EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2019/881 2024/EØS/63/38

av 17. april 2019

om ENISA (Den europeiske unions cybersikkerhetsbyrå), om cybersikkerhetssertifisering av informasjons- og kommunikasjonsteknologi og om oppheving av forordning (EU) nr. 526/2013 (cybersikkerhetsforordningen)(*)

EUROPAPARLAMENTET OG RÅDET FOR DEN EUROPEISKE UNION HAR

under henvisning til traktaten om Den europeiske unions virkemåte, særlig artikkel 114,

under henvisning til forslag fra Europakommisjonen,

etter oversending av utkast til regelverksakt til de nasjonale parlamentene,

under henvisning til uttalelse fra Den europeiske økonomiske og sosiale komité([1]),

under henvisning til uttalelse fra Regionkomiteen([2]),

etter den ordinære regelverksprosedyren([3]) og

ut fra følgende betraktninger:

1) Nett- og informasjonssystemer og elektroniske kommunikasjonsnett og -tjenester spiller en viktig rolle i samfunnet og utgjør nå ryggraden for økonomisk vekst. Informasjons- og kommunikasjonsteknologi (IKT) danner grunnlaget for de komplekse systemene som støtter samfunnsaktiviteter i hverdagen, holder økonomien i gang i viktige sektorer som helse, energi, finans og transport, og framfor alt bidrar til et velfungerende indre marked.

2) Bruken av nett- og informasjonssystemer blant borgere, organisasjoner og foretak er nå svært omfattende i hele Unionen. Digitalisering og tilkoplingsmuligheter er i ferd med å bli sentrale elementer i et stadig økende antall produkter og tjenester, og med framkomsten av tingenes internett (IoT) forventes det at det vil bli tatt i bruk et ekstremt høyt antall tilkoplede digitale enheter i hele Unionen i det neste tiåret. Selv om et økende antall enheter er koplet til internett, er det ikke tatt tilstrekkelig hensyn til sikkerhet og robusthet i utformingen av dem, noe som gir utilstrekkelig cybersikkerhet. Den begrensede bruken av sertifisering fører i denne sammenhengen til at privatpersoner, organisasjoner og foretak ikke har tilstrekkelig informasjon om cybersikkerhetsfunksjonene til IKT-produkter, IKT-tjenester og IKT-prosesser, noe som undergraver tilliten til digitale løsninger. Nett- og informasjonssystemer kan støtte alle aspekter av våre liv og bli en drivkraft for økonomisk vekst i Unionen. De utgjør grunnlaget for å virkeliggjøre et digitalt indre marked.

3) Økt digitalisering og tilkoplingsmuligheter fører til økt cybersikkerhetsrisiko, og gjør dermed samfunnet som helhet mer sårbart for cybertrusler og øker farene for enkeltpersoner, særlig for sårbare personer som barn. For å redusere disse risikoene må alle nødvendige tiltak treffes for å forbedre cybersikkerheten i Unionen, slik at nett- og informasjonssystemer, kommunikasjonsnett, digitale produkter, tjenester og enheter som brukes av borgere, organisasjoner og foretak – alt fra små og mellomstore bedrifter (SMB), som definert i kommisjonsrekommandasjon 2003/361/EF([4]), til operatører av kritisk infrastruktur – er bedre beskyttet mot cybertrusler.

(*) Denne unionsrettsakten, kunngjort i EUT L 151 av 7.6.2019, s. 15, er omhandlet i EØS-komiteens beslutning nr. 22/2023 av 3. februar 2023 om endring av EØS-avtalens vedlegg XI (Elektronisk kommunikasjon, audiovisuelle tjenester og informasjonssamfunnstjenester) og protokoll 37 om listen omhandlet i artikkel 101, se EØS-tillegget til *Den europeiske unions tidende* nr. 75 av 19.10.2023, s. 34.

([1]) EUT C 227 av 28.6.2018, s. 86.

([2]) EUT C 176 av 23.5.2018, s. 29.

([3]) Europaparlamentets holdning av 12. mars 2019 (ennå ikke offentliggjort i EUT) og rådsbeslutning av 9. april 2019.

([4]) Kommisjonsrekommandasjon av 6. mai 2003 om definisjonen av svært små, små og mellomstore bedrifter (EUT L 124 av 20.5.2003, s. 36).

4) Ved å gjøre relevant informasjon tilgjengelig for offentligheten bidrar Den europeiske unions byrå for nett- og informasjonssikkerhet (ENISA), opprettet ved europaparlaments- og rådsforordning (EU) nr. 526/2013([5]), til utviklingen av cybersikkerhetsbransjen i Unionen, særlig SMB-er og nyetablerte foretak. ENISA bør etterstrebe et tettere samarbeid med universiteter og forskningsenheter for å bidra til å redusere avhengigheten av cybersikkerhetsprodukter og -tjenester fra land utenfor Unionen, og for å styrke forsyningskjedene i Unionen.

5) Mengden av cyberangrep er økende, og tilkoplede økonomier og samfunn som er mer sårbare for cybertrusler og -angrep, krever sterkere vern. Selv om cyberangrep ofte skjer på tvers av landegrenser, er cybersikkerhetsmyndighetenes og de rettshåndhevende myndighetenes kompetanse og politiske respons i hovedsak nasjonal. Omfattende hendelser kan forstyrre ytingen av samfunnsviktige tjenester i hele Unionen. Dette krever effektiv og samordnet innsats og krisehåndtering på unionsplan, som bygger på målrettet politikk og utvidede instrumenter for europeisk solidaritet og gjensidig bistand. Det er dessuten viktig for beslutningstakere, bransjen og brukere at det foretas regelmessige vurderinger av situasjonen for cybersikkerhet og cyberrobusthet i Unionen, basert på pålitelige unionsdata samt systematiske prognoser for utviklingen og framtidige utfordringer og trusler, både på unionsplan og globalt plan.

6) I lys av de økende cybersikkerhetsutfordringene som Unionen står overfor, er det behov for et omfattende sett av tiltak som bygger videre på tidligere EU-tiltak og fremmer gjensidig forsterkende mål. Disse målene omfatter å øke medlemsstatenes og foretakenes kapasitet og beredskap ytterligere, samt forbedre samarbeidet, informasjonsutvekslingen og samordningen på tvers av medlemsstatene og Unionens institusjoner, organer, kontorer og byråer. Ettersom cybertruslene ikke stopper ved grensen, er det dessuten behov for å øke kapasiteten på unionsplan som kan utfylle medlemsstatenes tiltak, særlig ved omfattende grensekryssende hendelser og kriser, samtidig som det tas hensyn til viktigheten av å opprettholde og ytterligere styrke den nasjonale kapasiteten til å reagere på cybertrusler av alle slag.

7) Det er også behov for ytterligere innsats for å øke borgernes, organisasjonenes og foretakenes bevissthet om cybersikkerhetsspørsmål. Ettersom hendelser undergraver tilliten til tilbydere av digitale tjenester og til selve det digitale indre markedet, særlig blant forbrukere, bør tilliten styrkes ytterligere ved å tilby informasjon på en gjennomsiktig måte om sikkerhetsnivået for IKT-produkter, IKT-tjenester og IKT-prosesser, samtidig som det understrekes at selv ikke et høyt nivå av cybersikkerhetssertifisering kan garantere at IKT-produkter, IKT-tjenester eller IKT-prosesser er helt sikre. Styrket tillit kan fremmes gjennom unionsomfattende sertifisering som fastsetter felles cybersikkerhetskrav og -vurderingskriterier på tvers av nasjonale markeder og sektorer.

8) Cybersikkerhet er ikke bare et spørsmål knyttet til teknologi, men et spørsmål hvor menneskelig atferd er like viktig. Derfor bør det i sterk grad oppfordres til «cyberhygiene», det vil si enkle, rutinemessige tiltak som når de gjennomføres og iverksettes regelmessig av borgere, organisasjoner og foretak, minimerer deres eksponering for risikoer fra cybertrusler.

9) For å styrke Unionens cybersikkerhetsstrukturer er det viktig å opprettholde og utvikle medlemsstatenes kapasitet til å reagere på cybertrusler, også på grensekryssende hendelser, på en helhetlig måte.

10) Foretak og de enkelte forbrukere bør få nøyaktig informasjon om på hvilket tillitsnivå deres IKT-produkter, IKT-tjenester og IKT-prosesser er blitt sertifisert. Samtidig er det ingen IKT-produkter eller IKT-tjenester som er helt cybersikre, og det er nødvendig å fremme og prioritere grunnleggende regler for cyberhygiene. Med tanke på den økende tilgjengeligheten av IoT-utstyr er det en rekke frivillige tiltak som den private sektoren kan iverksette for å styrke tilliten til IKT-produkters, IKT-tjenesters og IKT-prosessers sikkerhet.

