Europeiska unionens råd

Bryssel den 29 maj 2018
(OR. en)

9350/18

Interinstitutionellt ärende:
2017/0225 (COD)

CYBER 115
TELECOM 152
CODEC 860
COPEN 163
COPS 175
COSI 129
CSC 170
CSCI 80
IND 143
JAI 514
JAIEX 55
POLMIL 61
RELEX 463

NOT

från:	Ordförandeskapet
till:	Rådet
Föreg. dok. nr:	8834/18
Komm. dok. nr:	12183/17
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") – Allmän riktlinje

I. INLEDNING

1. Den 13 september 2017 antog kommissionen, i samband med sin strategi för den digitala inre marknaden, det ovannämnda förslaget[1] med artikel 114 i EUF-fördraget som rättslig grund, och översände det till rådet och Europaparlamentet. Detta förslag ingår i det s.k. cybersäkerhetspaketet och syftar till en hög nivå av cybersäkerhet, cyberresiliens och förtroende inom unionen, i syfte att säkerställa en väl fungerande inre marknad.

2. Genom förslaget till förordning fastställs mål, uppgifter och organisatoriska aspekter för Enisa – EU:s cybersäkerhetsbyrå – och det skapas en ram för inrättandet av europeiska system för cybersäkerhetscertifiering i syfte att säkerställa en tillräcklig nivå avseende cybersäkerhet hos IKT-produkter och IKT-tjänster i unionen. Kommissionens förslag åtföljs av en konsekvensbedömning där åtta olika politiska alternativ utreds som omfattar översynen av Enisa och cybersäkerhetscertifieringen på IKT-området.

3. Förslaget till förordning innehåller följande två huvuddelar:

   - Ett permanent mandat för byrån med ett avgränsat tillämpningsområde med tanke på behoven i samband med de nya politiska prioriteringarna och instrumenten, och nya uppgifter och funktioner för byrån så att den på ett verksamt och effektivt sätt ska kunna stödja medlemsstaternas, EU-institutionernas och andra berörda parters ansträngningar att säkerställa en trygg cyberrymd.

   - En europeisk ram för cybersäkerhetscertifiering för IKT-produkter och IKT-tjänster och regelverk för europeiska system för cybersäkerhetscertifiering så att certifikat som utfärdats enligt dessa system blir giltiga och erkänns i alla medlemsstater och för att ta itu med den nuvarande marknadsfragmenteringen.

[1] Dok. 12183/17, 12183/1/17 REV 1, 12183/2/17 REV 2.

4. I oktober 2017 begärde Europeiska rådet[2] att kommissionens cybersäkerhetsförslag ska utformas med ett helhetsperspektiv, läggas fram i rätt tid och behandlas utan dröjsmål, på grundval av en handlingsplan som ska upprättas av rådet.

5. Den 12 december 2017 antog allmänna rådet handlingsplanen[3] för genomförandet av rådets slutsatser[4] om det gemensamma meddelandet[5] till Europaparlamentet och rådet: *Resiliens, avskräckning och försvar: stärkt cybersäkerhet i EU*. I handlingsplanen återspeglas rådets ambition att nå fram till en allmän riktlinje om förslaget senast i juni 2018.

6. Angelika NIEBLER (ITRE, EPP) har utnämnts till föredragande i Europaparlamentet. Utskottet för industrifrågor, forskning och energi kommer att rösta om betänkandet den 19 juni 2018.

7. Europeiska ekonomiska och sociala kommittén antog sitt yttrande den 14 februari 2018.

II. ARBETET INOM RÅDET

8. Kommissionen lade fram detta förslag med tillhörande konsekvensbedömning för den övergripande arbetsgruppen för cyberfrågor (nedan kallad *arbetsgruppen*) den 26 september 2017. Därefter behandlade arbetsgruppen konsekvensbedömningen den 20 oktober 2017. Diskussionerna handlade främst om byråns operativa kapacitet och omfattningen av dess interagerande med de nationella behöriga myndigheterna samt vilka konsekvenser ramen för certifiering kommer att få för marknaden och företagens konkurrenskraft. Rent allmänt ställde sig delegationerna positiva till både konsekvensbedömningen och förslaget.

---

2 EUCO 14/17, punkt 11.
3 Dok. 15748/17.
4 Dok. 14435/17.
5 Dok. 12211/17.

9. Diskussionen om själva förslaget inleddes i arbetsgruppen i november 2017 under det estniska ordförandeskapet och fortsatte under det bulgariska ordförandeskapet. Förslaget behandlades under tolv möten och åtta på varandra följande reviderade versioner av förslaget utarbetades i syfte att enas om en allmän riktlinje vid mötet i rådet (transport, telekommunikation och energi) den 8 juni 2018.

10. Resultatet av diskussionerna i arbetsgruppen den 14–15 maj 2018 och ordförandeskapets reviderade kompromisstext återfinns i bilagan. Skälen har anpassats så att de återspeglar ändringarna av de materiella bestämmelserna. Alla ändringar i förhållande till kommissionens förslag är markerade med **fetstil** eller [...]. Ändringar i förhållande till det senaste dokumentet från arbetsgruppen 8834/18 är markerade med **understruken fetstil** och samtliga strykningar med **[...].**

III. SLUTSATS

11. Ordförandeskapets kompromisstext i bilagan återspeglar ordförandeskapets och medlemsstaternas ansträngningar att nå fram till en väl avvägd text.

12. Den 25 maj 2018 nådde Coreper en överenskommelse om ordförandeskapets kompromisstext med förbehåll för ändringar i artiklarna 19.5 och 48.5 enligt bilagan.

13. Rådet uppmanas därför att anta en allmän riktlinje vid mötet den 8 juni 2018 och ge ordförandeskapet i uppdrag att inleda förhandlingar med Europaparlamentets och Europeiska kommissionens företrädare om detta ärende.

BILAGA

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING

om Enisa, "*[...] Europeiska unionens 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[6],

med beaktande av Regionkommitténs yttrande[7],

i enlighet med det ordinarie lagstiftningsförfarandet, och

[6] EUT C,, s. .
[7] EUT C,, s. .

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, 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[8] 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[9] som förlängde byråns mandat till mars 2012. Genom förordning (EU) nr 580/2011[10] förlängdes byråns mandat ytterligare till den 13 september 2013. Europaparlamentet och rådet antog år 2013 förordning (EU) nr 526/2013[11] om Enisa och om upphävande av förordning (EG) nr 460/2004, som förlängde byråns mandat till juni 2020.

---

8 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).

9 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).

10 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).

11 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).

(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 *direktivet om nät- och informationssäkerhet*). Direktivet om nät- och informationssäkerhet 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, 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 **stödja** [...] nationella insatser och **aktivt bidra till** unionsinsatser och utföra sina uppgifter i fullt samarbete med unionens institutioner, [...] byråer **och organ** 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 **och dess sektorsspecifika aspekter för att öka relevansen av EU:s politik och lagstiftning med en cybersäkerhetsdimension och möjliggöra konsekvens i genomförandet av denna på nationell nivå** [...]. 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 direktivet om nät- och informationssäkerhet, 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, [...] byråer **och organ** i deras arbete för att bygga upp och förbättra kapacitet och beredskap för att förebygga, upptäcka och reagera på cyber**hot**[...] och cyberincidenter 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. **Den verksamhet som bedrivs av Enisa avseende medlemsstaternas operativa kapacitet bör enbart utgöra ett komplement till medlemsstaternas egna åtgärder för att fullgöra sina skyldigheter enligt direktivet om nät- och informationssäkerhet och bör därför inte ersätta dem** [...].

(15a) Byrån bör också bistå med utveckling och uppdatering av unionens och på begäran 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 direktivet om nät- och informationssäkerhet 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 samt inom den privata sektorn, [...] **bör byrån** stödja **informationsutbyte inom och mellan sektorer, i synnerhet de sektorer som förtecknas i bilaga II till direktiv (EU) 2016/1148, genom att tillhandahålla bästa praxis och vägledning i fråga om tillgängliga verktyg och förfaranden samt om hur regleringsfrågor som rör informationsutbyte ska hanteras, exempelvis genom att underlätta** [...] inrättandet av sektorsvisa centrum för informationsutbyte och analys (ISAC) [...].

(18) Byrån bör sammanställa och analysera nationella rapporter **som delats på frivillig grund** från CSIRT-enheter och CERT-EU **för att hjälpa medlemsstaterna** att [...] upprätta gemensamma [...] **förfaranden**, gemensamt språk och gemensam terminologi för utbyte av information. Byrån bör även engagera den privata sektorn, inom ramen för direktivet om nät- och informationssäkerhet som lade grunden för frivilligt utbyte av teknisk information på operativ nivå [...] **inom** CSIRT-nätverket.

(19) Byrån bör bidra till insatser på EU-nivå i samband med storskaliga gränsöverskridande cybersäkerhetsincidenter och -kriser. Denna uppgift bör **utföras i enlighet med mandatet enligt denna förordning och en metod som medlemsstaterna enats om inom ramen för kommissionens rekommendation om samordnade insatser vid storskaliga cybersäkerhetsincidenter och cyberkriser. Uppgiften skulle kunna** 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 [...] **regelbundna** cybersäkerhetsövningar.

