

Nationella tillsynsmyndigheter för certifiering

1. Varje medlemsstat ska utse en nationell tillsynsmyndighet för certifiering.
2. Varje medlemsstat ska underrätta kommissionen om vilken myndighet som utsetts.
3. Varje nationell tillsynsmyndighet för certifiering ska, vad gäller dess organisation, beslut om finansiering, rättsliga struktur och beslutsfattande vara oberoende av de enheter som den utövar tillsyn över.
4. Medlemsstaterna ska säkerställa att de nationella tillsynsmyndigheterna för certifiering har tillräckliga resurser för att kunna utöva sina befogenheter och kunna utföra de uppgifter de tilldelats på ett effektivt och ändamålsenligt sätt.
5. För en effektiv tillämpning av förordningen är det lämpligt att dessa myndigheter deltar i den europeiska grupp för cybersäkerhetscertifiering som inrättats enligt artikel 53 på ett effektivt, ändamålsenligt och säkert sätt.
6. Nationella tillsynsmyndigheter för certifiering ska
   (a) övervaka och kontrollera tillämpningen av de bestämmelser som föreskrivs i denna avdelning på nationell nivå och övervaka att de certifikat som har utfärdats av organ för bedömning av överensstämmelse etablerade på deras respektive territorier uppfyller kraven i denna avdelning och i motsvarande europeiska system för cybersäkerhetscertifiering,
   (b) övervaka och kontrollera den verksamhet som organen för bedömning av överensstämmelse utför i enlighet med denna förordning, bland annat när det gäller anmälan av organ för bedömning av överensstämmelse och de relaterade uppgifter som anges i artikel 52 i denna förordning,
   (c) behandla klagomål som lämnas in av fysiska eller juridiska personer avseende certifikat som utfärdats av organ för bedömning av överensstämmelse som är etablerade på deras territorier, i lämplig utsträckning undersöka det ärende som klagomålet gäller och inom rimlig tid underrätta anmälaren om utvecklingen och resultatet av utredningen,
   (d) samarbeta med andra nationella tillsynsmyndigheter för certifiering eller andra myndigheter, bland annat genom att utbyta information om IKT-produkter och IKT-tjänster som eventuellt avviker från kraven i denna förordning eller särskilda europeiska system för cybersäkerhetscertifiering,
   (e) övervaka relevant utveckling på området cybersäkerhetscertifiering.
7. Varje nationell tillsynsmyndighet för certifiering ska minst ha följande befogenheter:
   (a) Kunna begära att organ för bedömning av överensstämmelse och innehavare av ett europeiskt cybersäkerhetscertifikat ska lägga fram alla uppgifter som myndigheten behöver för att kunna fullgöra sin uppgift.
   (b) Få genomföra undersökningar, i form av kontroller, av organ för bedömning av överensstämmelse och innehavare av ett europeiskt cybersäkerhetscertifikat, för att kunna verifiera överensstämmelse med bestämmelserna i avdelning III.

(c) Få vidta lämpliga åtgärder, i enlighet med nationell lagstiftning, för att säkerställa att organen för bedömning av överensstämmelse eller innehavare av ett europeiskt cybersäkerhetscertifikat uppfyller kraven i denna förordning eller med ett europeiskt system för cybersäkerhetscertifiering.

(d) Få tillgång till alla lokaler hos organ för bedömning av överensstämmelse och innehavare av ett europeiskt cybersäkerhetscertifikat i syfte att genomföra utredningar i enlighet med unionens eller medlemsstaternas processrätt.

(e) Kunna, i enlighet med nationell lagstiftning, återkalla certifikat som inte uppfyller kraven i denna förordning eller ett europeiskt system för cybersäkerhetscertifiering.

(f) Få utdöma sanktioner enligt artikel 54, i enlighet med nationell lagstiftning, och kräva att överträdelser av skyldigheterna i denna förordning omedelbart upphör.

8. Nationella tillsynsmyndigheter för certifiering ska samarbeta med varandra och kommissionen och, i synnerhet, utbyta information, erfarenheter och god praxis när det gäller cybersäkerhetscertifiering och tekniska frågor som rör cybersäkerhet hos IKT-produkter och IKT-tjänster.

Artikel 51

Organ för bedömning av överensstämmelse

1. Organen för bedömning av överensstämmelse ska ackrediteras av det nationella ackrediteringsorgan som utsetts i enlighet med förordning (EG) nr 765/2008 endast under förutsättning att de uppfyller kraven i bilagan till denna förordning.

2. Ackrediteringen ska utfärdas för en period på högst fem år och får förnyas på samma villkor under förutsättning att organet för bedömning av överensstämmelse uppfyller kraven i denna artikel. Ackrediteringsorgan ska återkalla ackrediteringen av ett organ för bedömning av överensstämmelse i enlighet med punkt 1 i denna artikel om villkoren för ackrediteringen inte, eller inte längre, uppfylls eller om åtgärder som vidtagits av organet för bedömning av överensstämmelse strider mot denna förordning.

Artikel 52

Anmälan

1. För varje europeiskt system för cybersäkerhetscertifiering som antagits enligt artikel 44 ska nationella tillsynsmyndigheter för certifiering till kommissionen anmäla de ackrediterade organ för bedömning av överensstämmelse som är ackrediterade att utfärda certifikat på angivna assuransnivåer enligt artikel 46 och, utan onödigt dröjsmål, eventuella senare ändringar av dessa.

2. Ett år efter ikraftträdandet av ett europeiskt system för cybersäkerhetscertifiering ska kommissionen offentliggöra en förteckning över anmälda organ för bedömning av överensstämmelse i *Europeiska gemenskapernas officiella tidning*.

3. Om kommissionen mottar en anmälan efter utgången av den period som avses i punkt 2 ska den i *Europeiska unionens officiella tidning* offentliggöra ändringarna av

den förteckning som avses i punkt 2 inom två månader från dagen för mottagandet av den anmälan.

4. En nationell tillsynsmyndighet för certifiering får lämna in en begäran till kommissionen om att stryka ett organ för bedömning av överensstämmelse, som anmälts av den nationella tillsynsmyndigheten för certifiering, från den förteckning som avses i punkt 2 i denna artikel. Kommissionen ska i *Europeiska unionens officiella tidning* offentliggöra motsvarande ändringar av förteckningen inom en månad från och med dagen för mottagandet av begäran från den nationella tillsynsmyndigheten för certifiering.

5. Kommissionen får genom genomförandeakter fastställa förutsättningar, format och förfaranden för de anmälningar som avses i punkt 1 i denna artikel. Dessa genomförandeakter ska antas i enlighet med det granskningsförfarande som avses i artikel 55.2.

Artikel 53

Europeiska gruppen för cybersäkerhetscertifiering

1. Europeiska gruppen för cybersäkerhetscertifiering (nedan kallad *gruppen*) ska inrättas.

2. Gruppen ska bestå av de nationella tillsynsmyndigheterna för certifiering. Myndigheterna ska företrädas av sina myndighetschefer eller av andra högre företrädare för nationella tillsynsmyndigheter för certifiering.