11) Moderne IKT-produkter og IKT-systemer omfatter ofte, og er avhengige av, én eller flere teknologier og komponenter fra tredjeparter, for eksempel programvaremoduler, biblioteker eller programgrensesnitt. Denne «avhengigheten» kan innebære ytterligere cybersikkerhetsrisiko, ettersom sårbarheter som finnes i tredjepartskomponenter, også kan påvirke sikkerheten til IKT-produkter, IKT-tjenester og IKT-prosesser. I mange tilfeller gjør identifisering og dokumentasjon av slike avhengigheter det mulig for sluttbrukere av IKT-produkter, IKT-tjenester og IKT-prosesser å forbedre sin håndtering av cybersikkerhetsrisiko, for eksempel ved å forbedre prosedyrene for håndtering og utbedring av sårbarheter knyttet til cybersikkerhet.

([5]) Europaparlaments- og rådsforordning (EU) nr. 526/2013 av 21. mai 2013 om Den europeiske unions byrå for nett- og informasjonssikkerhet (ENISA) og om oppheving av forordning (EF) nr. 460/2004 (EUT L 165 av 18.6.2013, s. 41).

12) Organisasjoner, produsenter eller leverandører som er involvert i utformingen og utviklingen av IKT-produkter, IKT-tjenester eller IKT-prosesser, bør oppfordres til å iverksette tiltak på et så tidlig stadium som mulig i utformingen og utviklingen for å ivareta sikkerheten for disse produktene, tjenestene og prosessene i størst mulig grad, på en slik måte at det forutsettes at cyberangrep vil skje og at konsekvensene av dem forutses og minimeres («innebygd sikkerhet»). Sikkerheten bør ivaretas i hele IKT-produktets, IKT-tjenestens eller IKT-prosessens levetid ved at det skjer en løpende utvikling av utformings- og utviklingsprosessene for å begrense skadevirkningene av ondsinnet utnytting.

13) Foretak, organisasjoner og den offentlige sektoren bør konfigurere de IKT-produktene, IKT-tjenestene eller IKT-prosessene som de utformer, på en måte som sikrer et høyere sikkerhetsnivå, som bør gi den første brukeren mulighet til å få en standardkonfigurasjon med så sikre innstillinger som mulig («sikkerhet som standard»), og dermed redusere den byrden det er for brukere å være nødt til å konfigurere et IKT-produkt, en IKT-tjeneste eller en IKT-prosess på en hensiktsmessig måte. Sikkerhet som standard bør ikke kreve omfattende konfigurering eller spesifikk teknisk forståelse eller handling som ikke er intuitiv fra brukerens side, og bør fungere enkelt og pålitelig når den brukes. Dersom en risiko- og brukervennlighetsanalyse i bestemte tilfeller fører til den konklusjonen at en slik standardinnstilling ikke er mulig, bør brukerne bli bedt om å velge den sikreste innstillingen.

14) Europaparlaments- og rådsforordning (EF) nr. 460/2004([6]) opprettet ENISA for å bidra til målene om å sikre et høyt og effektivt nivå for nett- og informasjonssikkerhet i Unionen og utvikle en nett- og informasjonssikkerhetskultur til fordel for borgere, forbrukere, foretak og offentlige forvaltninger. Europaparlaments- og rådsforordning (EF) nr. 1007/2008([7]) forlenget ENISAs mandatperiode fram til mars 2012. Europaparlaments- og rådsforordning (EU) nr. 580/2011([8]) forlenget ENISAs mandatperiode ytterligere fram til 13. september 2013. Forordning (EU) nr. 526/2013 forlenget ENISAs mandatperiode fram til 19. juni 2020.

15) Unionen har allerede truffet viktige tiltak for å sikre cybersikkerheten og øke tilliten til digital teknologi. I 2013 ble Den europeiske unions cybersikkerhetsstrategi vedtatt for å tjene som veiledning for Unionens politiske reaksjon på cybertrusler og -risikoer. For å beskytte borgerne bedre på nettet ble Unionens første rettsakt på cybersikkerhetsområdet vedtatt i 2016 i form av europaparlaments- og rådsdirektiv (EU) 2016/1148([9]). Direktiv (EU) 2016/1148 innførte krav til nasjonal kapasitet på cybersikkerhetsområdet, opprettet de første ordningene for å styrke det strategiske og driftsmessige samarbeidet mellom medlemsstatene og innførte forpliktelser med hensyn til sikkerhetstiltak og meldinger om hendelser i sektorer som er svært viktige for økonomien og samfunnet, som energi, transport, drikkevannsforsyning og -distribusjon, bankvirksomhet, finansmarkedsinfrastruktur, helsetjenester, digital infrastruktur samt tilbydere av viktige digitale tjenester (søkemotorer, skytjenester og nettbaserte markedsplasser).

ENISA fikk tildelt en viktig rolle for å støtte gjennomføringen av det nevnte direktivet. Dessuten er det å bekjempe datakriminalitet på en effektiv måte høyt prioritert i den europeiske sikkerhetsagendaen, og bidrar til det overordnede målet om å oppnå et høyt nivå av cybersikkerhet. Andre rettsakter, som europaparlaments- og rådsforordning (EU) 2016/679([10]) og europaparlaments- og rådsdirektiv 2002/58/EF([11]) og (EU) 2018/1972([12]), bidrar også til et høyt nivå av cybersikkerhet i det digitale indre markedet.

([6]) Europaparlaments- og rådsforordning (EF) nr. 460/2004 av 10. mars 2004 om opprettelse av Det europeiske byrå for nett- og informasjonssikkerhet (EUT L 77 av 13.3.2004, s. 1).

([7]) Europaparlaments- og rådsforordning (EF) nr. 1007/2008 av 24. september 2008 om endring av forordning (EF) nr. 460/2004 om opprettelse av Det europeiske byrå for nett- og informasjonssikkerhet med hensyn til varigheten av Byrået mandat (EUT L 293 av 31.10.2008, s. 1).

([8]) Europaparlaments- og rådsforordning (EF) nr. 580/2011 av 8. juni 2011 om endring av forordning (EF) nr. 460/2004 om opprettelse av Det europeiske byrå for nett- og informasjonssikkerhet med hensyn til byråets mandatperiode (EUT L 165 av 24.6.2011, s. 3).

([9]) Europaparlaments- og rådsdirektiv (EU) 2016/1148 av 6. juli 2016 om tiltak for å sikre et høyt felles nivå for sikkerhet i nett- og informasjonssystemer i hele Unionen (EUT L 194 av 19.7.2016, s. 1).

([10]) Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) (EUT L 119 av 4.5.2016, s. 1).

([11]) Europaparlaments- og rådsdirektiv 2002/58/EF av 12. juli 2002 om behandling av personopplysninger og personvern i sektoren for elektronisk kommunikasjon (direktivet om personvern og elektronisk kommunikasjon) (EFT L 201 av 31.7.2002, s. 37).

([12]) Europaparlaments- og rådsdirektiv (EU) 2018/1972 av 11. desember 2018 om fastsettelse av en europeisk kodeks for elektronisk kommunikasjon (EUT L 321 av 17.12.2018, s. 36).

16) Siden vedtakelsen av Den europeiske unions cybersikkerhetsstrategi i 2013 og den siste revisjonen av ENISAs mandat, har den overordnede politiske rammen endret seg vesentlig ettersom det globale miljøet har blitt mer uforutsigbart og mindre sikkert. På bakgrunn av dette og i forbindelse med den positive utviklingen av ENISAs rolle som et referansepunkt for rådgivning og ekspertise, som en tilrettelegger for samarbeid og kapasitetsoppbygging samt innenfor rammen av Unionens nye cybersikkerhetspolitikk, er det nødvendig å gjennomgå ENISAs mandat for å fastslå dets rolle i det endrede cybersikkerhetsøkosystemet og sikre at ENISA bidrar effektivt til Unionens reaksjon på cybersikkerhets-utfordringer som stammer fra det radikalt endrede trusselbildet på cyberområdet, noe det nåværende mandatet ikke er tilstrekkelig for, slik det også framkom ved vurderingen av ENISA.