(20) [...] **Till stöd för** det operativa **samarbetet** [...] bör byrån använda tillgänglig **teknisk och operativ** expertis från CERT-EU genom ett strukturerat [...] samarbete. [...]Vid behov bör särskilda arrangemang mellan de båda organisationerna inrättas för att definiera det praktiska genomförandet av detta samarbete **och undvika dubbelarbete**.

(21) I överensstämmelse med sina [...] uppgifter **till stöd för det operativa samarbetet inom CSIRT-nätverket** bör byrån kunna tillhandahålla stöd till medlemsstaterna **om de begär det**, till exempel genom att ge råd **om hur de ska förbättra sin förmåga att förebygga, upptäcka och reagera på incidenter, genom att [...] underlätta den** [...] tekniska **hanteringen av incidenter som har en betydande eller avsevärd inverkan,** eller **genom** att säkerställa analyser av hot och incidenter. **De åtgärder som underlättar den tekniska hanteringen av incidenter som har en betydande eller avsevärd inverkan bör framför allt omfatta Enisas stöd för frivilligt utbyte av tekniska lösningar mellan medlemsstater eller att Enisa tar fram kombinerad teknisk information (t.ex. tekniska lösningar som medlemsstaterna delar på frivillig grund).** 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 cybersäkerhetsincidenter och cyberkriser utan onödigt dröjsmål. Sådan information bör hjälpa Enisa att [...] **stödja det operativa samarbetet** [...].

(22) Som en del av det löpande samarbetet på teknisk nivå för att stödja en gemensam situationsmedvetenhet i unionen bör byrån regelbundet **och i nära samarbete med medlemsstaterna** 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 [...] eller de gemensamma kontaktpunkterna enligt direktivet om nät- och informationssäkerhet **(båda på frivillig grund),** 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) **Byråns stöd till t**ekniska efterhands**undersökningar** av incidenter med betydande konsekvenser [...] på begäran av [...] de **berörda** medlemsstaterna bör inriktas på att förhindra framtida incidenter [...]. **De berörda medlemsstaterna bör tillhandahålla den information som behövs för att göra det möjligt för byrån att effektivt stödja den tekniska undersökningen**.

(24) [...]

(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 **som är offentligt tillgänglig eller som delats på frivillig grund** 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 [...] cybersäkerhets**incidenter**, genom att utföra analyser av hot och incidenter.

(27) För att stärka unionens resiliens bör byrån utveckla spetskompetens i fråga om **cyber**säkerhet i **infrastrukturer, särskilt inom de sektorer som anges i bilaga II i direktivet om nät- och informationssäkerhet och de som används av de leverantörer av digitala tjänster som förtecknas i bilaga III i det direktivet** [...] 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, [...] byråer **och organ**, organisera regelbundna 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), **Europeiska byrån för GNSS (GSA)** 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 bör **i sin funktion** som sekretariat åt CSIRT-nätverket [...] stödja medlemsstaternas CSIRT-enheter och CERT-EU i det operativa samarbetet med alla relevanta uppgifter för CSIRT-nätverket som fastställs i direktivet om nät- och informationssäkerhet. 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 [...] **regelbundna** 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, [...] byråer **och organ** och, i tillämpliga fall, till medlemsstaterna på deras begäran om forskningsbehoven på området [...] cybersäkerhet. **För att identifiera behov och prioriteringar för forskningen bör byrån även rådfråga berörda användargrupper.**

(37) Cybersäkerhets**hot** [...] är globala frågor. Det behövs ett tätare internationellt samarbete för att förbättra **cyber**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, [...]byråer **och organ**.

(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 omfattar genomförandet av byråns årliga arbetsprogram** och ska föreläggas styrelsen, 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 [...]**a**rbets[...]**p**rogram, 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[12]. 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[13]. 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.

---

[12] 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).

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

(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) [...]

(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 direktivet om nät- och informationssäkerhet 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 för IKT-**processer**, 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 omfattar SOG-IS [...] endast 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 ett certifikat **och en EU-försäkran om överensstämmelse** 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 [...] **europeiska** 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-processer,** IKT-produkter och IKT-tjänster. Dessa system bör genomföras och övervakas av nationella [...]myndigheter för **cybersäkerhets**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 säkerställa att **IKT-processer**, IKT-produkter och IKT-tjänster som certifierats enligt ett sådant system uppfyller de angivna kraven [...] **i syfte** att [...] **skydda** 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 **under hela livscykeln** i den mening som avses i denna förordning. Det är inte möjligt att i denna förordning i detalj fastställa cybersäkerhetskraven för alla **IKT-processer**, IKT-produkter och IKT-tjänster. **IKT-processer**, 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-processer**, 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 **om inga lämpliga standarder finns tillgängliga**.

(55a) De tekniska specifikationer som ska användas i ett europeiskt system för cybersäkerhetscertifiering bör fastställas med iakttagande av principerna i bilaga II till förordning (EU) nr 1025/2012. Vissa avvikelser från dessa principer kan dock anses nödvändiga i vederbörligen motiverade fall där dessa tekniska specifikationer ska användas i ett europeiskt system för cybersäkerhetscertifiering med hänvisning till assuransnivån hög. Skälen för dessa avvikelser måste offentliggöras.

(55b) Certifierad bedömning av överensstämmelse avser det förfarande genom vilket man utvärderar om fastställda krav för en IKT-process, IKT-produkt eller IKT-tjänst har uppfyllts. Detta förfarande utförs av en oberoende tredje part, annan än produkttillverkaren eller tjänsteleverantören. Certifikat utfärdas efter framgångsrik utvärdering av en IKT-process, IKT-produkt eller IKT-tjänst. Detta bör betraktas som en bekräftelse på att en utvärdering har genomförts på ett korrekt sätt. Beroende på assuransnivå bör det europeiska systemet för cybersäkerhet ange om certifikatet utfärdats av ett privat eller offentligt organ. Bedömning av överensstämmelse och 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.

(55c) Certifikatsanvändarnas val av lämplig certifieringsnivå och därtill knutna säkerhetskrav bör grundas på en riskanalys som avser användning av IKT-processen, IKT-produkten eller IKT-tjänsten. Assuransnivån bör därför stå i proportion till nivån på den risk som är förenad med den avsedda användningen av en IKT-process, IKT-produkt eller IKT-tjänst.

(55d) Ett europeiskt system för cybersäkerhetscertifiering skulle kunna ge tillverkaren eller leverantören av IKT-produkter och IKT-tjänster möjlighet att på eget ansvar utföra en bedömning av överensstämmelse (självbedömning av överensstämmelse). I sådana fall är det tillräckligt att tillverkaren eller leverantören själv utför alla kontroller för att säkerställa IKT-processens, IKT-produkters eller IKT-tjänsters överensstämmelse med certifieringssystemet. Denna typ av bedömning av överensstämmelse bör anses lämplig för IKT-produkter och IKT-tjänster med lägre komplexitet (exempelvis enkel utformning och tillverkningsmetod) som inte utgör en stor risk för det allmänna samhällsintresset. Dessutom bör endast IKT-produkter och IKT-tjänster som motsvarar assuransnivån grundläggande kunna bli föremål för självbedömning av överensstämmelse.

(55e) Ett europeiskt system för cybersäkerhetscertifiering kan möjliggöra både certifiering och självbedömning av överensstämmelse för IKT-produkter och IKT-tjänster. I detta fall bör systemet föreskriva tydliga och begripliga möjligheter för konsumenter och andra användare att skilja mellan produkter och tjänster som bedöms under tillverkarens eller leverantörens ansvar och produkter och tjänster som har certifierats av en tredje part.

(55f) Tillverkare eller leverantörer av IKT-produkter och IKT-tjänster som utför en självbedömning av överensstämmelse bör upprätta och underteckna en EU-försäkran om överensstämmelse som ett led i förfarandet för bedömning av överensstämmelse. EU-försäkran om överensstämmelse är ett dokument som anger att en viss IKT-produkt eller IKT-tjänst uppfyller kraven i systemet. Genom att upprätta och underteckna EU-försäkran om överensstämmelse tar tillverkaren eller leverantören på sig ansvaret för att IKT-produkten eller IKT-tjänsten uppfyller de rättsliga kraven i systemet. En kopia av EU-försäkran om överensstämmelse bör lämnas in till den nationella myndigheten för cybersäkerhetscertifiering och till Enisa.

(55g) Tillverkaren eller leverantören av IKT-produkter och IKT-tjänster bör under en period som fastställs i det särskilda europeiska systemet för cybersäkerhetscertifiering ge den behöriga nationella myndigheten för cybersäkerhetscertifiering tillgång till EU-försäkran om överensstämmelse och teknisk dokumentation av all relevant information avseende IKT-produkternas eller IKT-tjänsternas överensstämmelse med systemet. Den tekniska dokumentationen bör specificera de tillämpliga kraven och, i den mån det krävs för bedömningen, även innehålla en beskrivning av IKT-produktens eller IKT-tjänstens konstruktion, tillverkning och funktion. Den tekniska dokumentationen bör utarbetas på ett sätt som möjliggör bedömning av en IKT-produkts eller en IKT-tjänsts överensstämmelse med de relevanta kraven.