3. Gruppen ska ha i uppgift att

   (a) ge råd till och bistå kommissionen i dess arbete för att säkerställa ett konsekvent genomförande och en konsekvent tillämpning av denna avdelning, särskilt när det gäller frågor som rör cybersäkerhetscertifiering, strategisamordning och utarbetandet av de europeiska systemen för cybersäkerhetscertifiering,

   (b) ge råd till, bistå och samarbeta med Enisa när det gäller utarbetande av förslag till system i enlighet med artikel 44 i denna förordning,

   (c) föreslå att kommissionen uppmanar byrån att utarbeta ett förslag till ett europeiskt system för cybersäkerhetscertifiering i enlighet med artikel 44 i denna förordning,

   (d) anta yttranden riktade till kommissionen rörande underhåll och översyn av befintliga europeiska system för cybersäkerhetscertifiering,

   (e) undersöka den relevanta utvecklingen på området cybersäkerhetscertifiering och utbyta god praxis om system för cybersäkerhetscertifiering,

   (f) underlätta samarbetet mellan nationella tillsynsmyndigheter för certifiering enligt denna avdelning genom utbyte av information, särskilt genom att fastställa metoder för ett effektivt informationsutbyte om alla frågor som rör cybersäkerhetscertifiering.

4. Kommissionen ska vara ordförande i gruppen och tillhandahålla sekretariatet för gruppen, med stöd från Enisa i enlighet med artikel 8 a.

Artikel 54

Sanktioner

Medlemsstaterna ska fastställa regler om sanktioner vid överträdelse av denna avdelning och europeiska system för cybersäkerhetscertifiering, och ska vidta alla nödvändiga åtgärder för att se till att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande. Medlemsstaterna ska till kommissionen anmäla dessa regler och åtgärder [senast den .../utan dröjsmål] samt eventuella ändringar som berör dem.

AVDELNING IV
SLUTBESTÄMMELSER

Artikel 55
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 4 i förordning (EU) nr 182/2011 tillämpas.

Artikel 56
Utvärdering och översyn

1. Senast fem år efter den dag som anges i artikel 58, och därefter vart femte år, ska kommissionen bedöma effekterna, ändamålsenligheten och effektiviteten hos byråns arbete samt dess arbetsmetoder och eventuella behov av att ändra byråns mandat samt de finansiella följderna av sådana ändringar. Utvärderingen ska beakta alla synpunkter som byrån mottagit beträffande sin verksamhet. Om kommissionen anser att byråns fortsatta existens inte längre är motiverad med avseende på de mål, mandat och uppgifter som den tilldelats, kan den föreslå att de bestämmelser i denna förordning som rör byrån ändras.
2. Utvärderingen ska även bedöma effekterna, ändamålsenligheten och effektiviteten hos bestämmelserna i avdelning III i fråga om målen att säkerställa en tillräcklig nivå avseende cybersäkerhet hos IKT-produkter och IKT-tjänster i unionen och förbättra den inre marknadens funktion.
3. Kommissionen ska översända utvärderingsrapporten tillsammans med dess slutsatser till Europaparlamentet, rådet och styrelsen. Utvärderingsrapportens resultat ska offentliggöras.

Artikel 57
Upphävande och succession

1. Förordning (EG) nr 526/2013 ska upphöra att gälla med verkan från och med den [….].
2. Hänvisningar till förordning (EG) nr 526/2013 och till Enisa ska betraktas som hänvisningar till denna förordning och till byrån.
3. Byrån efterträder den byrå som inrättades genom förordning (EG) nr 526/2013 när det gäller all äganderätt samt alla avtal, rättsliga skyldigheter, anställningskontrakt, finansiella åtaganden och ansvarsskyldigheter. Alla befintliga beslut som fattats av styrelsen och direktionen ska fortsätta att gälla, förutsatt att de inte strider mot bestämmelserna i denna förordning.
4. Byrån ska inrättas på obestämd tid med början den […].

5. Den verkställande direktör som har utsetts i enlighet med artikel 24.4 i förordning (EG) nr 526/2013 ska vara byråns verkställande direktör under den återstående delen av sin mandatperiod.

6. Styrelseledamöterna och deras suppleanter som utsetts i enlighet med artikel 6 i förordning (EG) nr 526/2013 ska vara ledamöter och suppleanter i byråns styrelse under den återstående delen av sin mandatperiod.

Artikel 58

1. Denna förordning träder i kraft den tjugonde dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

2. Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den

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

FINANSIERINGSÖVERSIKT FÖR RÄTTSAKT

1. GRUNDLÄGGANDE UPPGIFTER OM FÖRSLAGET ELLER INITIATIVET

1.1. Förslagets eller initiativets beteckning

Förslag till Europaparlamentets och rådets förordning om Enisa, ”EU:s cybersäkerhetsbyrå”, och om upphävande av förordning (EU) nr 526/2013 och om cybersäkerhetscertifiering av informations- och kommunikationsteknik (”cybersäkerhetsakten”)

1.2. Berörda politikområden

Politikområde: 09 - Kommunikationsnät, innehåll och teknik

Verksamhet: 09.02 Den digitala inre marknaden

1.3. Typ av förslag eller initiativ

☒ Ny åtgärd (Avdelning III – Certifiering)

☐ Ny åtgärd som bygger på ett pilotprojekt eller en förberedande åtgärd[43]

☒Befintlig åtgärd vars genomförande förlängs i tiden (Avdelning II – Enisas mandat)

☐ Tidigare åtgärd som omformas till eller ersätts av en ny

1.4. Mål

1.4.1. Fleråriga strategiska mål för kommissionen som förslaget eller initiativet är avsett att bidra till

1. Öka resiliensen hos medlemsstaterna, näringslivet och EU som helhet.

2. Säkerställa en väl fungerande inre marknad för IKT-varor och IKT-tjänster.

3. Öka konkurrenskraften på världsmarknaden för de EU-företag som är verksamma på IKT-området.

4. Tillnärma den nationella lagstiftning som fordrar cybersäkerhet.

1.4.2. Specifikt/specifika mål

Med de allmänna målsättningarna i åtanke, och sett i ett vidare sammanhang av den reviderade strategin för cybersäkerhet, är syftet med instrumentet att avgränsa Enisas räckvidd och mandat och skapa en EU-ram för certifiering av IKT-produkter och IKT-tjänster, för att uppnå följande specifika mål:

1. Öka medlemsstaternas och företagens **kapacitet och beredskap**.
2. Förbättra **samarbetet och samordningen** mellan medlemsstaterna och EU:s institutioner, byråer och organ.
3. Öka **EU:s förmåga att komplettera medlemsstaternas åtgärder**, i synnerhet när det gäller gränsöverskridande cyberkriser.
4. Öka allmänhetens och företagens **medvetenhet** om cybersäkerhetsfrågor.
5. Stärka förtroendet för den digitala inre marknaden och digital innovation genom att öka den övergripande **öppenheten i nivån av cybersäkerhet**[44] hos IKT-produkter

[43] I den mening som avses i artikel 54.2 a eller b i budgetförordningen.

och IKT-tjänster.

Genom följande åtgärder kommer Enisa bidra till att ovanstående mål nås:

Ökat bistånd vid beslutsfattande – ge kommissionen och medlemsstaterna vägledning och råd om hur man ska uppdatera och utveckla ett normativt regelverk för cybersäkerhet som präglas av en helhetssyn samt sektorspecifika initiativ till politik och lagstiftning som rör cybersäkerhet; bidra till arbetet i samarbetsgruppen (artikel 11 i direktiv (EU) 2016/1148) genom att tillhandahålla sakkunskap och tekniskt bistånd; stödja utvecklingen och genomförandet av politiken på områdena elektronisk identitet och betrodda tjänster; främja utbyte av bästa praxis mellan behöriga myndigheter.

Öka stödet till kapacitetsuppbyggnad – hjälpa medlemsstaterna och unionens institutioner, organ och byråer att utveckla och förbättra förebyggande, upptäckt och analys av cybersäkerhetsproblem och incidenter samt sin responskapacitet; hjälpa medlemsstaterna, på deras begäran, i utvecklingen av nationella CSIRT-enheter och nationella strategier för cybersäkerhet; bistå unionens institutioner vid utarbetandet och översynen av unionens strategier för cybersäkerhet; tillhandahålla utbildningar i cybersäkerhet; bistå medlemsstaterna via samarbetsgruppen med att utbyta bästa praxis; underlätta inrättandet av sektorsvisa centrum för informationsutbyte och analys (Isac).