17) ENISA som opprettet ved denne forordningen bør erstatte ENISA som opprettet ved forordning (EF) nr. 526/2013. ENISA bør utføre de oppgavene det er pålagt ved denne forordningen og andre unionsrettsakter på cybersikkerhets-området, blant annet ved å bidra med rådgivning og ekspertise og fungere som et senter for informasjon og kunnskap i Unionen. Det bør fremme utveksling av beste praksis mellom medlemsstatene og berørte parter i privat sektor, foreslå politiske tiltak for Kommisjonen og medlemsstatene, fungere som et referansepunkt for Unionens sektorpolitiske initiativer med hensyn til cybersikkerhetsspørsmål og fremme driftsmessig samarbeid, både mellom medlemsstatene og mellom medlemsstatene og Unionens institusjoner, organer, kontorer og byråer.

18) Innenfor rammen av beslutning 2004/97/EF, Euratom, truffet ved felles overenskomst mellom representanter for medlemsstatene, samlet på stats- eller regjeringssjefsplan([13]), besluttet medlemsstatenes representanter at ENISA skulle ha sitt sete i en by i Hellas som skulle utpekes av den greske regjeringen. ENISAs vertsstat bør sikre best mulige vilkår for en smidig og effektiv drift av ENISA. For at ENISA skal kunne utføre sine oppgaver korrekt og effektivt, rekruttere og beholde ansatte og øke effektiviteten av nettverksaktiviteter, er det nødvendig at byrået er plassert på et hensiktsmessig sted, der det blant annet er gode transportforbindelser og fasiliteter for ektefeller og barn som følger med ENISAs personale. De nødvendige ordningene bør fastsettes i en avtale mellom ENISA og vertsstaten, etter godkjenning i ENISAs styre.

19) Av hensyn til de økende cybersikkerhetsrisikoene og cybersikkerhetsutfordringene som Unionen står overfor, bør ENISA tildeles økte økonomiske og menneskelige ressurser for å gjenspeile dets utvidede rolle og oppgaver og dets sentrale posisjon i økosystemet av organisasjoner som forsvarer Unionens digitale økosystem, slik at ENISA effektivt kan utføre de oppgavene det er tildelt gjennom denne forordningen.

20) ENISA bør utvikle og opprettholde et høyt nivå av ekspertise og fungere som et referansepunkt og skape tiltro og tillit til det indre markedet i kraft av sin uavhengighet, kvaliteten på rådene og informasjonen det gir, åpenheten omkring dets prosedyrer og arbeidsmetoder samt hvor aktsomt det utfører sine oppgaver. ENISA bør aktivt støtte den nasjonale innsatsen og proaktivt bidra til Unionens innsats og bør utføre sine oppgaver i fullt samarbeid med Unionens institusjoner, organer, kontorer og byråer og med medlemsstatene, og dermed unngå dobbeltarbeid og fremme synergier. I tillegg bør ENISA bygge på bidrag fra og samarbeid med privat sektor, samt andre berørte parter. Gjennom et sett av oppgaver bør det fastsettes hvordan ENISA skal nå sine mål samtidig som byrået gis fleksibilitet i dets aktiviteter.

21) For å kunne gi tilstrekkelig støtte til det driftsmessige samarbeidet mellom medlemsstatene bør ENISA ytterligere styrke sin tekniske og menneskelige kapasitet og kompetanse. ENISA bør øke sin fagkunnskap og kapasitet. ENISA og medlemsstatene kan på frivillig grunnlag utarbeide programmer for utsending av nasjonale eksperter til ENISA, opprettelse av ekspertgrupper og utveksling av personale.

22) ENISA bør bistå Kommisjonen med råd, uttalelser og analyser i alle unionsspørsmål knyttet til utvikling av politikk og lovgivning, oppdateringer og gjennomgåelser på cybersikkerhetsområdet og dets sektorspesifikke aspekter for å øke relevansen av Unionens politikk og unionsretten med en cybersikkerhetsdimensjon, og muliggjøre konsekvens i gjennomføringen av denne politikken og lovgivningen på nasjonalt plan. ENISA bør fungere som et referansepunkt for rådgivning og ekspertise for sektorspesifikke politiske initiativer og lovgivningsinitiativer i Unionen i spørsmål som gjelder cybersikkerhet. ENISA bør regelmessig informere Europaparlamentet om sine aktiviteter.

([13]) Beslutning 2004/97/EF, Euratom, truffet ved felles overenskomst mellom representanter for medlemsstatene, samlet på stats- eller regjeringssjefsplan, av 13. desember 2003 om fastsettelse av sete for visse av Den europeiske unions kontorer og byråer (EUT L 29 av 3.2.2004, s. 15).

23) Den offentlige kjernen av det åpne internettet, det vil si dets viktigste protokoller og infrastruktur, som er et globalt offentlig gode, gir internett som helhet dets viktige funksjoner og danner grunnlaget for dets normale drift. ENISA bør støtte sikkerheten for den offentlige kjernen i det åpne internettet og stabiliteten i driften, inkludert, men ikke begrenset til, nøkkelprotokoller (særlig DNS, BGP og IPv6), driften av domenenavnsystemet (for eksempel driften av alle toppdomener) og driften av rotsonen.

24) ENISAs underliggende oppgave er å fremme konsekvent gjennomføring av den relevante rettslige rammen, særlig en effektiv gjennomføring av direktiv (EU) 2016/1148 og andre relevante rettslige virkemidler som gjelder cybersikkerhetsaspekter, som er viktig for å øke cyberrobustheten. På bakgrunn av det raskt utviklende trusselbildet på cyberområdet er det åpenbart at medlemsstatene må støttes gjennom en mer omfattende, tverrpolitisk tilnærming for å bygge opp cyberrobusthet.

25) ENISA bør bistå medlemsstatene og Unionens institusjoner, organer, kontorer og byråer i arbeidet med å bygge opp og forbedre kapasiteten og beredskapen for å forebygge, påvise og reagere på cybertrusler og cyberhendelser og i forbindelse med sikkerheten i nett- og informasjonssystemer. ENISA bør særlig støtte utviklingen og styrkingen av enhetene for håndtering av digitale hendelser (Computer Security Incident Response Teams, heretter kalt CSIRT-enheter) på nasjonalt plan og i Unionen som fastsatt i direktiv (EU) 2016/1148, med sikte på å oppnå et høyt felles modenhetsnivå for dem i Unionen. Aktiviteter som utføres av ENISA i forbindelse med medlemsstatenes driftskapasitet, bør aktivt støtte tiltak som medlemsstatene treffer for å oppfylle sine forpliktelser i henhold til direktiv (EU) 2016/1148, og bør derfor ikke erstatte dem.

26) ENISA bør også bistå med utvikling og oppdatering av strategiene for sikkerhet i nett- og informasjonssystemer på unionsplan og, på anmodning, på medlemsstatsplan, særlig for cybersikkerhet, og bør fremme spredningen av slike strategier og følge framdriften i gjennomføringen av dem. ENISA bør også bidra til å oppfylle behovet for opplæring og opplæringsmateriell, inkludert offentlige organers behov, og når det er relevant i stor grad «utdanne underviserne» (train the trainers) basert på den europeiske rammen for utvikling av digital kompetanse hos borgerne for å bistå medlemsstatene og Unionens institusjoner, organer, kontorer og byråer med å utvikle sin egen opplæringskapasitet.

27) ENISA bør støtte medlemsstatene på området bevisstgjøring om og utdanning i cybersikkerhet ved å fremme nærmere samordning og utveksling av beste praksis mellom medlemsstatene. Slik støtte kan blant annet bestå i utvikling av et nettverk av nasjonale kontaktpunkter for utdanning og utvikling av en opplæringsplattform for cybersikkerhet. Nettverket av nasjonale kontaktpunkter for utdanning kan fungere innenfor nettverket av nasjonale kontaktpersoner og være et utgangspunkt for framtidig samordning i medlemsstatene.

28) ENISA bør bistå samarbeidsgruppen opprettet ved direktiv (EU) 2016/1148 med utførelsen av dens oppgaver, særlig ved å tilby ekspertise og rådgivning og ved å lette utvekslingen av beste praksis, blant annet med hensyn til medlemsstatenes identifikasjon av ytere av samfunnsviktige tjenester, samt i forbindelse med gjensidig avhengighet over landegrensene når det gjelder risikoer og hendelser.

29) Med sikte på å stimulere til samarbeid mellom offentlig og privat sektor og innenfor den private sektoren, særlig for å støtte vernet av kritisk infrastruktur, bør ENISA støtte informasjonsutveksling i og mellom sektorer, særlig sektorene som er oppført i vedlegg II til direktiv (EU) 2016/1148, ved å gjøre tilgjengelig beste praksis og gi veiledning om tilgjengelige verktøyer og om prosedyrer, samt ved å veilede om hvordan reguleringsmessige spørsmål knyttet til informasjonsutveksling kan løses, for eksempel ved å tilrettelegge for opprettelse av sektorvise sentre for informasjonsutveksling og analyse.