(55h) Medlemsstaterna och berörda intresseorganisationer bör ha rätt att lämna förslag till den europeiska gruppen för cybersäkerhetscertifiering om utarbetande av ett förslag till system. Berörda intresseorganisationer är organisationer som företräder branschen eller konsumenterna, inklusive företrädare för organisationer för små och medelstora företag som har ett legitimt intresse i utarbetandet av ett särskilt europeiskt system för cybersäkerhetscertifiering. Sådana förslag bör undersökas mot bakgrund av de kriterier som utarbetats av den europeiska gruppen för cybersäkerhetscertifiering på grundval av riktlinjer som utgår från principerna om insyn, öppenhet, opartiskhet, samförstånd, effektivitet, relevans och samstämmighet.

(56) Kommissionen **och gruppen** bör ges befogenhet att begära att Enisa **utan onödigt dröjsmål** förbereder förslag till system för särskilda **IKT-processer,** IKT-produkter eller IKT-tjänster. Kommissionen bör, på grundval av Enisas förslag till system, ges befogenhet att anta det europeiska systemet för cybersäkerhetscertifiering genom genomförandeakter. Med beaktande av det allmänna syfte och de säkerhetsmål som fastställs i denna förordning bör det i europeiska system för cybersäkerhetscertifiering 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-processer**, 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 **och i förekommande fall utvärderingsnivåerna.**

(56a) Assuransnivån för ett europeiskt certifieringssystem utgör förtroendegrunden för att en IKT-process, IKT-produkt eller IKT-tjänst uppfyller säkerhetskraven i ett särskilt europeiskt system för cybersäkerhetscertifiering. I syfte att säkerställa konsekvens i regelverket för certifierade IKT-processer, IKT-produkter och IKT-tjänster kan ett europeiskt system för cybersäkerhetscertifiering specificera assuransnivån för europeiska cybersäkerhetscertifikat och EU-försäkringar om överensstämmelse som utfärdats inom ramen för det systemet. Varje certifikat kan avse någon av assuransnivåerna grundläggande, betydande eller hög, medan EU-försäkran om överensstämmelse endast kan avse assuransnivån grundläggande. Assuransnivåerna avspeglar motsvarande grad av ansträngning i fråga om utvärdering [...] och betecknas med hänvisning till tekniska specifikationer, standarder och förfaranden med koppling till detta, inbegripet tekniska kontroller, som ska mildra eller förhindra cybersäkerhetsincidenter. Varje assuransnivå bör vara konsekvent inom de olika sektoriella områden där certifiering tillämpas.

(56b) Ett europeiskt system för cybersäkerhetscertifiering kan ha flera utvärderingsnivåer beroende på hur stringent och djupgående utvärderingsmetoden är, vilken bör motsvara en av assuransnivåerna och vara kopplad till en lämplig kombination av assuranskomponenter. För samtliga assuransnivåer bör IKT-produkten eller IKT-tjänsten omfatta en rad säkra funktioner som definieras i systemet, exempelvis följande: säker nyskapande konfiguration, signerad kod, säker uppdatering och mekanismer för begränsad exploatering samt fullt stack-minnesskydd. Dessa funktioner bör utarbetas och upprätthållas med säkerhetsinriktade utvecklingsstrategier och tillhörande verktyg för att säkerställa att effektiva mekanismer (både maskin- och programvara) är inbyggda på ett tillförlitligt sätt. För assuransnivån grundläggande bör utvärderingen omfatta minst följande assuranskomponenter: I utvärderingen bör det åtminstone ingå en översyn av IKT-produktens eller IKT-tjänstens tekniska dokumentation som utförs av organet för bedömning av överensstämmelse. Om certifieringen omfattar IKT-processer bör den process som använts för att utforma, utveckla och upprätthålla en IKT-produkt eller IKT-tjänst även omfattas av den tekniska översynen. I de fall där ett europeiskt system för cybersäkerhetscertifiering ger möjlighet till självbedömning av överensstämmelse bör det vara tillräckligt att tillverkaren eller leverantören har gjort en självbedömning av IKT-processens, IKT-produktens eller IKT-tjänstens överensstämmelse med certifieringssystemet. För assuransnivån betydande bör utvärderingen, utöver det som krävs för assuransnivån grundläggande, åtminstone omfatta även en kontroll av överensstämmelsen mellan IKT-produktens eller IKT-tjänstens säkerhetsfunktioner och den tekniska dokumentationen. För assuransnivån hög bör utvärderingen, utöver det som krävs för assuransnivån betydande, åtminstone omfatta även ett effektivitetstest som bedömer resistensen hos IKT-produktens eller IKT-tjänstens säkerhetsfunktioner gentemot dem som utför genomtänkta cyberangrepp med betydande kompetens och resurser.

(56c) Vid utarbetandet av ett förslag till system bör Enisa samråda med alla berörda intressenter, exempelvis de europeiska standardiseringsorganisationerna, berörda nationella myndigheter, organisationer som är grundade på avtal om ömsesidigt erkännande, såsom SOG-IS-avtalet, små och medelstora företag, konsumentorganisationer samt miljö- och arbetstagarintressenter.

(56d) Enisa bör upprätthålla en webbplats med information om och offentliggörande av europeiska system för cybersäkerhetscertifiering som bör omfatta bland annat begäran om utarbetande av ett förslag till europeiskt system för cybersäkerhetscertifiering samt den återkoppling som mottagits i den samrådsprocess som genomförs av Enisa i förberedelsefasen. Denna webbplats bör också tillhandahålla information om certifikat och EU-försäkringar om överensstämmelse som utfärdas enligt denna förordning.

(57) Användningen av europeisk cybersäkerhetscertifiering **och en EU-försäkran om överensstämmelse** bör vara frivillig, om inte annat föreskrivs i unionslagstiftning eller nationell lagstiftning **som antagits i enlighet med unionslagstiftning**. **I avsaknad av harmoniserad lagstiftning får medlemsstaterna införa nationella tekniska föreskrifter i enlighet med direktiv (EU) 2015/1535 som föreskriver obligatorisk certifiering inom ramen för ett europeiskt system för cybersäkerhetscertifiering. Medlemsstaterna kan även använda europeisk cybersäkerhetscertifiering i samband med offentlig upphandling och direktiv 2014/214/EU.**

(57a) I syfte att uppnå målen för denna förordning och undvika en fragmentering av den inre marknaden, bör 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. Medlemsstaterna bör dock inte vara förhindrade att anta eller behålla nationella certifieringssystem för att skydda den nationella säkerheten.

(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 **begränsa, tillfälligt upphäva eller** 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) [...] Medlemsstaterna [...] **bör** utse en **eller flera myndigheter** för [...] cybersäkerhetscertifiering som övervakar efterlevnaden av **skyldigheterna enligt denna förordning. Om en medlemsstat finner det lämpligt kan uppgiften även tilldelas redan befintliga myndigheter. Medlemsstaterna bör också kunna fatta beslut, efter ömsesidig överenskommelse med en annan medlemsstat, om att utse en eller flera tillsynsmyndigheter på den andra medlemsstatens territorium. Myndigheten bör särskilt övervaka och verkställa de skyldigheter som åligger en tillverkare eller en leverantör av IKT-produkter och IKT-tjänster som är etablerad på deras respektive territorier med avseende på EU-försäkran om överensstämmelse, bistå de nationella ackrediteringsorganen med övervakning och kontroll av verksamhet som bedrivs av organen för bedömning av överensstämmelse genom att förse dem med sakkunskap och relevant information, tillåta organ för bedömning av överensstämmelse att utföra sina uppgifter om de uppfyller de ytterligare krav som finns fastställda i ett system och övervaka relevant utveckling på området för cybersäkerhetscertifiering**. [...] De nationella myndigheterna för **cybersäkerhets**certifiering bör behandla klagomål som lämnas in av fysiska eller juridiska personer avseende certifikat som utfärdats av **dem eller certifikat som utfärdats av organ för bedömning av överensstämmelse avseende assuransnivå hög**, i lämplig utsträckning undersöka det ärende som klagomålet gäller och underrätta den klagande om utvecklingen och resultatet av utredningen inom rimlig tid. De bör dessutom samarbeta med andra nationella [...] myndigheter för **cybersäkerhets**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 **företrädare för** nationella [...]myndigheter för **cybersäkerhets**certifiering **eller andra berörda nationella myndigheter**. 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 **byrån om förslag till system och till** kommissionen rörande underhåll och översyn av befintliga europeiska system för cybersäkerhetscertifiering.