Stöd till operativt samarbete och krishantering – stödja samarbete mellan behöriga offentliga organ och mellan intressenter genom att upprätta ett systematiskt samarbete med de av EU:s institutioner, organ, kontor och byråer som arbetar med cybersäkerhet, it-brottslighet, integritetsskydd och skydd av personuppgifter; tillhandahålla CSIRT-nätverkets sekretariat (artikel 12.2 i direktiv (EU) 2016/1148) samt bidra till det operativa samarbetet inom nätverket genom att i samarbete med CERT-EU ge stöd till medlemsstaterna, på deras begäran; anordna regelbundna cybersäkerhetsövningar; bidra till att utveckla en samarbetsinriktad respons på storskaliga gränsöverskridande cybersäkerhetsincidenter och cybersäkerhetskriser; i samarbete med CSIRT-nätverket göra tekniska efterhandsundersökningar av allvarliga incidenter och utfärda rekommendationer om uppföljning.

Marknadsrelaterade uppgifter (standardisering, certifiering) – utföra ett antal uppgifter som specifikt stöder den inre marknaden: utgöra ”marknadsobservatorium” inom cybersäkerhet genom att analysera relevanta trender på cybersäkerhetsmarknaden för att bättre matcha utbud och efterfråga; stödja och främja utvecklingen och genomförandet av EU:s politik för cybersäkerhetscertifiering av IKT-produkter och IKT-tjänster genom att förbereda förslag till europeiska system för cybersäkerhetscertifiering av IKT-produkter och IKT-tjänster, tillhandahålla sekretariatstjänster åt unionens cybersäkerhetscertifieringsgrupp, tillhandahålla riktlinjer och bästa praxis i fråga om säkerhetskrav för IKT-produkter och IKT-tjänster i samarbete med nationella tillsynsmyndigheter och branschen. **Ökat stöd till kunskapshöjande verksamhet och informations- och upplysningsverksamhet** – ge råd och stöd till kommissionen och medlemsstaterna för att uppnå en hög kunskapsnivå i hela unionen om nät- och frågor rörande informationssäkerhet och dess tillämpning till intressenterna från näringslivet. Detta förutsätter också att information om säkerhet i nätverks- och informationssystemen [eller cybersäkerhet] samlas in, sammanställs och tillgängliggörs för allmänheten via en särskild portal. En annan viktig faktor är upplysningsverksamhet och informationskampanjer riktade till allmänheten om cybersäkerhetsrisker.

[44] Med transparens i fråga om assuransnivån för cybersäkerhet avses att ge användarna tillräcklig information om cybersäkerhetsegenskaperna hos en viss IKT-produkt, IKT-tjänst eller IKT-process, så att de objektivt kan fastställa cybersäkerhetsnivån hos denna IKT-produkt, IKT-tjänst eller IKT-process.

Ökat stöd till forskning och innovation – ge råd om behov och prioriteringar för forskningen på området cybersäkerhet.

Stöd till internationellt samarbete – stödja unionens insatser när det gäller samarbete med tredjeländer och internationella organisationer för att främja internationellt samarbete kring cybersäkerhet.

CERTIFIERING

En certifieringsram kommer att bidra till att målen nås genom att öka den övergripande öppenheten i nivån av cybersäkerhet[45] hos IKT-produkter och IKT-tjänster och därigenom stärka förtroendet för den digitala inre marknaden och digital innovation. Detta bör dessutom bidra till att undvika en **uppsplittring av certifieringssystemen** i EU och de därtill knutna säkerhetskraven och utvärderingskriterierna i de olika medlemsstaterna och sektorerna;

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.

En förstärkning av Enisa (som ger stöd till förmåga, förebyggande, samarbete och information på EU-nivå, och således utformat att öka EU:s övergripande cyberresiliens) samt stöd till EU-ramen för certifiering av IKT-produkter och IKT-tjänster väntas få följande konsekvenser (förteckningen är inte uttömmande):

Övergripande effekt:

- Övergripande positiv effekt på den inre marknaden tack vare minskad fragmentering av marknaden och skapande av förtroende för digitala tekniker genom bättre samarbete, mer harmoniserade strategier för EU-politiken för cybersäkerhet och ökad kapacitet på EU-nivå. Detta bör ge en positiv ekonomisk effekt genom att det bidrar till att minska kostnaderna för cybersäkerhets-/it-brottslighetsincidenter, vars ekonomiska inverkan i unionen uppskattas till 0,41 % av EU:s BNP (dvs. Omkring 55 miljarder euro).

Specifika resultat:

Ökad cybersäkerhetskapacitet och beredskap i medlemsstaterna och näringslivet

– Förbättrad cybersäkerhetskapacitet och cybersäkerhetsberedskap i medlemsstaterna (tack vare långsiktig strategisk analys av cyberhot och cyberincidenter, riktlinjer och rapporter, förmedling av sakkunskap och god praxis, utbildning och tillgång till utbildningsmaterial och förstärkta Cyber Europe-övningar).

– Förbättring av de privata aktörernas kapacitet tack vare stöd till inrättandet av centrum för informationsutbyte och analys (Isac) inom olika sektorer.

– Förbättrad cybersäkerhetsberedskap i EU och medlemsstaterna tack vare noggrant inövade och överenskomna planer i händelse av storskaliga gränsöverskridande cybersäkerhetsincidenter som testats vid Cyber Europe-övningar.

Förbättrat samarbetet och förbättrad samordningen mellan medlemsstaterna och EU:s institutioner, byråer och organ

[45] Med transparens i fråga om assuransnivån för cybersäkerhet avses att ge användarna tillräcklig information om cybersäkerhetsegenskaperna hos en viss IKT-produkt, IKT-tjänst eller IKT-process, så att de objektivt kan fastställa cybersäkerhetsnivån hos denna IKT-produkt, IKT-tjänst eller IKT-process.

– Bättre samarbete både inom och mellan den offentliga och privata sektorn.

– Mer enhetlig hållning rörande genomförandet av it-säkerhetsdirektivet över gränser och mellan sektorer.

– Förbättrat samarbete kring certifiering tack vare en institutionell ram som möjliggör utveckling av europeiska cybersäkerhetscertifieringssystem och utveckling av en gemensam politik på detta område.

Ökad kapacitet på EU-nivå att komplettera medlemsstaternas åtgärder

– Förbättring av ”EU:s operativa kapacitet” att komplettera medlemsstaternas åtgärder och stödja dem, på begäran och beträffande ett begränsat antal och i förväg identifierade tjänster. Detta förväntas ha en positiv inverkan på förebyggande, upptäckt och respons för incidenter, både på medlemsstatsnivå och på EU-nivå.

Ökad medvetenhet hos allmänheten och företagen om cybersäkerhetsfrågor

– Ökning av den allmänna medvetenheten hos invånarna och företagen om cybersäkerhetsfrågor.

– Förbättrad förmåga att göra välgrundade köpbeslut för IKT-produkter och IKT-tjänster tack vare cybersäkerhetscertifiering.

Stärkt förtroende för den digitala inre marknaden och digital innovation genom ökad öppenhet i nivån av cybersäkerhet hos IKT-produkter och IKT-tjänster

– ökad öppenhet i nivån av cybersäkerhet[46] hos IKT-produkter och IKT-tjänster tack vare en förenkling av förfarandena för säkerhetscertifiering via en EU-omfattande ram.

– Förbättrade garantier rörande säkerhetsegenskaperna hos IKT-produkter och IKT-tjänster.