30) Ettersom de mulige negative konsekvensene av sårbarheter i IKT-produkter, IKT-tjenester og IKT-prosesser stadig øker, er det viktig å finne og utbedre slike sårbarheter for å redusere den samlede cybersikkerhetsrisikoen. Det har vist seg at samarbeid mellom organisasjoner, produsenter eller leverandører av sårbare IKT-produkter, IKT-tjenester og IKT-prosesser og medlemmer av forskningsmiljøer innen cybersikkerhet og myndigheter som finner sårbarheter, i vesentlig grad øker både oppdagelsen og utbedringen av sårbarheter i IKT-produkter, IKT-tjenester og IKT-prosesser. Samordnet offentliggjøring av sårbarheter består av en strukturert samarbeidsprosess der sårbarheter rapporteres til eieren av informasjonssystemet, noe som gir organisasjonen mulighet til å diagnostisere og utbedre sårbarheten før detaljert informasjon om sårbarheter blir gjort kjent for tredjeparter eller for offentligheten. Prosessen muliggjør også samordning mellom den som finner sårbarheter og organisasjonen i forbindelse med offentliggjøring av disse sårbarhetene. Samordnede retningslinjer for offentliggjøring av sårbarheter kan spille en viktig rolle i medlemsstatenes innsats for å øke cybersikkerheten.

31) ENISA bør samle og analysere nasjonale rapporter som deles på frivillig grunnlag fra CSIRT-enheter og den interinstitusjonelle enheten for IT-beredskap for Unionens institusjoner, organer og byråer, som er opprettet gjennom avtalen mellom Europaparlamentet, Det europeiske råd, Rådet for Den europeiske union, Europakommisjonen, Den europeiske unions domstol, Den europeiske sentralbank, Den europeiske revisjonsretten, Den europeiske tjenesten for utenriksforbindelser, Den europeiske økonomiske og sosiale komité, Den europeiske regionkomité og Den europeiske investeringsbank om organisering og drift av en enhet for IT-beredskap for Unionens institusjoner, organer og byråer (CERT-EU)([14]) for å bidra til å opprette felles prosedyrer, språk og terminologi for utveksling av informasjon. ENISA bør i denne sammenhengen involvere den private sektoren innenfor rammen av direktiv (EU) 2016/1148 som fastsetter grunnlaget for frivillig utveksling av teknisk informasjon på driftsmessig nivå i nettverket av enheter for håndtering av digitale hendelser («CSIRT-nettet») opprettet ved det nevnte direktivet.

32) ENISA bør bidra til innsats på unionsplan i forbindelse med omfattende grensekryssende hendelser og kriser knyttet til cybersikkerhet. Denne oppgaven bør utføres i samsvar med ENISAs mandat i henhold til denne forordningen og en metode som medlemsstatene skal bli enige om innenfor rammen av kommisjonsrekommandasjon (EU) 2017/1584([15]) og Rådets konklusjoner av 26. juni 2018 om en samordnet innsats ved omfattende cybersikkerhetshendelser og -kriser i Unionen. Denne oppgaven kan omfatte å samle inn relevant informasjon og legge til rette for kontakt mellom CSIRT-nettet og det tekniske fellesskapet, samt mellom beslutningstakere som har ansvar for krisehåndtering. Dessuten bør ENISA, når en eller flere medlemsstater ber om det, støtte det driftsmessige samarbeidet mellom medlemsstatene, i forbindelse med håndtering av hendelser ut fra et teknisk perspektiv, ved å fremme relevant utveksling av tekniske løsninger mellom medlemsstatene og ved å gi innspill til kommunikasjon med offentligheten. ENISA bør støtte det driftsmessige samarbeidet ved å teste ordningene for slikt samarbeid gjennom regelmessige cybersikkerhetsøvelser.

33) For å støtte det driftsmessige samarbeidet bør ENISA utnytte den tilgjengelige tekniske og driftsmessige ekspertisen fra CERT-EU gjennom strukturert samarbeid. Et slikt strukturert samarbeid kan bygge på ENISAs ekspertise. Når det er hensiktsmessig, bør det opprettes egne ordninger mellom de to enhetene for å definere den praktiske gjennomføringen av et slikt samarbeid og for å unngå dobbeltarbeid.

34) Når ENISA utfører sine oppgaver med å støtte det driftsmessige samarbeidet innenfor CSIRT-nettet, bør det på anmodning kunne gi støtte til medlemsstatene, for eksempel ved å gi råd om hvordan de kan forbedre sin kapasitet til å forebygge, påvise og reagere på hendelser, ved å lette den tekniske håndteringen av hendelser som har en betydelig eller vesentlig innvirkning, eller ved å sikre at cybertrusler og cyberhendelser analyseres. ENISA bør lette den tekniske håndteringen av hendelser som har en betydelig eller vesentlig innvirkning, særlig ved å støtte frivillig utveksling av tekniske løsninger mellom medlemsstatene eller ved å framlegge kombinert teknisk informasjon, for eksempel tekniske løsninger som medlemsstatene deler på frivillig grunnlag. I rekommandasjon (EU) 2017/1584 anbefales det at medlemsstatene samarbeider i god tro og uten unødig opphold deler informasjon med hverandre og med ENISA om omfattende hendelser og kriser knyttet til cybersikkerhet. Slik informasjon vil kunne hjelpe ENISA ytterligere med å utføre sin oppgave med å støtte det driftsmessige samarbeidet.

35) Som del av det løpende samarbeidet på teknisk nivå for å støtte situasjonsbevisstheten i Unionen, bør ENISA i nært samarbeid med medlemsstatene utarbeide en regelmessig, detaljert teknisk situasjonsrapport om cybersikkerhet i EU, om hendelser og cybertrusler basert på offentlig tilgjengelig informasjon, sin egen analyse og rapporter som ENISA får fra medlemsstatenes CSIRT-enheter eller de nasjonale felles kontaktpunktene for sikkerheten i nett- og informasjonssystemer («felles kontaktpunkter») som er fastsatt i direktiv (EU) 2016/1148, begge på frivillig grunnlag, Det europeiske senter for bekjempelse av cyberkriminalitet (EC3) i Europol, CERT-EU og, dersom det er relevant, Den europeiske unions etterretnings- og situasjonssenter (EU INTCEN) ved Den europeiske tjenesten for utenriksforbindelser. Rapporten bør gjøres tilgjengelig for Rådet, Kommisjonen, Unionens høyrepresentant for utenrikssaker og sikkerhetspolitikk og CSIRT-nettet.

36) ENISAs støtte til tekniske undersøkelser i ettertid av hendelser med betydelige eller vesentlige konsekvenser, som gjennomføres på anmodning fra de berørte medlemsstatene, bør fokusere på å forebygge framtidige hendelser. De berørte medlemsstatene bør framlegge den informasjonen og gi den bistanden som er nødvendig for at ENISA skal kunne støtte den tekniske undersøkelsen i ettertid på en effektiv måte.

([14]) EUT C 12 av 13.1.2018, s. 1.

([15]) Kommisjonsrekommandasjon (EU) 2017/1584 av 13. september 2017 om samordnet innsats ved omfattende cybersikkerhetshendelser og -kriser (EUT L 239 av 19.9.2017, s. 36).

37) Medlemsstatene kan oppfordre de foretakene som er berørt av hendelsen, til å samarbeide ved å gi ENISA nødvendig informasjon og bistand, uten at dette berører deres rett til å beskytte følsom forretningsinformasjon og informasjon som er relevant for den offentlige sikkerheten.

38) For bedre å forstå utfordringene på cybersikkerhetsområdet og med sikte på å levere strategisk langsiktig rådgivning til medlemsstatene og Unionens institusjoner, organer, kontorer og byråer, må ENISA analysere nåværende og nye cybersikkerhetsrisikoer. For dette formålet bør ENISA i samarbeid med medlemsstatene og, dersom det er relevant, med statistikkorganer og andre organer samle inn relevant informasjon som er offentlig tilgjengelig eller delt på frivillig grunnlag, og utføre analyser av ny teknologi og gi emnespesifikke vurderinger av de forventede samfunnsmessige, rettslige, økonomiske og reguleringsmessige konsekvensene av teknologiske innovasjoner på nett- og informasjonssikkerhet, særlig cybersikkerhet. ENISA bør dessuten støtte medlemsstatene og Unionens institusjoner, organer, kontorer og byråer med å identifisere nye cybersikkerhetsrisikoer og forebygge hendelser ved å utføre analyser av cybertrusler, sårbarheter og hendelser.