(60a) Gruppen bör underlätta utbytet av god praxis och expertis mellan de nationella myndigheter för cybersäkerhetscertifiering som är ansvariga för bemyndigande av organ för bedömning av överensstämmelse och utfärdande av certifikat. Gruppen bör stödja framtagandet av en mekanism för inbördes granskning i samband med utarbetandet av ett förslag till system och genomförandet av det för organ som utfärdar europeiska cybersäkerhetscertifikat för assuransnivån hög. Sådana inbördes granskningar bör särskilt bedöma huruvida de berörda organen har lämplig expertis och utför sina uppgifter på ett harmoniserat sätt. Resultaten av de inbördes granskningarna bör göras allmänt tillgängliga. Dessa organ får vidta lämpliga åtgärder för att anpassa sin praxis och expertis.

(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.

(61a) För att ytterligare underlätta handeln och erkänna att IKT-leveranskedjorna är globala får avtal om ömsesidigt erkännande av de certifikat som utfärdats genom de system som inrättats inom den europeiska ramen för cybersäkerhetscertifiering ingås av unionen i enlighet med artikel 218 i EUF-fördraget. Kommissionen får med beaktande av rådgivningen från Enisa och den europeiska gruppen för cybersäkerhetscertifiering rekommendera att relevanta förhandlingar inleds. Varje system bör föreskriva särskilda villkor för ömsesidigt erkännande med tredjeländer.

(62) [...]

(63) [...]

(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 [...] myndigheterna för **cybersäkerhets**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

1. 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, "[...]**Europeiska unionens** 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-processer,** 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.

2. **Denna förordning 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 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 kan **skada, störa eller på ett annat** negativt **sätt** 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 **eller bedömning av överensstämmelse** av informations- och kommunikationstekniska (IKT) **processer,** produkter och tjänster som omfattas av tillämpningsområdet för det systemet.

9a. *nationellt system för cybersäkerhetscertifiering*: en vittomfattande uppsättning regler, tekniska krav, standarder och förfaranden som utvecklas och antas av en nationell offentlig myndighet och som tillämpas på certifiering eller bedömning av överensstämmelse av IKT-processer, IKT-produkter och IKT-tjänster som omfattas av tillämpningsområdet för det systemet.

10. *europeiskt cybersäkerhetscertifikat*: ett dokument [...] som intygar att en viss IKT**-process,** IKT-produkt eller IKT-tjänst [...] **har utvärderats med avseende på överensstämmelse med** specifika **säkerhets**krav som fastställs i ett europeiskt system för cybersäkerhetscertifiering.

11. *IKT-produkt* [...]: en del, eller grupp av delar, i nät- och informationssystem.

11a. *IKT-tjänst*: en tjänst som helt eller huvudsakligen består i överföring, lagring, hämtning eller behandling av information via nät- och informationssystem.

11b. *IKT-process*: all verksamhet som utförs för att utforma, utveckla, tillhandahålla och upprätthålla en IKT-produkt eller IKT-tjänst.

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.

16a. *teknisk specifikation*: ett dokument där det fastställs vilka tekniska krav som ska uppfyllas av en IKT-process, IKT-produkt eller IKT-tjänst.

16b. *assuransnivå*: förtroendegrund för att en IKT-process, IKT-produkt eller IKT-tjänst uppfyller säkerhetskraven i ett särskilt europeiskt system för cybersäkerhetscertifiering och anger på vilken nivå den har utvärderats; assuransnivån mäter inte säkerheten i själva IKT-processen, IKT-produkten eller IKT-tjänsten.

AVDELNING II

Enisa – "*[...] Europeiska unionens cybersäkerhetsbyrå*"

KAPITEL I

MANDAT OCH MÅL *[...]*

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 [...] **i hela** unionen **särskilt genom att stödja medlemsstaterna och unionens institutioner, byråer och organ i arbetet med att förbättra cybersäkerheten**. **Byrån ska fungera som en referenspunkt för rådgivning och expertis i fråga om cybersäkerhet för unionens institutioner, byråer och organ.**

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.

2a. Vid utförandet av sina uppgifter ska byrån agera självständigt och ta största möjliga hänsyn till nationell expertis vid medlemsstaternas berörda myndigheter och samtidigt undvika dubbelarbete.

3. [...]

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 **unionens** politiska åtgärder som rör cybersäkerhet**, inbegripet sektorspolitik på cybersäkerhetsområdet.**

3. Byrån ska stödja kapacitetsuppbyggnad och beredskap i hela unionen genom att bistå unionens **institutioner, byråer och organ**, **liksom** medlemsstaterna och offentliga och privata intressenter i syfte att öka skyddet av deras nät- och informationssystem, utveckla **och förbättra cyberresiliens och insatskapacitet samt utveckla** färdigheter och kompetens inom området cybersäkerhet [...].

4. Byrån ska främja samarbete och samordning på unionsnivå mellan medlemsstater, unionens institutioner, byråer och organ samt berörda **privata och offentliga** intressenter [...] i frågor som rör cybersäkerhet.

5. Byrån ska **bidra till att öka** [...] cybersäkerhetskapaciteten på unionsnivå i syfte att [...] **bistå** medlemsstaterna i arbetet med att förebygga och vidta åtgärder mot cyberhot, särskilt vid gränsöverskridande incidenter.

6. Byrån ska främja användningen av certifiering, **i syfte att undvika en fragmentering av certifieringssystemen i EU. Byrån ska särskilt 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.

KAPITEL IA
UPPGIFTER

Artikel 5

[...] 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) medlemsstaternas 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 [...] säkerhets**incidenter** 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

[...] ***Kapacitetsuppbyggnad***

1. Byrån ska bistå

a) medlemsstaterna i deras ansträngningar för att förbättra förebyggandet, upptäckten och analysen av, samt kapaciteten att reagera på, cyber**hot** [...] och cyberincidenter genom att förse dem med nödvändiga kunskaper och nödvändig expertis,

b) unionens institutioner, [...] byråer **och organ**, i deras ansträngningar för att förbättra förebyggandet, upptäckten och analysen av, samt kapaciteten att reagera på, cyber**hot** [...] och cyberincidenter **särskilt** 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 [...] **följa upp** 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 **regelbundna** [...] 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, **i** [...] 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 **stödja informationsutbyte inom och mellan sektorer** [...], 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

[...] ***Operativt samarbete på unionsnivå***

1. Byrån ska stödja operativt samarbete mellan **medlemsstater, unionens institutioner, byråer och** [...] organ och mellan intressenter.

2. Byrån ska samarbeta på operativ nivå och skapa synergier med unionens institutioner, [...] byråer **och organ**, 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 **i denna egenskap** [...] underlätta informationsutbytet och samarbetet mellan nätverkets medlemmar.

4. Byrån ska **stödja** [...] det operativa samarbetet inom CSIRT-nätverket och stödja medlemsstater, **på deras begäran,** genom att

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

b) [...] **underlätta den** tekniska **hanteringen** [...] av incidenter som har en betydande eller avsevärd inverkan**, särskilt genom att stödja frivilligt utbyte av tekniska lösningar mellan medlemsstaterna**,

c) analysera sårbarheter [...] och incidenter**,**

ca) ge stöd till tekniska efterhandsundersökningar av incidenter som har en betydande eller avsevärd inverkan enligt direktiv (EU) 2016/1148.

Vid fullgörandet av dessa uppgifter ska byrån och CERT-EU samarbeta på ett strukturerat sätt för att dra nytta av synergier **och undvika dubbelarbete** [...].

5. [...]

[...]

6. Byrån ska organisera **regelbundna** [...] cybersäkerhetsövningar på unionsnivå och bistå medlemsstater och EU:s institutioner, byråer och organ med att organisera övningar på deras begäran. **Sådana övningar på unionsnivå får innehålla tekniska, operativa och strategiska element [...]. En gång vartannat år ska en omfattande övning organiseras där alla element ingår.** Byrån ska också bidra till och hjälpa till att organisera, när det är lämpligt, sektorsvisa cybersäkerhetsövningar tillsammans med berörda [...] **organisationer som får** delta även **i** [...] cybersäkerhetsövningar på unionsnivå.

7. Byrån ska**, i nära samarbete med medlemsstaterna,** 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 [...] eller de gemensamma kontaktpunkterna enligt direktivet om nät- och informationssäkerhet (**båda på frivillig grund** [...]), 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 **som delats på frivillig grund** 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) [...] **på begäran av medlemsstaterna, underlätta** den tekniska hanteringen av incidenter eller kriser, **särskilt genom** [...] **att stödja frivilligt** utbyte av tekniska lösningar mellan medlemsstaterna,

d) stödja **EU:s institutioner, byråer och organ och, på begäran, medlemsstater i den** offentliga kommunikationen om incidenter eller kriser,

e) **stödja medlemsstaterna, om de begär det, att** testa[...] samarbetsplanerna för hantering av sådana incidenter eller kriser.

Artikel 8

[...] Marknad, cybersäkerhetscertifiering och standardisering

Byrån ska

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

1. utarbeta förslag till europeiska system för cybersäkerhetscertifiering för **IKT-processer**, IKT-produkter och IKT-tjänster **i samarbete med branschen och 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 [...]myndigheter för **cybersäkerhets**certifiering och branschen,

3a. rekommendera lämpliga tekniska specifikationer för användning vid utvecklingen av de europeiska system för cybersäkerhetscertifiering som avses i artikel 47.1 b i fall där standarder inte finns tillgängliga,

3b. bidra till en tillräcklig kapacitetsuppbyggnad i samband med utvärderings- och certifieringsprocesser genom att sammanställa och offentliggöra riktlinjer samt ge stöd till medlemsstaterna på deras begäran,

b) underlätta upprättandet och tillämpningen av europeiska och internationella standarder för riskhantering och för säkerheten hos **IKT-processer,** IKT-produkter och IKT-tjänster [...],

ba) i samarbete med medlemsstater utarbeta 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

*[...]**Kunskap*** **och** ***information***[...]