– Ökad användning av säkerhetscertifiering som stimuleras av förenklade förfaranden, lägre kostnader och utsikter till EU-omfattande affärsmöjligheter som inte hindras av marknadsfragmentering.

– Förbättrad konkurrenskraft inom EU:s marknad för cybersäkerhet på grund av minskade kostnader och administrativa bördor för små och medelstora företag och undanröjande av potentiella hinder för marknadstillträde orsakade av många olika nationella certifieringssystem.

Övrigt

– Ingen betydande miljöpåverkan förväntas för något av målen.

– Med avseende på EU-budgeten kan effektivitetsvinster förväntas genom ökat samarbete och samordning av verksamheten mellan EU:s institutioner, byråer och organ.

1.4.4. Indikatorer för bedömning av resultat eller verkan

Ange vilka indikatorer som ska användas för att följa upp hur förslaget eller initiativet genomförs.

(a)

[46] Med transparens i fråga om assuransnivån för cybersäkerhet avses att ge användarna tillräcklig information om cybersäkerhetsegenskaperna hos en viss IKT-produkt, IKT-tjänst eller IKT-process, så att de objektivt kan fastställa cybersäkerhetsnivån hos denna IKT-produkt, IKT-tjänst eller IKT-process.

Mål: Öka medlemsstaternas och företagens förmåga och beredskap:

- Antal utbildningar som anordnas av Enisa.
- Geografisk täckning (antal länder och områden) hos det direkta stödet från Enisa.
- Beredskapsnivå som nåtts av medlemsstaterna i fråga om CSIRT-enheternas löptid och övervakning av cybersäkerhetsrelaterade rättsliga åtgärder.
- Olika typer av EU-omfattande bästa praxis för kritisk infrastruktur som tillhandahålls av Enisa.
- Olika typer av EU-omfattande bästa praxis för små och medelstora företag som tillhandahålls av Enisa.
- Årlig strategisk analys av cyberhot och cyberincidenter som offentliggörs av Enisa för att identifiera nya trender.
- Regelbundna bidrag från Enisa till arbetet inom cybersäkerhetsarbetsgrupperna inom de europeiska standardiseringsorganisationerna.

Mål: Förbättra samarbetet och samordningen mellan medlemsstaterna och EU:s institutioner, byråer och organ:

- Antal medlemsstater som har använt Enisas rekommendationer och yttranden i sin beslutsprocess.
- Antal EU:s institutioner, byråer och organ som har använt Enisas rekommendationer och yttranden i sin beslutsprocess.
- Regelbundet genomförande av CSIRT-nätverkets arbetsprogram, och väl fungerande it-infrastruktur och kommunikationskanaler inom CSIRT-nätverket.
- Antalet tekniska rapporter som ställs till förfogande för och används av samarbetsgruppen.
- Konsekvent strategi för it-säkerhetsdirektivets genomförande över gränser och mellan sektorer.
- Antalet utvärderingar som Enisa gör av hur regelverket följs.
- Antalet ISAC verksamma i olika sektorer, särskilt för kritiska infrastrukturer.
- Upprättande och regelbunden drift av en informationsplattform för spridning av cybersäkerhetsinformation från EU:s institutioner, byråer och organ.
- Regelbundna bidrag till utarbetandet av arbetsprogrammen för EU:s forskning och innovation.
- Samarbetsavtal mellan Enisa, EC3 och CERT-EU på plats.
- Antalet certifieringssystem som tagits med i och utvecklats inom ramprogrammet.

Mål: Öka EU:s förmåga att komplettera medlemsstaternas åtgärder, i synnerhet när det gäller gränsöverskridande cyberkriser:

- Årlig strategisk analys av cyberhot och cyberincidenter som offentliggörs av Enisa för att identifiera nya trender.
- Offentliggörande av aggregerade uppgifter om incidenter som rapporterats av Enisa i enlighet med it-säkerhetsdirektivet.

- Antalet EU-omfattande övningar som samordnas av byrån och antalet medlemsstater och organisationer som deltar.
- Antalet förfrågningar från medlemsstaterna om stöd från Enisa med incidenthanteringsåtgärder och antalet åtgärder som Enisa gett stöd till.
- Antal analyser av sårbarhet, artefakter och incidenter som utförs av Enisa i samarbete med CERT-EU.
- Tillgång till EU-omfattande lägesrapporter på grundval av de uppgifter som medlemsstaterna och av andra parter ställer till förfogande för Enisa i händelse av storskaliga gränsöverskridande cyberincidenter.

Mål: Öka allmänhetens och företagens medvetenhet om cybersäkerhetsfrågor:

- Anordnande av regelbundna EU-omfattande och nationella informationskampanjer och regelbundna uppdateringar av ämnena i överensstämmelse med de framväxande utbildningsbehoven.
- Ökning av cybermedvetenheten bland EU-medborgarna.
- Anordnande av regelbundna frågesporter om cybersäkerhetsmedvetenhet och en ökning av andelen korrekta svar med tiden.
- Regelbundet offentliggörande av bra praxis i fråga om cybersäkerhet och cyberförsvar riktat till anställda och organisationer.

Mål: Stärka förtroendet för den digitala inre marknaden och digital innovation genom att öka den övergripande öppenheten i nivån av cybersäkerhet[47] hos IKT-produkter och IKT-tjänster:

- Antalet system som följer EU:s ram
- Minskade kostnader för att få IKT-säkerhetsintyg.
- Antalet organ för bedömning av överensstämmelse specialiserade inom IKT-certifiering, i alla medlemsstater.
- Inrättandet av en EU-cybercertifieringsgrupp och anordnande av regelbundna möten.
- Riktlinjer för certifiering enligt den gällande EU-ramen.
- Regelbundet offentliggörande av analyser av de viktigaste utvecklingstendenserna på EU-marknaden för cybersäkerhet.
- Antalet certifierade IKT-produkter och IKT-tjänster enligt EU-ramen för IKT-säkerhetscertifiering.
- Ökat antal slutanvändare som är medvetna om säkerhetsdetaljerna i IKT-produkter och -tjänster.

(b)

1.4.5. Behov som ska tillgodoses på kort eller lång sikt

Med beaktande av de rättsliga kraven och de snabba förändringarna i cybersäkerhetslandskapet fordras en översyn av Enisas mandat för att fastställa en ny

[47] Med transparens i fråga om assuransnivån för cybersäkerhet avses att ge användarna tillräcklig information om cybersäkerhetsegenskaperna hos en viss IKT-produkt, IKT-tjänst eller IKT-process, så att de objektivt kan fastställa cybersäkerhetsnivån hos denna IKT-produkt, IKT-tjänst eller IKT-process.

uppsättning uppgifter och funktioner, med målet att på ett verksamt och effektivt sätt stödja medlemsstaternas, EU-institutionernas och andra berörda parters ansträngningar att säkerställa en trygg cyberrymd i Europeiska unionen. Räckvidden hos det föreslagna mandatet är avgränsad. De områden där byrån har visat ett tydligt mervärde stärks, och tillägg görs av nya områden där bistånd fordras med anledning av nya politiska prioriteringar och instrument, särskilt it-säkerhetsdirektivet, översynen av EU:s strategi för cybersäkerhet, EU:s cybersäkerhetsplan för samarbete vid cyberkriser och IKT-säkerhetscertifiering. Syftet med det föreslagna nya mandatet är att ge byrån en tydligare och mer central roll, särskilt genom att stödja medlemsstaterna mer aktivt i deras arbete med att bemöta specifika hot (operativ kapacitet) och genom att bli ett expertcentrum som bistår medlemsstaterna och kommissionen vid cybersäkerhetscertifiering.