39) For å styrke Unionens robusthet bør ENISA utvikle ekspertise på cybersikkerhetsområdet for infrastrukturer, særlig for å støtte sektorene oppført i vedlegg II til direktiv (EU) 2016/1148 og de som brukes av tilbyderne av digitale tjenester oppført i vedlegg III til det nevnte direktivet, ved å gi råd, utstede retningslinjer og utveksle beste praksis. For å sikre enklere tilgang til bedre strukturert informasjon om cybersikkerhetsrisikoer og mulige løsninger, bør ENISA utvikle og opprettholde Unionens «informasjonsnav», en felles nettportal som gir offentligheten informasjon om cybersikkerhet fra Unionens og nasjonale institusjoner, organer, kontorer og byråer. Enklere tilgang til bedre strukturert informasjon om cybersikkerhetsrisikoer og mulige løsninger kan også hjelpe medlemsstatene å styrke sin kapasitet og tilpasse sin praksis, og dermed øke sin samlede robusthet mot cyberangrep.

40) ENISA bør bidra til å øke offentlighetens bevissthet om cybersikkerhetsrisikoer, blant annet gjennom en holdningskampanje på EU-plan ved å fremme utdanning og gi veiledning om god praksis for den enkelte bruker, rettet mot borgere, organisasjoner og foretak. ENISA bør også bidra til å fremme beste praksis og løsninger, inkludert cyberhygiene og cyberkompetanse hos borgere, organisasjoner og foretak, ved å samle inn og analysere offentlig tilgjengelig informasjon om betydelige hendelser, og ved å sammenstille og offentliggjøre rapporter og veiledning for borgere, organisasjoner og foretak for å forbedre deres generelle nivå av beredskap og robusthet. ENISA bør også bestrebe seg på å gi forbrukerne relevant informasjon om gjeldende sertifiseringsordninger, for eksempel ved å utarbeide retningslinjer og gi anbefalinger. ENISA bør dessuten, i tråd med handlingsplanen for digital utdanning fastsatt i Kommisjonens melding av 17. januar 2018 og i samarbeid med medlemsstatenes og Unionens institusjoner, organer, kontorer og byråer, organisere regelmessige informasjons- og opplysningskampanjer rettet mot sluttbrukere for å fremme sikrere atferd på nettet for enkeltpersoner og digital kompetanse, for å øke bevisstheten om mulige cybertrusler, inkludert datakriminalitet som phishing-angrep, botnett, økonomisk svindel og banksvindel, datasvindel, samt for å fremme grunnleggende rådgivning om flerfaktorautentisering, oppdatering, kryptering, anonymisering og datasikring.

41) ENISA bør spille en sentral rolle når det gjelder å øke sluttbrukernes bevissthet om utstyrs sikkerhet og sikker bruk av tjenester, og bør fremme innebygd sikkerhet og innebygd personvern på unionsplan. For å nå dette målet bør ENISA benytte seg av tilgjengelig beste praksis og erfaring, særlig beste praksis og erfaring fra akademiske institusjoner og fra forskere på IT-sikkerhet.

42) For å støtte foretak som er aktive i cybersikkerhetssektoren, samt brukere av cybersikkerhetsløsninger, bør ENISA utvikle og opprettholde et «markedsobservatorium» ved å gjennomføre regelmessige analyser og formidle opplysninger om de viktigste tendensene på markedet for cybersikkerhet, både på etterspørsels- og tilbudssiden.

43) ENISA bør bidra til Unionens innsats for å samarbeide med internasjonale organisasjoner samt innenfor relevante rammer for internasjonalt samarbeid på cybersikkerhetsområdet. ENISA bør særlig, når det er hensiktsmessig, bidra til samarbeid med organisasjoner som OECD, OSSE og NATO. Et slikt samarbeid bør kunne omfatte felles cybersikkerhetsøvelser og felles samordning av innsats ved hendelser. Disse aktivitetene skal utføres i fullt samsvar med prinsippene om inkludering, gjensidighet og selvstendig beslutningsmyndighet, uten at det berører sikkerhets- og forsvarspolitikkens særlige karakter i hver enkelt medlemsstat.

44) For å sikre at ENISA oppnår sine mål fullt ut, bør byrået samarbeide med relevante tilsynsmyndigheter i Unionen og med andre vedkommende myndigheter i Unionen, Unionens institusjoner, organer, kontorer og byråer, inkludert CERT-EU, EC3, Det europeiske forsvarsbyrå (EDA), Det europeiske byrå for globale satellittnavigasjonssystemer (Det europeiske GNSS-byrå), Sammenslutningen av europeiske reguleringsmyndigheter for elektronisk kommunikasjon (BEREC), Det europeiske byrå for driftsforvaltning av store IT-systemer på området frihet, sikkerhet og rettferdighet (eu-LISA), Den europeiske sentralbank (ESB), Den europeiske banktilsynsmyndighet (EBA), Det europeiske personvernråd, Byrået for samarbeid mellom energireguleringsmyndigheter (ACER), Den europeiske unions luftfarts-sikkerhetsbyrå (EASA) og alle andre unionsbyråer som arbeider med cybersikkerhet. ENISA bør også samarbeide med myndigheter som håndterer personvern, for å utveksle fagkunnskap og beste praksis, og bør gi råd om cybersikkerhetsspørsmål som kan påvirke deres arbeid. Representanter for rettshåndhevende myndigheter og personvernmyndigheter på nasjonalt plan og unionsplan bør kunne være representert i ENISAs rådgivende gruppe. I sine kontakter med rettshåndhevende myndigheter om nett- og informasjonssikkerhetsspørsmål som kan påvirke deres arbeid, bør ENISA respektere eksisterende informasjonskanaler og etablerte nett.

45) Det kan opprettes partnerskap med akademiske institusjoner som har forskningsinitiativer på relevante områder, og det bør finnes passende kanaler for innspill fra forbrukerorganisasjoner og andre organisasjoner, som bør tas i betraktning.

46) ENISA bør i sin rolle som sekretariat for CSIRT-nettet, støtte medlemsstatenes CSIRT-enheter og CERT-EU i det driftsmessige samarbeidet i forbindelse med de relevante oppgavene til CSIRT-nettet, som nevnt i direktiv (EU) 2016/1148. Dessuten bør ENISA fremme og støtte samarbeidet mellom relevante CSIRT-enheter når hendelser inntreffer og ved angrep på eller forstyrrelser i nett eller infrastrukturer som forvaltes eller vernes av CSIRT-enhetene, og som berører eller kan berøre minst to CSIRT-enheter, samtidig som det tas behørig hensyn til CSIRT-nettets standardiserte driftsprosedyrer.

47) For å styrke Unionens beredskap for å reagere på hendelser bør ENISA regelmessig organisere cybersikkerhetsøvelser på unionsplan, og på deres anmodning bistå medlemsstatene og Unionens institusjoner, organer, kontorer og byråer med å organisere cybersikkerhetsøvelser. Annethvert år bør det organiseres omfattende øvelser i stor skala som omfatter tekniske, driftsmessige eller strategiske elementer. ENISA bør dessuten regelmessig kunne organisere mindre omfattende øvelser med samme mål om å øke Unionens beredskap for å reagere på hendelser.

48) ENISA bør videreutvikle og opprettholde sin ekspertise innen cybersikkerhetssertifisering med sikte på å støtte Unionens politikk på dette området. ENISA bør bygge videre på gjeldende beste praksis og fremme utbredelsen av cybersikkerhetssertifisering i Unionen, blant annet ved å bidra til innføring og opprettholdelse av en europeisk ramme for cybersikkerhetssertifisering på unionsplan (den europeiske rammen for cybersikkerhetssertifisering), med sikte på å øke gjennomsiktigheten i forbindelse med cybersikkerhet for IKT-produkter, IKT-tjenester og IKT-prosesser, og dermed styrke tilliten til det digitale indre markedet og dets konkurranseevne.