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 [...] cybersäkerhets**incidenter**,

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 [...] de infrastrukturer som understödjer de sektorer som förtecknas i bilaga II till direktiv (EU) 2016/1148 **och de som används av de leverantörer av digitala tjänster som förtecknas i bilaga III i det direktivet**,

d) via en särskild portal samla, organisera och för allmänheten tillgängliggöra information om cybersäkerhet som tillhandahålls av unionens institutioner, byråer och organ **och, på frivillig grund, av medlemsstaterna samt privata och offentliga intressenter**,

e) [...]

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) [...].

Artikel 9a

Medvetandehöjande åtgärder och utbildning

Byrån ska

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

b) i samarbete med medlemsstaterna, unionens institutioner, organ, byråer och näringsliv organisera regelbundna informationskampanjer för att öka cybersäkerheten och dess synlighet i unionen,

c) bistå medlemsstaterna i deras insatser för att öka medvetenheten om cybersäkerhet och främja utbildning i cybersäkerhet,

d) stödja tätare samordning och utbyte av bästa praxis mellan medlemsstaterna när det gäller utbildning och medvetenhet om cybersäkerhet genom att göra det lättare att upprätta och underhålla ett nätverk av nationella utbildningskontaktpunkter.

Artikel 10

*[...]**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

*[...]**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) [...] **inom ramarna för relevant internationellt samarbete** underlätta utbytet av bästa praxis[...],

c) på begäran tillhandahålla kommissionen expertis**,**

ca) i samarbete med den europeiska grupp för cybersäkerhetscertifiering som inrättats enligt artikel 53 ge råd och stöd till kommissionen i frågor som rör avtal om ömsesidigt erkännande av cybersäkerhetscertifikat med tredjeländer.

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,[...]

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

da) ett nätverk för nationella kontaktpersoner, som ska utföra de uppgifter som anges i artikel 20a.

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.

ca) Övervaka genomförandet av den fleråriga och årliga programplaneringen som ingår i det samlade programdokumentet.

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. [...]

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**, inbegripet genomförandet av det årliga arbetsprogrammet,** 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.

la) Regelbundet utbyte med unionens institutioner, byråer och organ om deras cybersäkerhetsverksamhet för att säkerställa att EU:s policy utvecklas och genomförs på ett enhetligt sätt.

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. **Där så är nödvändigt för att byrån ska kunna utföra sina uppgifter på ett effektivt och ändamålsenligt sätt och grundat på en ändamålsenlig kostnads–nyttoanalys, får** den verkställande direktören besluta [...]**att inrätta ett eller flera lokala kontor i en eller flera medlemsstater**. Innan den verkställande direktören beslutar att inrätta ett lokalt kontor ska han eller hon **inhämta ett yttrande från den eller de berörda medlemsstaterna, däribland den medlemsstat där byrån har sitt säte, och** ett förhandsgodkännande från kommissionen **och** styrelsen[...]. **Om oenighet råder under samrådsprocessen mellan den verkställande direktören och de berörda medlemsstaterna ska frågan överlämnas till rådet för diskussion.** 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.[...] **Antalet anställda vid alla lokala kontor ska begränsas till ett minimum och sammanlagt inte uppgå till över 40 % av [...] personalen i den medlemsstat där byrån har sitt säte. Antalet anställda vid varje lokalt kontor ska inte uppgå till över 10 % av [...] personalen i den medlemsstat där byrån har sitt säte.**

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, **leverantörer av samhällsviktiga tjänster,** 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.

5a. Den ständiga intressentgruppen ska regelbundet informera styrelsen om sin verksamhet.

AVSNITT 4A
NÄTVERK FÖR NATIONELLA KONTAKTPERSONER

Artikel 20a

Nätverk för nationella kontaktpersoner

1. Styrelsen ska, på förslag av den verkställande direktören, inrätta ett nätverk för nationella kontaktpersoner som består av företrädare för medlemsstaterna.

2. Nätverket för nationella kontaktpersoner ska bestå av företrädare för alla medlemsstater. Varje medlemsstat ska utse en företrädare. Nätverkets möten med experter kan hållas i olika format.

3. Nätverket för nationella kontaktpersoner ska särskilt underlätta informationsutbytet mellan Enisa och medlemsstaterna. Det ska framför allt stödja Enisa i dess arbete med att informera relevanta intressenter runtom i EU om byråns verksamhet, slutsatser och rekommendationer.

4. De nationella kontaktpersonerna ska fungera som kontaktpunkter på nationell nivå för att underlätta samarbetet mellan Enisa och nationella experter inom ramen för genomförandet av Enisas arbetsprogram.

5. De nationella kontaktpersonerna ska ha ett nära samarbete med styrelseledamöterna från deras respektive länder, men själva nätverket ska inte utföra samma arbete som styrelsen eller andra EU-forum.

6. Uppgifter och förfaranden avseende nätverket för nationella kontaktpersoner ska fastställas i byråns interna verksamhetsregler och ska offentliggöras.

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[14] 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.

[14] 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).

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.

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[15] och 2015/444[16]. Dessa regler ska omfatta bestämmelser om utbyte, behandling och lagring av säkerhetsskyddsklassificerade uppgifter.

---

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

[16] 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).

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 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[17] 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.

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.

[17] 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).

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[18] 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.

[18] 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).

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.

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 **fyra**[...] 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 **fyra**[...] 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[...].

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[...].

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[19]. 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[20].

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.

---

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

[20] 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).

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.

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 [...]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 III
RAM FÖR CYBERSÄKERHETSCERTIFIERING

Artikel 43

[…]***En europeisk* ram *för cybersäkerhetscertifiering***

1. **En europeisk ram för cybersäkerhetscertifiering ska inrättas för att förbättra förutsättningarna för den inre marknadens funktion genom att höja cybersäkerhetsnivån i unionen. Genom ramen inrättas en styrning som möjliggör en harmoniserad strategi på EU-nivå för europeiska system för cybersäkerhetscertifiering i syfte att skapa en digital inre marknad för IKT-processer, IKT-produkter och IKT-tjänster.**

2. **Genom den europeiska ramen för cybersäkerhetscertifiering fastställs en mekanism för inrättandet av** [...]europeiska system för cybersäkerhetscertifiering [...]**och för att** intyga att de **IKT-processer,** IKT-produkter och IKT-tjänster som har [...]**utvärderats** i enlighet med sådan**a** system uppfyller de angivna **säkerhets**kraven[...] **i syfte att skydda** tillgängligheten, autenticiteten, integriteten och konfidentialiteten hos lagrade, överförda eller behandlade data eller de funktioner eller tjänster som tillhandahålls av eller är tillgängliga via dessa produkter, processer **och** tjänster [...]**under hela livscykeln**.

Artikel 44

Utarbetande och antagande av ett europeiskt system för cybersäkerhetscertifiering

1. Efter en begäran från kommissionen **eller den europeiska grupp för cybersäkerhetscertifiering (nedan kallad *gruppen*) som inrättats enligt artikel 53**, ska Enisa utarbeta ett förslag till ett europeiskt system för cybersäkerhetscertifiering som uppfyller kraven i artiklarna 45, 46 och 47 i denna förordning.[...]

1a. Medlemsstaterna eller berörda intresseorganisationer får lämna förslag till gruppen om utarbetande av ett förslag till ett europeiskt system för cybersäkerhetscertifiering. Gruppen ska göra en bedömning av sådana förslag utifrån kriterier som fastställs av gruppen med hjälp av riktlinjer i enlighet med artikel 53.3 ca och får begära att Enisa utarbetar 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 **genom öppna samrådsprocesser** och bedriva ett nära samarbete med gruppen. Gruppen ska ge Enisa bistånd och expertråd [...]vid utarbetandet av förslaget till system **och anta ett yttrande om förslaget till system innan det läggs fram för kommissionen**[...]. **Enisa ska säkerställa att de föreslagna systemen överensstämmer med den tillämpliga harmoniserade standard som används för ackreditering av organ för bedömning av överensstämmelse.**

3. Enisa ska **ta största möjliga hänsyn till gruppens yttrande innan byrån till kommissionen översänder** [...]det förslag till [...]system 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 55.2 för europeiska system för cybersäkerhetscertifiering av **IKT-processer,** IKT-produkter och IKT-tjänster som uppfyller kraven i artiklarna 45, 46 och 47 i denna förordning.

5. [...]

Artikel 44a

Underhåll av ett europeiskt system för cybersäkerhetscertifiering

1. Byrån ska upprätthålla en särskild webbplats med information om och offentliggörande av europeiska system för cybersäkerhetscertifiering, certifikat och EU-försäkringar om överensstämmelse som utfärdats i enlighet med artikel 47a.