Samtidigt inrättas en EU-ram för cybersäkerhetcertifiering av IKT-produkter och IKT-tjänster i förslaget, och Enisas väsentliga funktioner och uppgifter inom cybersäkerhetscertifiering specificeras. I ramen fastställs gemensamma bestämmelser och förfaranden som möjliggör skapandet av ett EU-omfattande system för cybersäkerhetscertifiering av särskilda IKT-produkter och IKT-tjänster eller för cybersäkerhetsrisker. Genom att europeiska system för cybersäkerhetscertifiering inrättas i enlighet med ramavtalet kommer de certifikat som utfärdats enligt dessa system att kunna vara giltiga och erkännas i alla medlemsstater, och det kommer att bli möjligt att ta itu med den nuvarande marknadsfragmenteringen.

1.4.6. Mervärde av en åtgärd på unionsnivå

Cybersäkerhet är en global fråga, som är gränsöverskridande till sin natur och alltmer sektorsövergripande på grund av ömsesidiga beroendeförhållanden mellan nät och informationssystem. Cybersäkerhetsincidenterna ökar över tiden sett till antal, komplexitet, omfattning och i fråga om inverkan på ekonomi och samhälle, och de förväntas öka ytterligare i takt med den tekniska utvecklingen, till exempel spridningen av sakernas internet. Detta innebär att behovet av ökade gemensamma insatser av medlemsstaterna, EU-institutionerna och privata aktörer för att möta hoten mot cybersäkerheten inte förväntas minska i framtiden.

Syftet med Enisa har sedan inrättandet 2004 varit att främja samarbete mellan medlemsstaterna och nät- och informationssäkerhetsintressenterna, inklusive att stödja offentligt-privat samarbete. Detta samarbetsstöd omfattade det tekniska arbetet för att få en EU-övergripande uppfattning av hotbilden, inrättandet av expertgrupper och anordnandet av cyberincident- och krishanteringsövningar på europeisk nivå inom den offentliga och privata sektorn (särskilt ”Cyber Europe”). Genom it-säkerhetsdirektivet anförtroddes Enisa ytterligare uppgifter, bland annat rollen som sekretariat för CSIRT-nätverket för operativt samarbete mellan medlemsstaterna.

Mervärdet med åtgärder på europeisk nivå, för att främja samarbetet mellan i synnerhet medlemsstaterna men även mellan olika nät- och informationssäkerhetsorgan, har erkänts i rådets slutsatser från 2016[48], och det framgår även tydligt av 2017 års utvärdering av Enisa som visar att byråns mervärde främst ligger i dess förmåga att öka samarbetet mellan dessa intressenter. Det finns ingen annan aktör på EU-nivå som stödjer samarbete mellan samma mängd intressenter på området nät- och informationssäkerhet.

Enisas mervärde, att föra samman aktörer och intressenter på cybersäkerhetsområdet,

[48] Rådets slutsatser om att stärka Europas system för cyberresiliens och främja en konkurrenskraftig och innovativ cybersäkerhetsbransch – 15 november 2016.

gäller även i fråga om certifiering. Ökningen av it-brottsligheten och säkerhetshoten har lett till framväxten av nationella initiativ där man infört höga krav på cybersäkerhet och certifiering för IKT-komponenter som används i traditionell infrastruktur. Dessa initiativ är visserligen viktiga men riskerar att skapa en fragmentering av den inre marknaden och hinder för driftskompatibiliteten. En IKT-försäljare kan behöva genomgå flera certifieringsprocesser för att få sälja sina produkter eller tjänster i flera medlemsstater. Ineffektivitet i de nuvarande certifieringssystemen kommer sannolikt inte att kunna avhjälpas utan ingripande från EU:s sida. I avsaknad av åtgärder är det mycket troligt att fragmenteringen av marknaden ökar på kort till medellång sikt (de närmaste 5–10 åren) i takt med framväxten av nya certifieringssystem. Bristen på samordning och driftskompatibilitet mellan sådana system är en faktor som minskar den digitala inre marknadens potential. Detta visar på mervärdet av att inrätta en europeisk ram för cybersäkerhetscertifieringen hos IKT-produkter och IKT-tjänster genom att skapa de rätta förutsättningarna för att på ett effektivt sätt hantera problemet med förekomsten av flera olika certifieringsförfaranden i olika medlemsstater, vilket sänker certifieringskostnaderna och därigenom gör certifiering i EU generellt mer attraktivt ur ett kommersiellt perspektiv.

1.4.7. Huvudsakliga erfarenheter från liknande försök eller åtgärder

I enlighet med den rättsliga grunden för Enisa har kommissionen gjort en utvärdering av Enisa som omfattar en oberoende undersökning och ett offentligt samråd. I utvärderingen drogs slutsatsen att Enisas mål fortfarande är relevanta i dag. Mot bakgrund av den tekniska utvecklingen, de framväxande hoten och ett betydande behov av ökad nät- och informationssäkerhet i EU finns det ett behov av teknisk sakkunskap om utvecklingen inom nät- och informationssäkerhetsfrågor. Medlemsstaterna behöver öka sin förmåga att förstå och bemöta hot, och intressenterna måste samarbeta inom olika tematiska områden och institutioner emellan.

Enisa har framgångsrikt bidragit till ökad nät- och informationssäkerhet i Europa genom att erbjuda kapacitetsuppbyggnad i 28 medlemsstater, förbättra samarbetet mellan medlemsstaterna och nät- och informationssäkerhetsintressenterna, tillhandahålla sakkunskap, vidta gemenskapsbyggande insatser och ge stöd till politiken.

Även om Enisa har lyckats få till stånd en förändring, åtminstone i viss utsträckning, inom det vidsträckta området nät- och informationssäkerhet, har den ännu inte helt lyckats utveckla ett starkt varumärke och få tillräcklig stor synlighet för att bli erkänd som det ”officiella” centrumet för sakkunskap i Europa. Förklaringen till detta ligger i att Enisa givits ett brett mandat utan att erhålla proportionerliga medel. Dessutom är Enisa den enda EU-byrån med ett tidsbegränsat mandat, vilket begränsar dess förmåga att utveckla en långsiktig vision och stödja sina intressenter på ett hållbart sätt. Detta står också i skarp motsats till bestämmelserna i it-säkerhetsdirektivet, där byrån ges uppgifter utan något slutdatum.

När det gäller cybersäkerhetscertifiering för IKT-produkter och IKT-tjänster finns det för närvarande ingen europeisk ram. Ökningen av it-brottsligheten och säkerhetshoten har lett till framväxten av nationella initiativ, vilket skapar en risk för fragmentering av den inre marknaden.

1.4.8. Förenlighet med andra finansieringsformer och eventuella synergieffekter

Initiativet är i hög grad förenligt med den befintliga politiken, särskilt på området den inre marknaden. Det har utformats i enlighet med den övergripande strategin för cybersäkerhet,

enligt definitionen i översynen av strategin för den digitala inre marknaden, som ett komplement till en omfattande uppsättning åtgärder, såsom översynen av EU:s cybersäkerhetsstrategi, planen för samarbete vid cyberkriser och initiativen för att bekämpa it-brottslighet. Det skulle säkerställa anpassning till och bygga på bestämmelserna i den befintliga lagstiftningen om cybersäkerhet, särskilt it-säkerhetsdirektivet, i syfte att driva arbetet med cyberresiliens inom EU vidare tack vare en ökning av kompetensen, samarbetet, riskhanteringen och medvetenheten om cybersäkerhet.

De föreslagna certifieringsåtgärderna bör tackla den möjliga fragmentering som orsakas av befintliga och nya nationella certifieringssystem, och därmed bidra till utvecklingen av den digitala inre marknaden. Initiativet stöder och kompletterar även genomförandet av it-säkerhetsdirektivet genom att förse de företag som omfattas av direktivet med ett verktyg för att visa att nät- och informationssäkerhetskraven uppfylls i hela unionen.