49) Effektive cybersikkerhetsstrategier bør bygge på velutviklede metoder for risikovurdering, både i offentlig og privat sektor. Metoder for risikovurdering brukes på ulike nivåer uten noen felles praksis for hvordan de benyttes effektivt. Utvikling og fremming av beste praksis for risikovurdering og for samvirkende løsninger for risikohåndtering i organisasjoner i offentlig og privat sektor vil øke cybersikkerhetsnivået i Unionen. For dette formålet bør ENISA støtte samarbeidet mellom berørte parter på unionsplan og lette deres arbeid med å opprette og innføre europeiske og internasjonale standarder for risikohåndtering og for målbar sikkerhet for elektroniske produkter, systemer, nett og tjenester, som sammen med programvare utgjør nett- og informasjonssystemene.

50) ENISA bør oppmuntre medlemsstatene, produsentene og leverandørene av IKT-produkter, IKT-tjenester eller IKT-prosesser til å heve sine generelle sikkerhetsstandarder slik at alle internettbrukere kan treffe de nødvendige tiltakene for å sørge for sin egen cybersikkerhet, og de bør gis incentiver til å gjøre dette. Særlig bør produsenter og leverandører av IKT-produkter, IKT-tjenester eller IKT-prosesser sørge for alle nødvendige oppdateringer og tilbakekalle, trekke tilbake eller gjenvinne IKT-produkter, IKT-tjenester eller IKT-prosesser som ikke oppfyller cybersikkerhetsstandardene, mens importører og distributører bør sikre at de IKT-produktene, IKT-tjenestene og IKT-prosessene som de bringer i omsetning i Unionen, oppfyller gjeldende krav og ikke utgjør en risiko for forbrukerne i Unionen.

51) I samarbeid med de vedkommende myndighetene bør ENISA kunne formidle opplysninger om cybersikkerhetsnivået for IKT-produkter, IKT-tjenester og IKT-prosesser som tilbys på det indre markedet, og bør utstede advarsler rettet mot produsenter eller leverandører av IKT-produkter, IKT-tjenester eller IKT-prosesser og kreve at de forbedrer sikkerheten for sine IKT-produkter, IKT-tjenester og IKT-prosesser, inkludert cybersikkerheten.

52) ENISA bør fullt ut ta hensyn til pågående forskning, utvikling og teknologivurdering, særlig aktiviteter som utøves innenfor ulike unionsinitiativer på forskningsområdet, for på anmodning å gi råd til Unionens institusjoner, organer, kontorer og byråer, samt der det er relevant til medlemsstatene dersom de ber om det , om forskningsbehov på cybersikkerhetsområdet. For å identifisere behovene og prioriteringene for forskningen bør ENISA også rådføre seg med de relevante brukergruppene. Nærmere bestemt bør det kunne opprettes samarbeid med Det europeiske forskningsråd, Det europeiske institutt for innovasjon og teknologi og Den europeiske unions institutt for sikkerhetsstudier.

53) Under utarbeidingen av de europeiske cybersikkerhetssertifiseringsordningene bør ENISA regelmessig rådføre seg med standardiseringsorganisasjoner, særlig europeiske standardiseringsorganisasjoner.

54) Cybertrusler er et problem over hele verden. Det er behov for et tettere internasjonalt samarbeid for å forbedre cybersikkerhetsstandardene, blant annet ved å definere felles atferdsnormer og vedta atferdsregler, bruk av internasjonale standarder og informasjonsutveksling, noe som vil fremme et raskere internasjonalt samarbeid som reaksjon på problemer som gjelder nett- og informasjonssikkerhet og fremme en global tilnærming til slike problemer. ENISA bør derfor støtte Unionens fortsatte engasjement og samarbeid med tredjestater og internasjonale organisasjoner ved å bistå relevante institusjoner, organer, kontorer og byråer i Unionen med nødvendig ekspertise og nødvendige analyser ved behov.

55) ENISA bør kunne svare på ad hoc-anmodninger om rådgivning og bistand fra medlemsstatenes og Unionens institusjoner, organer, kontorer og byråer i saker som omfattes av ENISAs mandat.

56) Det er fornuftig og tilrådelig å gjennomføre visse prinsipper for ENISAs forvaltning for å overholde den felles erklæringen og den felles tilnærmingen som den tverrinstitusjonelle arbeidsgruppen om EUs desentraliserte byråer vedtok i juli 2012, og som har som formål å effektivisere de desentraliserte byråenes aktiviteter og forbedre deres resultater. Anbefalingene i den felles erklæringen og den felles tilnærmingen bør også gjenspeiles, der det er hensiktsmessig, i ENISAs arbeidsprogrammer, i ENISAs vurderinger og i ENISAs rapporterings- og forvaltningspraksis.

57) Styret, som består av representanter for medlemsstatene og for Kommisjonen, bør fastsette de generelle retningslinjene for ENISAs drift og sikre at byrået utfører sine oppgaver i samsvar med denne forordningen. Styret bør ha de nødvendige fullmaktene til å fastsette budsjettet, kontrollere gjennomføringen av det, vedta hensiktsmessige finansielle regler, fastsette gjennomsiktige prosedyrer for ENISAs beslutningstaking, vedta ENISAs samlede programdokument, vedta sin egen forretningsorden, utnevne daglig leder og treffe beslutninger om forlengelse og opphør av daglig leders mandatperiode.

58) For at ENISA skal fungere godt og effektivt bør Kommisjonen og medlemsstatene sørge for at personene som oppnevnes til styret, har relevant faglig ekspertise og erfaring. For å sikre kontinuitet i styrets arbeid bør Kommisjonen og medlemsstatene også bestrebe seg på å begrense utskiftingen av sine respektive representanter i styret.

59) For at ENISA skal fungere på en tilfredsstillende måte bør den daglige lederen utnevnes på grunnlag av egnethet og dokumenterte administrasjons- og ledelsesferdigheter samt kvalifikasjoner og erfaring som er relevant for cybersikkerhet. Den daglige lederens oppgaver bør utføres med full uavhengighet. Den daglige lederen bør, etter samråd med Kommisjonen, utarbeide et forslag til ENISAs årlige arbeidsprogram og treffe alle nødvendige tiltak for å sikre at dette arbeidsprogrammet blir gjennomført på riktig måte. Den daglige lederen bør utarbeide en årsrapport som skal framlegges for styret, som omfatter gjennomføringen av ENISAs årlige arbeidsprogram, utarbeide et utkast til overslag over ENISAs inntekter og utgifter samt gjennomføre budsjettet. Den daglige lederen bør ha mulighet til å opprette midlertidige arbeidsgrupper for å behandle bestemte spørsmål, særlig spørsmål av vitenskapelig, teknisk, rettslig eller samfunnsøkonomisk art. Særlig i forbindelse med utarbeidingen av et forslag til en spesifikk europeisk cybersikkerhetssertifiseringsordning («forslag til ordning») anses det å være nødvendig å opprette en midlertidig

arbeidsgruppe. Den daglige lederen bør sikre at medlemmene av de midlertidige arbeidsgruppene velges på grunnlag av et høyest mulig ekspertisenivå, med sikte på å oppnå en jevn kjønnsfordeling og en representativ balanse, etter det som er hensiktsmessig i hver enkelt sak, mellom medlemsstatenes offentlige forvaltninger, Unionens institusjoner, organer, kontorer og byråer og privat sektor, herunder bransjen, brukere og eksperter med akademisk utdanning innenfor nett- og informasjonssikkerhet.

60) Styrets arbeidsutvalg bør bidra til at styret fungerer på en effektiv måte. Som ledd i det forberedende arbeidet i forbindelse med styrets beslutninger bør arbeidsutvalget undersøke relevant informasjon nøye, utforske tilgjengelige alternativer og tilby råd og løsninger for å forberede styrets beslutninger.

61) ENISA bør ha ENISAs rådgivende gruppe som et rådgivende organ, for å sikre regelmessig dialog med privat sektor, forbrukerorganisasjoner og andre berørte parter. ENISAs rådgivende gruppe, som er opprettet av styret etter forslag fra den daglige lederen, bør konsentrere seg om spørsmål som er relevante for berørte parter, og bør gjøre ENISA oppmerksom på dem. ENISAs rådgivende gruppe bør rådspørres, særlig med hensyn til utkastet til ENISAs årlige arbeidsprogram. Sammensetningen av ENISAs rådgivende gruppe og de oppgavene den tildeles bør sikre tilstrekkelig representasjon av berørte parter i ENISAs arbeid.