2. Byrån ska, i nära samarbete med gruppen, åtminstone vart femte år se över de antagna europeiska systemen för cybersäkerhetscertifiering och därvid beakta återkopplingen från berörda intressenter. Kommissionen eller gruppen får, om det anses nödvändigt, begära att byrån inleder processen med att utarbeta ett reviderat förslag till system i enlighet med artikel 44.2 och 44.3.

Artikel 45

Säkerhetsmålen för europeiska system för cybersäkerhetscertifiering

Ett europeiskt system för cybersäkerhetscertifiering ska vara utformat [...]**för** att, i tillämpliga fall, **uppnå åtminstone** 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 **under hela processens, produktens eller tjänstens livscykel**.

b) Att skydda data som lagras, överförs eller på andra sätt behandlas, mot oavsiktlig eller otillåten förstöring eller [...]förlust, oavsiktliga eller otillåtna ändringar **eller bristande tillgänglighet under hela processens, produktens eller tjänstens livscykel**.

c) [...]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 [...]**någon haft åtkomst till, som använts eller på andra sätt behandlats,** vid vilken tidpunkt och av vem.

e) [...]Att det är möjligt att kontrollera vilka data, tjänster eller funktioner som någon haft åtkomst till, [...]som använts eller **på andra sätt behandlats**, vid vilken tidpunkt och av vem.

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

g) [...]Att **IKT-processer,** IKT-produkter och IKT-tjänster tillhandahålls med uppdaterad programvara **och maskinvara** som inte innehåller **allmänt kända** brister, och med mekanismer för säkra uppdateringar[...].

ga) Att IKT-processer, IKT-produkter och IKT-tjänster utvecklas, framställs och levereras i enlighet med de säkerhetskrav som fastställs i det specifika systemet.

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-processer**, IKT-produkter och IKT-tjänster[...]. **Assuransnivån ska stå i proportion till nivån på den risk som är förenad med den avsedda användningen av en IKT-process, IKT-produkt eller IKT-tjänst.**

2. Assuransnivåerna grundläggande, betydande och hög ska [...] **avse ett certifikat eller en EU-försäkran om överensstämmelse som utfärdats inom ramen för ett europeiskt system för cybersäkerhetscertifiering, med säkerhetskrav för varje assuransnivå, inbegripet säkerhetsfunktioner och motsvarande grad av ansträngning i fråga om utvärdering av en IKT-process, IKT-produkt eller IKT-tjänst. Certifikatet eller EU-försäkran om överensstämmelse betecknas med hänvisning till tekniska specifikationer, standarder och förfaranden med koppling till detta, inbegripet tekniska kontroller, som ska minska risken för eller förhindra cybersäkerhetsincidenter enligt följande:**

a) **Ett europeiskt cybersäkerhetscertifikat eller en EU-försäkran om överensstämmelse med** assuransnivån *grundläggande* **försäkrar att IKT-processer, IKT-produkter och IKT-tjänster uppfyller respektive säkerhetskrav, inbegripet säkerhetsfunktioner, och att de har utvärderats i en utsträckning som syftar till att minimera kända grundläggande risker för cyberincidenter och cyberattacker. Utvärderingen ska innefatta åtminstone en granskning av den tekniska dokumentationen eller, där detta inte är tillämpligt, innefatta alternativa insatser med likvärdig effekt**[...].

b) **Ett europeiskt cybersäkerhetscertifikat med** assuransnivån *betydande* **försäkrar att IKT-processer, IKT-produkter och IKT-tjänster uppfyller respektive säkerhetskrav, inbegripet säkerhetsfunktioner, och att de har utvärderats i en utsträckning som syftar till att minimera kända cyberrisker, cyberincidenter och cyberattacker som genomförs av aktörer med begränsade kunskaper och resurser. Utvärderingen ska innefatta åtminstone en granskning av att allmänt kända brister inte föreligger och testning av att IKT-processer, IKT-produkter och IKT-tjänster på ett korrekt sätt genomför nödvändiga säkerhetsfunktioner eller, där detta inte är tillämpligt, innefatta alternativa insatser med likvärdig effekt**[...].

c) **Ett europeiskt cybersäkerhetscertifikat med** assuransnivån *hög* **försäkrar att IKT-processer, IKT-produkter och IKT-tjänster uppfyller respektive säkerhetskrav, inbegripet säkerhetsfunktioner, och att de har utvärderats i en utsträckning som syftar till att minimera risken för avancerade cyberattacker som genomförs av aktörer med omfattande kunskaper och resurser. Utvärderingen ska innefatta åtminstone en granskning av att allmänt kända brister inte föreligger, testning av att IKT-processer, IKT-produkter och IKT-tjänster på ett korrekt sätt genomför nödvändiga säkerhetsfunktioner, med den senaste tekniken, och en bedömning av motståndskraften mot kunniga angripare genom penetrationsprovning, eller, där detta inte är tillämpligt, innefatta alternativa insatser med likvärdig effekt**[...]**.**

2a. Ett europeiskt system för cybersäkerhetscertifiering kan ha flera olika utvärderingsnivåer beroende på hur stringent och djupgående utvärderingsmetoden är. Var och en av utvärderingsnivåerna ska motsvara en av assuransnivåerna och definieras genom en lämplig kombination av assuranskomponenter.

Artikel 47

Komponenter i europeiska system för cybersäkerhetscertifiering

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

a) Föremålet och tillämpningsområdet för **certifieringssystemet**, inbegripet typen eller kategorierna av de **IKT-processer,** IKT-produkter och IKT-tjänster som omfattas av certifieringssystemet **samt en redogörelse för hur certifieringssystemet motsvarar de förväntade målgruppernas behov**.

b) [...]En hänvisning till [...]de internationella**, europeiska eller nationella** standarder **som följts vid utvärderingen. Om inga standarder finns tillgängliga ska hänvisning göras till** [...]tekniska specifikationer **som uppfyller kraven i bilaga II till förordning (EU) nr 1025/2012 eller, om sådana inte finns tillgängliga, till tekniska specifikationer eller andra cybersäkerhetskrav som fastställs i systemet**.

c) I tillämpliga fall, en eller flera assuransnivåer.

ca) I tillämpliga fall, särskilda eller ytterligare krav som gäller för organ för bedömning av överensstämmelse för att garantera deras tekniska kompetens att utvärdera cybersäkerhetskraven.

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

e) **I tillämpliga fall,** uppgifter som en sökande ska lämna till **eller på annat sätt göra tillgängliga** för 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) [...]Reglerna för övervakning av efterlevnaden av certifieringskraven **eller EU-försäkran om överensstämmelse**, inklusive mekanismer för att visa fortsatt överensstämmelse med de angivna cybersäkerhetskraven.

h) **I tillämpliga fall,** villkor för beviljande **och förnyelse av ett certifikat samt** bibehållande, fortsättande, utvidgning **eller** inskränkning av tillämpningsområdet för certifiering.

i) Bestämmelser om följderna om certifierade IKT-produkter och IKT-tjänster **eller sådana produkter och tjänster som varit föremål för självbedömning** inte överensstämmer med [...] kraven **i systemet**.

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

k) **I tillämpliga fall,** bestämmelser om hur organ för bedömning av överensstämmelse ska bevara sina uppgifter.

l) Identifiering av nationella **eller internationella** system för cybersäkerhetscertifiering som omfattar samma typ eller kategorier av **IKT-processer,** IKT-produkter och IKT-tjänster**, säkerhetskrav samt utvärderingskriterier och utvärderingsmetoder**.

m) Innehållet i det utfärdade certifikatet **eller EU-försäkran om överensstämmelse**.

ma) Den period under vilken tillverkaren eller leverantören av IKT-produkter och IKT-tjänster ska bevara EU-försäkran om överensstämmelse och den tekniska dokumentationen av all relevant information

mb[...]) Längsta giltighetstid för certifikat.

mc[...]) Offentlighetspolicy för beviljade, ändrade och återkallade certifikat.

md[...]) Villkor för ömsesidigt erkännande av certifieringssystem med tredjeländer.

me[...]) I tillämpliga fall, bestämmelser om en mekanism för inbördes granskning för organ som utfärdar europeiska cybersäkerhetscertifikat med assuransnivån hög enligt artikel 48.4a.

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 **eller EU-försäkran om överensstämmelse** 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 47a

Självbedömning av överensstämmelse

1. Ett europeiskt system för cybersäkerhetscertifiering kan ge tillverkaren eller leverantören av IKT-produkter och IKT-tjänster möjlighet att på eget ansvar utföra en bedömning av överensstämmelse. En sådan bedömning av överensstämmelse ska endast vara tillämplig på IKT-produkter och IKT-tjänster med låg risk som motsvarar assuransnivån grundläggande.

2. Tillverkaren eller leverantören av IKT-produkter och IKT-tjänster får utfärda en EU-försäkran om överensstämmelse med angivande av att det har visats att kraven i systemet är uppfyllda. Genom att upprätta en sådan försäkran tar tillverkaren eller leverantören av IKT-produkter och IKT-tjänster ansvar för att IKT-produkten eller IKT-tjänsten uppfyller de krav som anges i systemet.