Den föreslagna europeiska ramen för IKT-cybersäkerhetscertifiering påverkar inte den allmänna dataskyddsförordningen[49], i synnerhet inte de relevanta bestämmelserna rörande certifiering[50], eftersom de gäller säkerhet vid behandling av personuppgifter. Sist men inte minst bör de system som föreslås inom den framtida EU-ramen så långt som möjligt att bygga på internationella standarder för att undvika handelshinder och säkerställa samstämmighet med internationella initiativ.

[49] 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).

[50] T.ex. artiklarna 42 (Certifiering) och 43 (Certifieringsorgan), och artiklarna 57, 58 och 70 om de oberoende tillsynsmyndigheternas relevanta uppgifter och befogenheter och Europeiska dataskyddsstyrelsens uppgifter.

1.5. Tid under vilken åtgärden kommer att pågå respektive påverka resursanvändningen

☐ Förslag eller initiativ som pågår under en **begränsad tid**

– ☐ Förslaget eller initiativet ska gälla från [den DD/MM]ÅÅÅÅ till [den DD/MM]ÅÅÅÅ.

– ☐ Det påverkar resursanvändningen från ÅÅÅÅ till ÅÅÅÅ.

☒ Förslag eller initiativ som pågår under en **obegränsad tid**

– Efter en inledande period 2019–2020,

– beräknas genomförandetakten nå en stabil nivå.

1.6. Planerad metod för genomförandet[51]

☒ **Direkt förvaltning** som sköts av kommissionen (Avdelning III – Certifiering) via

– ☐ genomförandeorgan.

☐ **Delad förvaltning** med medlemsstaterna

☒ **Indirekt förvaltning** genom att uppgifter som ingår i budgetgenomförandet delegeras till

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

☐EIB och Europeiska investeringsfonden,

☒ organ som avses i artiklarna 208 och 209 i budgetförordningen (Avdelning II – Enisa),

☐ offentligrättsliga organ,

☐ privaträttsliga organ som anförtrotts uppgifter som faller inom offentlig förvaltning och som lämnat tillräckliga ekonomiska garantier,

☐ organ som omfattas av privaträtten i en medlemsstat, som anförtrotts genomförandet av ett offentlig-privat partnerskap och som lämnat tillräckliga ekonomiska garantier,

☐ personer som anförtrotts ansvaret för genomförandet av särskilda åtgärder inom Gusp som följer av avdelning V i fördraget om Europeiska unionen och som anges i den grundläggande rättsakten.

Anmärkningar

Förordningen gäller följande: – I avdelning II i förslaget till förordning görs en översyn av mandatet för Europeiska unionens byrå för nät- och informationssäkerhet (Enisa), varigenom byrån ges en viktig roll när det gäller certifiering. – I avdelning III fastställs en ram för inrättandet av europeiska system för cybersäkerhetscertifiering av IKT-produkter och IKT-tjänster, där Enisa spelar en avgörande roll.

[51] 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.

2. FÖRVALTNING

2.1. Bestämmelser om uppföljning och rapportering

Ange intervall och andra villkor för sådana åtgärder:

Övervakningen ska inledas direkt efter antagandet av rättsakten och kommer att inriktas på dess antagande. Kommissionen kommer att anordna möten med Enisa, företrädare för medlemsstaterna (t.ex. expertgrupp) och de relevanta intressenterna för att i synnerhet underlätta genomförandet av bestämmelserna om certifiering, t.ex. inrättandet av styrelsen.

Den första utvärderingen bör äga rum fem år efter ikraftträdandet av det rättsliga instrumentet, förutsatt att tillräckliga uppgifter finns tillgängliga. En uttrycklig utvärderings- och översynsklausul [artikel XXX], enligt vilken kommissionen ska göra en oberoende bedömning, införs i det rättsliga instrumentet. Kommissionen kommer därefter att avlägga rapport till Europaparlamentet och rådet om sin utvärdering, som vid behov åtföljs av ett förslag om översyn av direktivet, för att mäta förordningens inverkan och mervärde. Ytterligare utvärderingar bör ske vart femte år. Kommissionen ”bättre lagstiftning”-metod för utvärderingar kommer att användas. Dessa utvärderingar kommer att genomföras med hjälp av riktade expertdiskussioner, studier och omfattande samråd med berörda parter.

Byråns verkställande direktör bör lägga fram en efterhandsutvärdering av Enisas verksamhet för styrelsen vartannat år. Byrån bör även utarbeta en handlingsplan för uppföljning av de slutsatser som dragits av efterhandsutvärderingarna samt rapportera om framstegen till kommissionen vartannat år. Styrelsen bör bära ansvaret för att övervaka att det sker en lämplig uppföljning av de slutsatserna.

Påstådda missförhållanden i byråns verksamhet kan komma att undersökas av Europeiska ombudsmannen i enlighet med artikel 228 i fördraget.

Uppgiftskällorna till den planerade övervakningen kommer huvudsakligen att vara Enisa, europeiska gruppen för cybersäkerhetscertifiering (*European Cyber-Certification Group*), CSIRT-nätverket och medlemsstaternas myndigheter. Utöver uppgifterna i rapporterna (inklusive de årliga verksamhetsrapporterna) från Enisa, europeiska gruppen för cybersäkerhetscertifiering, samarbetsgruppen och CSIRT-nätverket, kommer särskilda verktyg för uppgiftsinsamling vid behov att användas (t.ex. enkäter till de nationella myndigheterna, rapporter från ”månaden för cybersäkerhet”-kampanjen och EU-omfattande övningar).

2.2. Administrations- och kontrollsystem

2.2.1. Risker som identifierats:

De risker som identifierats är begränsade: Det finns redan en EU-byrå, och dess mandat kommer att avgränsas: de områden där byrån har visat ett tydligt mervärde kommer att stärkas och nya områden kommer att läggas till där bistånd behövs med anledning av nya politiska prioriteringar och instrument, särskilt it-säkerhetsdirektivet, översynen av EU:s strategi för cybersäkerhet, den kommande EU-samordningsplanen för samarbete vid cyberkriser, och IKT-säkerhetscertifieringen.

I förslaget redogörs därför i detalj för byråns uppgifter och det leder till effektivitetsvinster. De ökade operativa befogenheterna och uppgifterna utgör inte någon verklig risk, eftersom de

skulle komplettera medlemsstaternas åtgärder och stödja dem, på begäran och i ett begränsad antal och i förväg identifierade tjänster.

Den föreslagna modellen för byrån, i enlighet med den gemensamma ansatsen, säkerställer att kontrollen är tillräcklig för att Enisa ska arbeta för att uppfylla sina mål. De operativa och finansiella riskerna för de föreslagna ändringarna förefaller begränsade.

Samtidigt är det nödvändigt att säkerställa tillräckliga finansiella medel för att Enisa ska kunna fullgöra sina uppgifter enligt det nya mandatet, bland annat i fråga om certifiering.

2.2.2. Planerade kontrollmetoder

Byråns räkenskaper kommer att överlämnas till revisionsrätten för godkännande och vara föremål för förfarandet för beviljande av ansvarsfrihet och revisioner planeras.

Byråns verksamhet ska också övervakas av ombudsmannen i enlighet med bestämmelserna i artikel 228 i fördraget.

Se även punkt 2.1 och punkt 2.2.1 ovan.