62) Det bør opprettes en cybersikkerhetssertifiseringsgruppe for berørte parter for å hjelpe ENISA og Kommisjonen ved å fremme samråd med berørte parter. Cybersikkerhetssertifiseringsgruppen for berørte parter bør bestå av medlemmer som representerer bransjen, med en balansert sammensetning, både på etterspørsels- og tilbudssiden når det gjelder IKT-produkter og IKT-tjenester, og særlig inkludert SMB-er, leverandører av digitale tjenester, europeiske og internasjonale standardiseringsorganer, nasjonale akkrediteringsorganer, tilsynsmyndigheter for personvern og samsvarsvurderingsorganer i henhold til europaparlaments- og rådsforordning (EF) nr. 765/2008([16]) samt den akademiske verden og forbrukerorganisasjoner.

63) ENISA bør ha regler for å forebygge og håndtere interessekonflikter. ENISA bør også anvende relevante unionsbestemmelser for offentlig tilgang til dokumenter som fastsatt i europaparlaments- og rådsforordning (EF) nr. 1049/2001([17]). ENISAs behandling av personopplysninger bør være i samsvar med europaparlaments- og rådsforordning (EU) 2018/1725([18]). ENISA bør overholde de bestemmelsene som gjelder for Unionens institusjoner, organer, kontorer og byråer, og den nasjonale lovgivningen om håndtering av informasjon, særlig sensitive ikke-graderte opplysninger og graderte EU-opplysninger (EUCI).

64) For å sikre ENISA full selvstendighet og uavhengighet og gi det mulighet til å utføre ytterligere oppgaver, blant annet uforutsette oppgaver i krisesituasjoner, bør byrået ha et tilstrekkelig stort og eget budsjett der inntektene hovedsakelig kommer fra et bidrag fra Unionen og bidrag fra tredjeland som deltar i ENISAs arbeid. Et tilstrekkelig budsjett er av avgjørende betydning for å sikre at ENISA har tilstrekkelig kapasitet til å utføre alle sine voksende oppgaver og nå sine mål. Størstedelen av ENISAs personale bør være direkte involvert i den praktiske gjennomføringen av ENISAs mandat. Vertsstaten og alle andre medlemsstater bør kunne gi frivillige bidrag til ENISAs budsjett. Unionens budsjettbehandling bør fortsatt få anvendelse når det gjelder eventuelle tilskudd som skal dekkes over Unionens alminnelige budsjett. Videre bør Revisjonsretten revidere ENISAs regnskap for å sikre gjennomsiktighet og ansvarlighet.

65) Cybersikkerhetssertifisering spiller en viktig rolle for å øke tilliten til og sikkerheten for IKT-produkter, IKT-tjenester og IKT-prosesser. Det digitale indre markedet, og særlig dataøkonomien og tingenes internett, kan bare ha framgang hvis allmennheten har tillit til at slike produkter, tjenester og prosesser har et visst nivå av cybersikkerhet. Oppkoplede og selvkjørende biler, elektronisk medisinsk utstyr, industrielle automatiserte styringssystemer og intelligente nett er bare noen eksempler på sektorer der sertifisering allerede brukes i stor grad eller sannsynligvis vil bli brukt i nær framtid. De sektorene som er regulert av direktiv (EU) 2016/1148, er også sektorer der cybersikkerhetssertifisering er av avgjørende betydning.

([16]) Europaparlaments- og rådsforordning (EF) nr. 765/2008 av 9. juli 2008 om fastsettelse av kravene til akkreditering og markedstilsyn for markedsføring av produkter, og om oppheving av forordning (EØF) nr. 339/93 (EUT L 218 av 13.8.2008, s. 30).

([17]) Europaparlaments- og rådsforordning (EF) nr. 1049/2001 av 30. mai 2001 om offentlig tilgang til Europaparlamentets, Rådets og Kommisjonens dokumenter (EFT L 145 av 31.5.2001, s. 43).

([18]) Europaparlaments- og rådsforordning (EU) 2018/1725 av 23. oktober 2018 om vern av fysiske personer i forbindelse med behandling av personopplysninger i Unionens institusjoner, organer, kontorer og byråer og om fri utveksling av slike opplysninger samt om oppheving av forordning (EF) nr. 45/2001 og beslutning nr. 1247/2002/EF (EUT L 295 av 21.11.2018, s. 39).

66) I sin melding fra 2016 med tittelen «Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry» beskrev Kommisjonen behovet for rimelige og driftskompatible cybersikkerhetsprodukter og -løsninger av høy kvalitet. Tilbudet av IKT-produkter, IKT-tjenester og IKT-prosesser i det indre markedet er fortsatt svært fragmentert geografisk. Dette skyldes at cybersikkerhetsbransjen i Europa i stor grad har utviklet seg på grunnlag av nasjonal statlig etterspørsel. I tillegg er mangelen på driftskompatible løsninger (tekniske standarder), praksis og ordninger for sertifisering på unionsplan noen av de andre faktorene som påvirker det indre markedet på cybersikkerhetsområdet. Dette gjør det vanskelig for europeiske foretak å konkurrere på nasjonalt plan, unionsplan og globalt plan. Det begrenser også utvalget av bærekraftig og brukbar cybersikkerhetsteknologi som enkeltpersoner og foretak har tilgang til. I sin melding fra 2017 om midtveisvurderingen av gjennomføringen av strategien for det digitale indre markedet – «A Connected Digital Single Market for All», understreket Kommisjonen behovet for sikre oppkoplede produkter og systemer, og viste til at opprettelsen av en europeisk ramme for IKT-sikkerhet som fastsetter regler for hvordan IKT-sikkerhetssertifisering skal organiseres i Unionen, både vil kunne bevare tilliten til internett og håndtere den nåværende oppsplittingen av det indre markedet.

67) For tiden brukes cybersikkerhetssertifisering av IKT-produkter, IKT-tjenester og IKT-prosesser bare i begrenset omfang. Dersom den forekommer, er det oftest på medlemsstatsplan eller innenfor rammen av bransjedrevne ordninger. Et sertifikat utstedt av en nasjonal cybersikkerhetssertifiseringsmyndighet er i en slik sammenheng i prinsippet ikke anerkjent i andre medlemsstater. Foretakene kan dermed bli nødt til å sertifisere sine IKT-produkter, IKT-tjenester og IKT-prosesser i flere medlemsstater der de har virksomhet, for eksempel for å delta i nasjonale anskaffelsesprosedyrer, noe som øker kostnadene deres. Selv om det utvikles nye ordninger, ser det ikke ut til at det finnes noe sammenhengende og helhetlig syn på overordnede cybersikkerhetsspørsmål, for eksempel på området tingenes internett. Eksisterende ordninger har betydelige mangler og forskjeller med hensyn til produktdekning, tillitsnivåer, grunnleggende kriterier og faktisk bruk, noe som hindrer ordninger for gjensidig anerkjennelse i Unionen.

68) Det er gjort en viss innsats for å sikre gjensidig anerkjennelse av sertifikater i Unionen. Dette har imidlertid bare vært delvis vellykket. Det viktigste eksempelet i denne forbindelse er avtalen om gjensidig anerkjennelse (MRA) fra gruppen av høyere tjenestemenn for informasjonssystemers sikkerhet (SOG-IS). SOG-IS er den viktigste modellen for samarbeid og gjensidig anerkjennelse på området sikkerhetssertifisering, men omfatter bare noen av medlemsstatene. Dette har begrenset SOG-IS-avtalens effektivitet med hensyn til det indre markedet.

69) Det er derfor nødvendig å vedta en felles tilnærming til og opprette en europeisk ramme for cybersikkerhetssertifisering som fastsetter de viktigste overordnede kravene til europeiske cybersikkerhetssertifiseringsordninger som skal utvikles, og som gjør det mulig å anerkjenne og bruke europeiske cybersikkerhetssertifikater og EU-samsvarserklæringer for IKT-produkter, IKT-tjenester eller IKT-prosesser i alle medlemsstater. I denne sammenhengen er det viktig å bygge på eksisterende nasjonale og internasjonale ordninger, samt på systemer for gjensidig anerkjennelse, særlig SOG-IS, og muliggjøre en smidig overgang fra eksisterende ordninger under slike systemer til ordninger innenfor den nye europeiske rammen for cybersikkerhetssertifisering. Den europeiske rammen for cybersikkerhetssertifisering bør ha et dobbelt formål. For det første bør den bidra til å øke tilliten til IKT-produkter, IKT-tjenester og IKT-prosesser som er blitt sertifisert i samsvar med europeiske cybersikkerhetssertifiseringsordninger. For det andre bør den bidra til å unngå at det oppstår mange motstridende eller overlappende nasjonale cybersikkerhetssertifiseringsordninger, og dermed redusere kostnadene for foretak som har virksomhet på det digitale indre markedet. De europeiske cybersikkerhetssertifiseringsordningene bør være ikke-diskriminerende og bygge på europeiske eller internasjonale standarder, med mindre disse standardene er ineffektive eller uegnede for å oppfylle Unionens legitime mål på dette området.