3. Tillverkaren eller leverantören av IKT-produkter och IKT-tjänster ska under en period som fastställs i det motsvarande europeiska systemet för cybersäkerhetscertifiering ge den nationella myndighet för cybersäkerhetscertifiering som avses i artikel 50.1 tillgång till EU-försäkran om överensstämmelse och teknisk dokumentation av all relevant information avseende IKT-produkternas eller IKT-tjänsternas överensstämmelse med systemet. En kopia av EU-försäkran om överensstämmelse ska lämnas in till den nationella myndigheten för cybersäkerhetscertifiering och till Enisa.

4. Det är frivilligt att utfärda EU-försäkran om överensstämmelse om inte annat anges i unionslagstiftningen eller i medlemsstaternas lagstiftning.

5. En EU-försäkran om överensstämmelse som utfärdats i enlighet med denna artikel ska erkännas i alla medlemsstater.

Artikel 48

Cybersäkerhetscertifiering

1. **IKT-processer,** 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 anges i unionslagstiftningen **eller i medlemsstaternas lagstiftning**.

3. Ett europeiskt cybersäkerhetscertifikat i enlighet med denna artikel **som avser assuransnivå grundläggande eller betydande** 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 **cybersäkerhetscertifiering** föreskriva att ett europeiskt cybersäkerhetscertifikat som är ett resultat av det systemet kan utfärdas endast av ett offentligt organ. Ett sådant [...]organ ska vara ett av följande:

a) En nationell [...]myndighet för **cybersäkerhets**certifiering som avses i artikel 50.1.

b) Ett **offentligt** organ som är ackrediterat som organ för bedömning av överensstämmelse i enlighet med artikel 51.1[...].

c) [...].

4a. I de fall där ett europeiskt system för cybersäkerhetscertifiering enligt artikel 44 kräver assuransnivå hög kan certifikatet endast utfärdas av en nationell myndighet för cybersäkerhetscertifiering enligt artikel 50.1 eller, på följande villkor, av ett organ för bedömning av överensstämmelse enligt artikel 51:

a) Efter förhandsgodkännande av den nationella myndigheten för cybersäkerhetscertifiering för varje enskilt certifikat som utfärdats av ett organ för bedömning av överensstämmelse, eller

b) efter allmän delegering på förhand av denna uppgift till ett organ för bedömning av överensstämmelse från den nationella myndigheten för cybersäkerhetscertifiering.

5. Den fysiska eller juridiska person som lämnar in sina **IKT-processer,** IKT-produkter eller IKT-tjänster till certifieringsmekanismen ska [...]**göra** all information som krävs för att genomföra certifieringsförfarandet **tillgänglig för** det organ för bedömning av överensstämmelse som avses i artikel 51 **eller för den nationella myndighet för cybersäkerhetscertifiering som avses i artikel 50**, **om denna myndighet är det organ som utfärdar certifikatet**.

5a. Innehavaren av ett certifikat ska informera det organ som utfärdar certifikatet om alla sårbarheter eller oegentligheter som upptäckts senare och som rör säkerheten för den certifierade IKT-processen, IKT-produkten eller IKT-tjänsten som kan påverka de krav som sammanhänger med certifieringen. Organet ska utan onödigt dröjsmål vidarebefordra denna information till den nationella myndigheten för cybersäkerhetscertifiering.

6. Certifikat ska utfärdas för [...]**den period som fastställs i det enskilda certifieringssystemet** och får förnyas [...]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-processer,** 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. **N**ationella system för cybersäkerhetscertifiering och därtill hörande förfaranden för **IKT-processer,** 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-processer,** IKT-produkter och IKT-tjänster som omfattas av ett befintligt europeiskt system för cybersäkerhetscertifiering.

3. Befintliga certifikat som utfärdats enligt nationella system för cybersäkerhetscertifiering **och som omfattas av ett europeiskt system för cybersäkerhetscertifiering** ska förbli giltiga tills de löper ut.

Artikel 50

Nationella [...]myndigheter för* cybersäkerhets*certifiering

1. Varje medlemsstat ska **utse en** [...]**eller flera** nationella **myndigheter för cybersäkerhets**certifiering **på sitt territorium eller, efter ömsesidig överenskommelse med en annan medlemsstat, utse en eller flera myndigheter som är etablerade i denna andra medlemsstat som ansvariga för tillsynsuppgifterna i den utseende medlemsstaten**.

2. Varje medlemsstat ska underrätta kommissionen om **vilka myndigheter som utsetts [...]och om vilka uppgifter som de tilldelats**.

3. **Utan att det påverkar tillämpningen av artikel 48.4 a och 48.4a ska** [...]varje nationell [...]myndighet för **cybersäkerhets**certifiering, vad gäller dess organisation, beslut om finansiering, rättsliga struktur och beslutsfattande vara oberoende av de enheter som den utövar tillsyn över.

3a. Medlemsstaterna ska säkerställa att den verksamhet som bedrivs av den nationella myndigheten för cybersäkerhetscertifiering i samband med utfärdande av certifikat i enlighet med artikel 48.4 a och 48.4a följer en strikt fördelning av uppgifter och ansvarsområden i förhållande till tillsynsverksamheten enligt denna artikel och att båda verksamheterna utförs oberoende av varandra.

4. Medlemsstaterna ska säkerställa att de nationella [...]myndigheterna för **cybersäkerhets**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 [...]myndigheter för **cybersäkerhets**certifiering ska

a) [...]

aa) övervaka och verkställa de skyldigheter som åligger en tillverkare eller en leverantör av IKT-produkter och IKT-tjänster som är etablerad på deras respektive territorier enligt artikel 47a.2 och 47a.3 och enligt motsvarande europeiskt system för cybersäkerhetscertifiering,

b) [...]**utan att det påverkar tillämpningen av artikel 51.1b bistå de nationella ackrediteringsorganen med övervakning och kontroll** av verksamhet som bedrivs av organen för bedömning av överensstämmelse i enlighet med denna förordning,

ba) övervaka och kontrollera den verksamhet som bedrivs av de organ som avses i artikel 48.4,

bb) utfärda bemyndiganden för organ för bedömning av överensstämmelse som avses i artikel 51.1b och begränsa, tillfälligt upphäva eller återkalla befintliga bemyndiganden om kraven i denna förordning inte uppfylls,

c) behandla klagomål som lämnas in av fysiska eller juridiska personer avseende certifikat som utfärdats av [...]**den nationella myndigheten för cybersäkerhetscertifiering eller, i enlighet med artikel 48.4a, av organ för bedömning av överensstämmelse**, 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 [...]myndigheter för **cybersäkerhets**certifiering eller andra myndigheter, bland annat genom att utbyta information om **IKT-processer,** 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 [...]myndighet för **cybersäkerhets**certifiering ska minst ha följande befogenheter:

a) Kunna begära att organ för bedömning av överensstämmelse, [...]innehavare av ett europeiskt cybersäkerhetscertifikat **och utfärdare en av EU-försäkran om överensstämmelse** 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**,** [...]innehavare av ett europeiskt cybersäkerhetscertifikat **och utfärdare av en EU-försäkran om överensstämmelse**, för att kunna verifiera överensstämmelse med bestämmelserna i avdelning III.

c) Få vidta lämpliga åtgärder, i enlighet med nationell lagstiftning, för att säkerställa att organ för bedömning av överensstämmelse, [...]innehavare av certifikat **och utfärdare av en EU-försäkran om överensstämmelse** uppfyller kraven i denna förordning eller 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 utfärdats av den nationella myndigheten för cybersäkerhetscertifiering eller, i enlighet med artikel 48.4a, av organ för bedömning av överensstämmelse** 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 [...]myndigheter för **cybersäkerhets**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-processer,** 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.

1a. I fall där ett europeiskt cybersäkerhetscertifikat utfärdas av en nationell myndighet för cybersäkerhetscertifiering enligt artikel 48.4 a och 48.4a ska certifieringsorganet hos den nationella myndigheten för cybersäkerhetscertifiering ackrediteras som organ för bedömning av överensstämmelse enligt punkt 1 i denna artikel.

1b. I tillämpliga fall ska organen för bedömning av överensstämmelse bli bemyndigade av den nationella myndigheten för cybersäkerhetscertifiering att utföra sina uppgifter när de uppfyller särskilda eller ytterligare krav som fastställs i det europeiska systemet för certifiering enligt artikel 47.1 ca.

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 **vidta alla lämpliga åtgärder inom en rimlig tidsram för att begränsa, tillfälligt upphäva eller** 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 [...]myndigheter för **cybersäkerhets**certifiering till kommissionen anmäla de [...]organ för bedömning av överensstämmelse som är ackrediterade **och, i tillämpliga fall, bemyndigade enligt artikel 51.1b** 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 unionens 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 [...]myndighet för **cybersäkerhets**certifiering får lämna in en begäran till kommissionen om att stryka ett organ för bedömning av överensstämmelse, som anmälts av den medlemsstaten, 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 [...]myndigheten för **cybersäkerhets**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 **företrädare för** nationella [...]myndigheter för **cybersäkerhets**certifiering **eller företrädare för andra berörda nationella myndigheter**. [...] **Varje gruppmedlem får företräda endast en annan medlemsstat**.