2.3. Åtgärder för att förebygga bedrägeri och oegentligheter/oriktigheter

Beskriv förebyggande åtgärder (befintliga eller planerade)

Enisas förebyggande åtgärder skulle särskilt gälla följande:

– Betalningen för beställda tjänster eller undersökningar ska kontrolleras av byråns personal 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.

– Byrån ska, inom sex månader från dagen för den här förordningens ikraftträdande, 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) och ska utan dröjsmål anta erforderliga bestämmelser som ska vara 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 anslag	Bidrag			
		Diff./ Icke-diff[52].	från Efta-länder[53]	från kandidat-länder[54]	från tredje-länder	enligt artikel 21.2 b i budgetförordningen
1a Konkurrenskraft för tillväxt och sysselsättning	09.0203 Enisa och IKT-säkerhetscertifiering	Diff.	JA	NEJ	NEJ	NEJ
5 Administrativa utgifter]	09.0101 Utgifter för personal i aktiv tjänst inom politikområdet kommunikationsnät, innehåll och teknik 09.0102 Utgifter för extern personal i aktiv tjänst inom politikområdet kommunikationsnät, innehåll och teknik	Icke-diff.	NEJ	NEJ	NEJ	NEJ

[52] Differentierade respektive icke-differentierade anslag.
[53] Efta: Europeiska frihandelssammanslutningen.
[54] Kandidatländer och i förekommande fall potentiella kandidatländer i västra Balkan.

	09.010211 Andra administrativa utgifter					

3.2. Beräknad inverkan på utgifterna

3.2.1. Sammanfattning av den beräknade inverkan på utgifterna

Miljoner euro (avrundat till tre decimaler)

Rubrik i den fleråriga budgetramen	1a	Konkurrenskraft för tillväxt och sysselsättning

Enisa			**Grund** **2017 (31/12/2016)**		**2019** ***(fr.o.m. 1/7/2019)***	**2020**	**2021**	**2022**	**TOTALT**
Avdelning 1: Personalkostnader *(inklusive utgifter för rekrytering av personal, utbildning, socialmedicinsk infrastruktur och externa tjänster)*	Åtaganden	1	6,387		9,899	12,082	13,349	13,894	**49,224**
	Betalningar	2	6,387		9,899	12,082	13,349	13,894	**49,224**
Avdelning 2: Infrastruktur- och driftsutgifter	Åtaganden	1a	1,770		1,957	2,232	2,461	2,565	**9,215**
	Betalningar	2 a	1,770		1,957	2,232	2,461	2,565	**9,215**
Avdelning 3: Driftsutgifter	Åtaganden	3 a	3,086		4,694	6,332	6,438	6,564	**24,028**
	Betalningar	3b	3,086		4,694	6,332	6,438	6,564	**24,028**
TOTALA anslag till Enisa	Åtaganden	=1+1a +3a	**11,244**		16,550	20,646	22,248	23,023	**82,467**
	Betalningar	=2+2a +3b	**11,244**		**16,550**	**20,646**	**22,248**	**23,023**	**82,467**

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

Miljoner euro (avrundat till tre decimaler)

		2019 *(fr.o.m. 1/7/2019)*	**2020**	**2021**	**2022**	**TOTALT**
GD: CNECT						
• Personalresurser		0,216	0,846	0,846	0,846	**2,754**
• Övriga administrativa utgifter		0,102	0,235	0,238	0,242	**0,817**
TOTALT GD CNECT	Anslag	0,318	1,081	1,084	1,088	**3,571**

Personalkostnader har beräknats enligt planerat anställningsdatum (anställningen påbörjas 1.7.2019).

Utsikterna för medlen efter 2020 är preliminära och utan påverkar inte kommissionens förslag till den fleråriga budgetramen för perioden efter 2020.

TOTALA anslag för RUBRIK 5 i den fleråriga budgetramen	(summa åtaganden = summa betalningar)	0,318	1,081	1,084	1,088	**3,571**

Miljoner euro (avrundat till tre decimaler)

		2019	**2020**	**2021**	**2022**	**TOTALT**
TOTALA anslag för RUBRIKERNA 1–5 i den fleråriga budgetramen	Åtaganden	16,868	21,727	23,332	24,11	**86,038**
	Betalningar	16,868	21,727	23,332	24,11	**86,038**

3.2.2. Beräknad inverkan på byråns anslag

– ☐ 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)

Mål- och resultatbeteckning[55] ⇩	**2019**	**2020**	**2021**	**2022**	**TOTALT**
Öka medlemsstaternas och företagens förmåga och beredskap.	1,408	1,900	1,931	1,969	7,208
Förbättra samarbetet och samordningen mellan medlemsstaterna och EU:s institutioner, byråer och organ.	0,939	1,266	1,288	1,313	4,806
Öka kapaciteten på EU-nivå för att komplettera medlemsstaternas åtgärder, i synnerhet när det gäller gränsöverskridande cyberkriser.	0,704	0,950	0,965	0,985	3,604
Öka medborgarnas och företagens medvetenhet om cybersäkerhetsfrågor.	0,704	0,950	0,965	0,985	3,604
Stärka förtroendet för den digitala inre marknaden och digital innovation genom att öka den övergripande öppenheten i nivån av cybersäkerhet hos IKT-produkter och IKT-tjänster.	0,939	1,266	1,288	1,313	4,806
TOTAL KOSTNAD	4 694	6,332	6,437	6,565	24,028

[55] * I denna tabell anges endast driftsutgifter enligt avdelning 3

3.2.3. Beräknad inverkan på Enisas personalresurser

3.2.3.1. Sammanfattning

– ☐ 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)

	Q3/4 2019	**2020**	**2021**	**2022**
Tillfälligt anställda (lönegrad AD)	4,242	5,695	6,381	6,709
Tillfälligt anställda (lönegrad AST)	1,601	1,998	2,217	2,217
Kontraktsanställda	2,041	2,041	2,041	2,041
Nationella experter	0,306	0,447	0,656	0,796
TOTALT	**8,190**	**10,181**	**11,295**	**11,763**

Personalkostnader har beräknats enligt planerat anställningsdatum (för nuvarande Enisa-personal antogs tillsättning av samtliga poster har skett fr.o.m. 1.1.2019). För den nya personalen planerades tillsättningen av tjänsterna ske successivt fr.o.m. 1.7.2019 och samtliga tjänster ha tillsatts 2022. Prognosen för resurserna efter 2020 är preliminär och påverkar inte kommissionens förslag till den fleråriga budgetramen för perioden efter 2020.

Beräknad inverkan på personalen (ytterligare heltidsekvivalenter) – tjänsteförteckning

Tjänstegrupper och grader	2017 **Nuvarande Enisa**	Q3/Q4.2019	2020	2021	2022
AD16					
AD15	1				
AD14					
AD13					
AD12	3	3			
AD11					
AD10	5				
AD9	10	2			
AD8	15	4	2		1
AD7			3	3	2
AD6			3	3	
AD5					
AD Totalt	34	9	8	6	3

AST11 AST10 AST9 AST8 AST7 AST6 AST5 AST4 AST3 AST2 AST1	 2 5 5 2	 1 2	 1 1	 1	
AST Totalt	14	3	2	1	
AST/forskning (SC) 6 AST/forskning (SC) 5 AST/forskning (SC) 4 AST/forskning (SC) 3 AST/forskning (SC) 2 AST/forskning (SC) 1					
AST/SC Totalt					
TOTALT	48	12	10	7	3

Uppgifter för ytterligare AD/AST-personal för att uppnå instrumentets mål enligt beskrivningen i avsnitt 1.4.2:

Uppgifter	AD	AST	SNE	Totalt
Politikutveckl. och kapacitetsuppbyggnad	8	1		9
Operativt samarbete	8	1	7	16
Certifiering (marknadsrelaterade uppgifter)	9	3	2	14
Kunskap, information och medvetenhet	1	1		2
TOTALT	26	6	9	41

Beskrivning av arbetsuppgifterna:

Uppgifter	**Ytterligare resurser som krävs**
Utvecklingen och genomförandet av EU:s politik & kapacitetsuppbyggnad	Bl.a. bistå samarbetsgruppen, stödja enhetligt genomförande av it-säkerhetsdirektivet över gränserna, regelbunden rapportering om hur genomförandet av EU:s regelverk framskrider; ge råd till och samordna sektorsinriktade cybersäkerhetsinitiativ, bl.a. inom energi, transport (t.ex. luftfart, väg, sjöfart, uppkopplade fordon), hälsa, finans, och ge stöd till upprättandet av centrum för informationsutbyte och analys (ISAC) inom olika sektorer.