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,

ba) anta ett yttrande om förslaget till system enligt artikel 44 i denna förordning,

c) [...]**uppmana** byrån att utarbeta ett förslag till ett europeiskt system för cybersäkerhetscertifiering i enlighet med artikel 44 i denna förordning,

ca) utarbeta och anta riktlinjer om kriterier för bedömning av förslag om utarbetande av förslag till system som överlämnas till [...]gruppen i enlighet med artikel 44.1a,

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 [...]myndigheter för **cybersäkerhets**certifiering enligt denna avdelning genom **kapacitetsuppbyggnad**, utbyte av information, särskilt genom att fastställa metoder för ett effektivt informationsutbyte om alla frågor som rör cybersäkerhetscertifiering,

fa) tillhandahålla stöd för genomförandet av mekanismen för inbördes granskning i enlighet med de regler som fastställts i ett europeiskt system för cybersäkerhetscertifiering enligt artikel 47.1 md i denna förordning.

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

Artikel 53a

Rätten att lämna in ett klagomål hos den nationella [...]myndigheten för* cybersäkerhets*certifiering

1. Fysiska och juridiska personer ska ha rätt att lämna in ett klagomål hos den nationella myndigheten för cybersäkerhetscertifiering rörande ett certifikat som utfärdats av denna myndighet eller, i enlighet med artikel 48.4a, av organ för bedömning av överensstämmelse.

2. Den nationella myndighet för cybersäkerhetscertifiering till vilken klagomålet har ingetts ska underrätta den klagande om hur arbetet med klagomålet fortskrider och vad resultatet blir, inbegripet möjligheten till rättslig prövning enligt artikel 53b.

Artikel 53b

Rätten till ett effektivt rättsmedel

1. Fysiska och juridiska personer ska ha rätt till ett effektivt rättsmedel mot ett rättsligt bindande beslut från en nationell myndighet för cybersäkerhetscertifiering som berör dem.

2. Fysiska och juridiska personer ska ha rätt till ett effektivt rättsmedel om den nationella myndigheten för cybersäkerhetscertifiering inte hanterar ett klagomål.

3. Talan mot en nationell myndighet för cybersäkerhetscertifiering ska väckas vid domstol i den medlemsstat där myndigheten är etablerad.

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 5**.4 b** i förordning (EU) nr 182/2011 tillämpas.

Artikel 56

Utvärdering och granskning

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

Ikraftträdande

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

1a. Denna förordning ska tillämpas från och med […] med undantag för artiklarna 50, 51, 52, 53a, 53b och 54 som ska tillämpas från och med [24 månader 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*

BILAGA

KRAV SOM ORGANEN FÖR BEDÖMNING AV ÖVERENSSTÄMMELSE SKA UPPFYLLA

De organ för bedömning av överensstämmelse som önskar bli ackrediterade ska uppfylla följande krav:

1. Ett organ för bedömning av överensstämmelse ska inrättas i enlighet med nationell lag och vara en juridisk person.

2. Ett organ för bedömning av överensstämmelse ska vara ett tredjepartsorgan som är oberoende av den organisation eller de IKT-produkter eller IKT-tjänster som den bedömer.

3. Detta organ får vara ett organ som hör till en näringslivsorganisation eller branschorganisation som företräder företag som är involverade i konstruktion, tillverkning, leverans, installation, användning eller underhåll av de IKT-produkter eller IKT-tjänster som det bedömer, förutsatt att det kan styrkas att organet för bedömning av överensstämmelse är oberoende och att det saknas intressekonflikter.

4. Ett organ för bedömning av överensstämmelse, dess högsta ledning och den personal som ansvarar för att bedömningen av överensstämmelse görs, får inte utgöras av den som utformar, tillverkar, levererar, installerar, köper, äger, använder eller underhåller den IKT-produkt eller IKT-tjänst som bedöms och inte heller av den som företräder någon av dessa parter. Detta ska inte hindra att bedömda produkter som är nödvändiga för verksamheten inom organet för bedömning av överensstämmelse används eller att produkterna används för personligt bruk.

5. Ett behörigt bedömningsorgan, dess högsta ledning och den personal som ansvarar för genomförandet av bedömningen av överensstämmelse får varken delta direkt i konstruktionen, tillverkningen, marknadsföringen, installationen, användningen eller underhållet av dessa IKT-produkter eller IKT-tjänster, eller företräda de parter som bedriver denna verksamhet. De får inte delta i någon verksamhet som kan påverka deras objektivitet eller integritet i samband med den bedömning av överensstämmelse som anmälan avser. Detta ska framför allt gälla konsulttjänster.

6. Organ för bedömning av överensstämmelse ska se till att deras dotterbolags eller underentreprenörers verksamhet inte påverkar sekretessen, objektiviteten eller opartiskheten i organens bedömningar av överensstämmelse.

7. Organ för bedömning av överensstämmelse och deras personal ska utföra bedömningen av överensstämmelse med största möjliga yrkesintegritet, ha erforderlig teknisk kompetens på det specifika området och vara fria från alla påtryckningar och incitament, inklusive av ekonomisk natur, som kan påverka deras omdöme eller resultaten av deras bedömning av överensstämmelse, särskilt när det gäller personer eller grupper av personer som berörs av denna verksamhet.

8. Ett behörigt bedömningsorgan ska vara i stånd att utföra alla de uppgifter för bedömning av överensstämmelse som det utsetts att utföra enligt denna förordning, oavsett om uppgifterna utförs av organet för bedömning av överensstämmelse självt eller av annan part för dess räkning och på dess ansvar.

9. Vid alla tidpunkter och vid varje bedömning av överensstämmelse och för varje typ, kategori eller underkategori av IKT-produkter eller IKT-tjänster, ska ett organ för bedömning av överensstämmelse ha till sitt förfogande

a) personal med teknisk kunskap och tillräcklig och lämplig erfarenhet för att utföra de uppgifter som ingår i bedömningen av överensstämmelse,

b) erforderliga beskrivningar av förfarandena i enlighet med vilka bedömningar av överensstämmelse utförs, som säkerställer insyn i dessa förfaranden och möjlighet att reproducera dem. Det ska förfoga över lämpliga riktlinjer och förfaranden för att skilja mellan de uppgifter som det utför i sin egenskap av anmält organ och all annan verksamhet.

c) förfaranden som gör det möjligt för organet att utöva sin verksamhet med vederbörlig hänsyn tagen till ett företags storlek, bransch och struktur, den berörda IKT-produktteknikens eller IKT-tjänsteteknikens komplexitet och om det rör sig om massproduktion eller serietillverkning.

10. Ett organ för bedömning av överensstämmelse ska ha de nödvändiga medlen för att korrekt kunna utföra de tekniska och administrativa uppgifterna i samband med bedömningen av överensstämmelse och ska ha tillgång till den utrustning och de hjälpmedel som är nödvändiga.

11. Den personal som ansvarar för att utföra bedömningen av överensstämmelse ska ha

a) en grundlig teknisk utbildning och yrkesutbildning som omfattar all verksamhet i samband med bedömning av överensstämmelse,

b) tillfredsställande kunskap om kraven för de bedömningar som de gör och fullgod befogenhet att utföra dessa bedömningar,

c) lämpliga kunskaper och förståelse om de tillämpliga kraven och provningsstandarderna,

d) förmåga att upprätta intyg, protokoll och rapporter som visar att bedömningarna har utförts.

12. Det ska garanteras att organ för bedömning av överensstämmelse, deras högsta ledning och bedömningspersonal är opartiska.

13. Ersättningen till den högsta ledningen för och av bedömningspersonalen vid ett organ för bedömning av överensstämmelse får inte vara beroende av antalet bedömningar som görs eller resultaten av bedömningarna.

14. Organ för bedömning av överensstämmelse ska vara ansvarsförsäkrade, såvida inte ansvaret åligger staten enligt nationell lag i punkt 1 eller medlemsstaten själv tar direkt ansvar för bedömningen av överensstämmelse.

15. Personalen vid ett organ för bedömning av överensstämmelse ska iaktta tystnadsplikt beträffande all information som de erhåller vid utförandet av sina uppgifter i enlighet med denna förordning eller de nationella bestämmelser som genomför den, utom gentemot de behöriga myndigheterna i de medlemsstater där verksamheten utförs.

16. Organen för bedömning av överensstämmelse ska uppfylla de krav som anges i **relevant** standard **som harmoniserats enligt förordning (EG) 765/2008 för ackreditering av organ för bedömning av överensstämmelse som utför certifiering av en process, produkt eller tjänst**[...].

17. Organen för bedömning av överensstämmelse ska säkerställa att de provningslaboratorier som används för att prova överensstämmelsen uppfyller de krav som anges i **relevant** standard **som harmoniserats enligt förordning (EG) 765/2008 för ackreditering av laboratorier som utför provningar**[...].