Operativt samarbete och krishantering	**Uppgifterna skulle omfatta följande:** Tillhandahålla sekretariat till CSIRT-nätverket genom att bl.a. säkerställa att CSIRT-nätverkets it-infrastruktur och kommunikationskanaler fungerar väl. Säkerställa ett strukturerat samarbete med CERT-EU, EC3 och andra relevanta EU-organ. Anordna **Cyber Europe-övningar**[56] – uppgifter i samband med en utökning från vartannat år till varje år samt se till att ett tillbuds samtliga faser, från början till slut, beaktas. **Tekniskt stöd** – uppgifterna skulle bl.a. omfatta strukturerat samarbete med CERT-EU för att tillhandahålla tekniskt stöd i händelse av betydande incidenter och stödja incidentanalys. Detta skulle inbegripa att bistå medlemsstaterna vid incidenthantering och analys av svagheter, artefakter och incidenter. Underlätta samarbetet mellan enskilda medlemsstater kring hantering av nödsituationer genom att analysera och sammanställa nationella lägesrapporter på grundval av uppgifter som ställs till byråns förfogande av medlemsstaterna och andra parter. **Plan för samordnade insatser vid storskaliga gränsöverskridande cyberincidenter** – Enisa kommer att bidra till att utveckla en samarbetsinriktad respons på unions- och medlemsstatsnivå vid stora gränsöverskridande incidenter eller kriser som rör cybersäkerhet, genom att utföra en rad uppgifter, alltifrån att skapa situationsmedvetenhet på unionsnivå till att testa samarbetsplaner för incidenter. **Tekniska efterhandsundersökningar av incidenter** – utföra eller bidra till efterhandsutredningar om incidenter i samarbete med CSIRT-nätverket i syfte att utfärda rekommendationer och stärka kapaciteten i form av offentliga rapporter för att bättre förebygga framtida incidenter.
Marknadsrelaterade uppgifter	Bland uppgifterna skulle ingå att aktivt stödja det

[56] Cyber Europe är den största och mest omfattande cybersäkerhetsövningen på EU-nivå hittills och omfattar över 700 personer som arbetar med cybersäkerhet från samtliga 28 medlemsstater. Den hålls vartannat år. I utvärderingen av Enisa och 2013 års EU-strategi för cybersäkerhet påpekas det att många intressenter föreslår att man ska utöka Cyber Europe till att bli ett årligt evenemang med tanke på den snabba utvecklingen av cyberhot. Detta är dock inte möjligt för närvarande med tanke på Enisas begränsade resurser.

(standardisering, certifiering)	arbete som utförs inom certifieringsramen, bl.a. tillhandahålla teknisk expertis för utarbetande av förslag till europeiska system för cybersäkerhetscertifiering. Bland uppgifterna kommer också ingå stöd till utveckling och genomförande av unionens politik rörande standardisering, certifiering och marknadsobservatorium – det fordrar att man främjar användning av riskhanteringsstandarder för elektroniska produkter, nät och tjänster, och ger råd till leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster om tekniska säkerhetskrav. Det kommer också att ingå att tillhandahålla en analys av de viktigaste tendenserna på marknaden för cybersäkerhet.
Kunskap och information, öka medvetenheten:	För att underlätta tillgången till information om cybersäkerhetsrisker och om hur de kan avhjälpas, och bättre strukturera denna information, får byrån i ny uppgift att utveckla och underhålla unionens ”informationsnav”. Detta omfattar bl.a. att samla och organisera information om säkerheten, särskilt cybersäkerheten, hos de nätverks- och informationssystem som tillhandahålls av EU:s institutioner, byråer och organ, samt gör dessa tillgängliga för allmänheten via en särskild portal. Det skulle också ingå att stödja Enisas verksamhet inom medvetandehöjning för att göra det möjligt för byrån att utöka insatserna.

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)

		Ytterligare personal			
	Grundstruktur 2017	Q3/4 2019	2020	2021	2020
• **Tjänster som tas upp i tjänsteförteckningen (tjänstemän och tillfälligt anställda)**					
09 01 01 01 (vid huvudkontoret eller vid kommissionens kontor i medlemsstaterna)	1	2	3		
• **Extern personal (i heltidsekvivalenter)**[57]					
09 01 02 01 (kontraktsanställda, nationella experter och vikarier finansierade genom ramanslaget)	1	2			
TOTALT		**4**	**3**		

Beskrivning av arbetsuppgifterna:

Tjänstemän och tillfälligt anställda	Företräda kommissionen i byråns styrelse. Utarbeta kommissionens yttrande om Enisas årliga samlade programdokument och övervaka genomförandet av det. Övervaka förberedelserna av byråns budget och övervaka genomförandet den. Bistå byrån med utveckling av verksamheten i enlighet med unionens politik, bland annat genom att delta i relevanta möten. Övervaka genomförandet av ramen för europeiska system för cybersäkerhetscertifiering av IKT-produkter och IKT-tjänster. Upprätthålla kontakterna med medlemsstaterna och andra berörda intressenter när det gäller certifiering. Samarbeta med Enisa kring förslag till system. Ta fram förslag till europeiska

[57] [Denna fotnot förklarar vissa initialförkortningar som inte används i den svenska versionen].

	cybersäkerhetssystem.
Extern personal	Som ovan

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

Förslaget kräver omfördelningar av artikel 09 02 03 till följd av översynen av Enisas mandat, genom vilken Enisa ges nya uppgifter som bl.a. rör it-säkerhetsdirektivets genomförande och den europeiska ramen för cybersäkerhetscertifiering. Berörda belopp:

Budgetår	Planerat	Begärt
2019	10,739	16,550
2020	10,954	20,646
2021	Ej tillämpligt	22,248*
2022	Ej tillämpligt	23,023*

* Detta är en uppskattning. EU-finansieringen efter 2020 kommer att granskas i samband med en kommissionsomfattande diskussion om alla förslag för perioden efter 2020. Det här betyder att kommissionen när den lagt fram sitt förslag för nästa fleråriga budgetram kommer att lägga fram en ändrad finansieringsöversikt för rättsakt som beaktar slutsatserna från konsekvensanalysen[58].

– ☐ Förslaget/initiativet förutsätter att flexibilitetsmekanismen utnyttjas eller att den fleråriga budgetramen revideras[59].

3.2.5. Bidrag från tredje part

– ☐ Det ingår inga bidrag från tredje part i det aktuella förslaget eller initiativet.

– ☒ Förslaget eller initiativet kommer att medfinansieras enligt följande:

[58] Länk till sidan med konsekvensbedömningen.

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

	Budgetår **2019**	Budgetår **2020**	Budgetår **2021**	Budgetår **2022**
Efta:	p.m[60].	p.m.	p.m.	p.m.

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 diverse.

[60] Det exakta beloppet för de efterföljande åren kommer att vara känt när Eftas proportionalitetsfaktor ska fastställas för det berörda året.