70) Den europeiske rammen for cybersikkerhetssertifisering bør innføres på en ensartet måte i alle medlemsstater for å hindre «sertifiseringsshopping» som følge av ulikt kravnivå i de forskjellige medlemsstatene.

71) Europeiske cybersikkerhetssertifiseringsordninger bør bygge på det som allerede finnes på internasjonalt og nasjonalt plan, og om nødvendig på tekniske spesifikasjoner fra fora og konsortier, der man kan lære av nåværende sterke sider og vurdere og korrigere svakheter.

72) Fleksible cybersikkerhetsløsninger er nødvendig for at bransjen skal kunne foregripe cybertrusler, og derfor bør alle sertifiseringsordninger utformes slik at de ikke risikerer å bli raskt foreldet.

73) Kommisjonen bør gis myndighet til å vedta europeiske cybersikkerhetssertifiseringsordninger for særlige grupper av IKT-produkter, IKT-tjenester og IKT-prosesser. Nasjonale cybersikkerhetssertifiseringsmyndigheter bør gjennomføre og føre tilsyn med disse ordningene, og sertifikater utstedt i henhold til disse ordningene bør være gyldige og anerkjennes i hele Unionen. Sertifiseringsordninger som drives av bransjen eller andre private organisasjoner, bør ikke omfattes av denne forordningen. Organene som driver slike ordninger, bør imidlertid kunne foreslå at Kommisjonen anser slike ordninger som grunnlag for å godkjenne dem som en europeisk cybersikkerhetssertifiseringsordning.

74) Bestemmelsene i denne forordningen bør ikke berøre unionsretten som inneholder særlige regler om sertifisering av IKT-produkter, IKT-tjenester og IKT-prosesser. Særlig i forordning (EU) 2016/679 er det fastsatt bestemmelser om innføring av sertifiseringsmekanismer samt om personvernsegl og -merker for å vise at de behandlingsansvarliges og databehandlernes behandlingsaktiviteter oppfyller kravene i den forordningen. Slike sertifiseringsmekanismer og personvernsegl og -merker bør gjøre det mulig for de registrerte å raskt vurdere nivået for vern av personopplysninger for relevante IKT-produkter, IKT-tjenester og IKT-prosesser. Denne forordningen berører ikke sertifiseringen av databehandling i henhold til forordning (EU) 2016/679, heller ikke når slik behandling er integrert i IKT-produkter, IKT-tjenester og IKT-prosesser.

75) Målet med europeiske cybersikkerhetssertifiseringsordninger bør være å sikre at IKT-produkter, IKT-tjenester og IKT-prosesser som er sertifisert i henhold til slike ordninger, oppfyller særlige krav som har som mål å beskytte tilgjengeligheten, autentisiteten, integriteten og fortroligheten til lagrede, overførte eller behandlede data eller til tilknyttede funksjoner eller tjenester som tilbys eller er tilgjengelige via disse produktene, tjenestene og prosessene gjennom hele deres livssyklus. Det er ikke mulig å fastsette detaljerte cybersikkerhetskrav for alle IKT-produkter, IKT-tjenester og IKT-prosesser i denne forordningen. IKT-produkter, IKT-tjenester og IKT-prosesser og cybersikkerhetsbehovene knyttet til disse produktene, tjenestene og prosessene er så forskjellige at det er svært vanskelig å utarbeide generelle cybersikkerhetskrav som gjelder under alle omstendigheter. Det er derfor nødvendig å gå inn for en omfattende og generell oppfatning av cybersikkerhet med henblikk på sertifisering, som bør utfylles med et sett av særlige cybersikkerhetsmål som skal tas i betraktning ved utformingen av europeiske cybersikkerhetssertifiseringsordninger. Vilkårene for å oppnå slike mål i særlige IKT-produkter, IKT-tjenester og IKT-prosesser bør deretter angis nærmere i den individuelle sertifiseringsordningen som vedtas av Kommisjonen, for eksempel ved henvisning til standarder eller tekniske spesifikasjoner dersom det ikke foreligger egnede standarder.

76) De tekniske spesifikasjonene som skal brukes i europeiske cybersikkerhetssertifiseringsordninger, bør oppfylle kravene fastsatt i vedlegg II til europaparlaments- og rådsforordning (EU) nr. 1025/2012([19]). Noen avvik fra disse kravene kan imidlertid anses som nødvendige i behørig begrunnede tilfeller der disse tekniske spesifikasjonene skal brukes i en europeisk cybersikkerhetssertifiseringsordning som viser til tillitsnivået «høyt». Årsakene til slike avvik bør offentliggjøres.

77) En samsvarsvurdering er en prosedyre for å vurdere om de nærmere angitte kravene til et IKT-produkt, en IKT-tjeneste eller en IKT-prosess er oppfylt. Denne prosedyren utføres av en uavhengig tredjepart som ikke er produsenten eller leverandøren av de IKT-produktene, IKT-tjenestene eller IKT-prosessene som vurderes. Et europeisk cybersikkerhetssertifikat bør utstedes etter en vellykket vurdering av et IKT-produkt, en IKT-tjeneste eller en IKT-prosess. Et europeisk cybersikkerhetssertifikat bør anses som en bekreftelse på at vurderingen er blitt gjennomført korrekt. Avhengig av tillitsnivået bør den europeiske cybersikkerhetssertifiseringsordningen angi om det europeiske cybersikkerhetssertifikatet skal utstedes av et privat eller offentlig organ. Samsvarsvurdering og sertifisering utgjør i seg selv ingen garanti for at sertifiserte IKT-produkter, IKT-tjenester og IKT-prosesser er cybersikre. Det dreier seg i stedet om prosedyrer og tekniske metoder for å bekrefte at IKT-produkter, IKT-tjenester og IKT-prosesser er blitt testet, og at de oppfyller visse cybersikkerhetskrav som er fastsatt andre steder, for eksempel i tekniske standarder.

78) Brukerne av europeiske cybersikkerhetssertifikaters valg av passende sertifisering og tilhørende sikkerhetskrav bør bygge på en analyse av risikoene knyttet til bruk av IKT-produkter, IKT-tjenester eller IKT-prosesser. Tillitsnivået bør derfor stå i forhold til det risikonivået som er knyttet til den tiltenkte bruken av et IKT-produkt, en IKT-tjeneste eller en IKT-prosess.

([19]) Europaparlaments- og rådsforordning (EU) nr. 1025/2012 av 25. oktober 2012 om europeisk standardisering og om endring av rådsdirektiv 89/686/EØF og 93/15/EØF samt europaparlaments- og rådsdirektiv 94/9/EF, 94/25/EF, 95/16/EF, 97/23/EF, 98/34/EF, 2004/22/EF, 2007/23/EF, 2009/23/EF og 2009/105/EF og om oppheving av rådsvedtak 87/95/EØF og europaparlaments- og rådsbeslutning nr. 1673/2006/EF (EUT L 316 av 14.11.2012, s. 12).

79) Europeiske cybersikkerhetssertifiseringsordninger bør kunne gi produsenten eller leverandøren av IKT-produkter, IKT-tjenester eller IKT-prosesser mulighet til å utføre en samsvarsvurdering på eget ansvar (heretter kalt «egenvurdering av samsvar»). I slike tilfeller bør det være tilstrekkelig at produsenten eller leverandøren av IKT-produkter, IKT-tjenester eller IKT-prosesser selv utfører alle kontrollene for å sikre at IKT-produktene, IKT-tjenestene eller IKT-prosessene er i samsvar med den europeiske cybersikkerhetssertifiseringsordningen. Egenvurdering av samsvar bør anses som hensiktsmessig for IKT-produkter, IKT-tjenester eller IKT-prosesser med lav kompleksitet, som utgjør en lav risiko for offentligheten, for eksempel enkle utformings- og produksjonsmekanismer. Dessuten bør egenvurdering av samsvar bare tillates for IKT-produkter, IKT-tjenester eller IKT-prosesser dersom de tilsvarer tillitsnivået «grunnleggende».

80) Europeiske cybersikkerhetssertifiseringsordninger kan gi mulighet for både egenvurdering av samsvar og sertifisering av IKT-produkter, IKT-tjenester eller IKT-prosesser. I så fall bør ordningen gi forbrukere eller andre brukere klare og forståelige metoder for å skille mellom IKT-produkter, IKT-tjenester eller IKT-prosesser som produsenten eller leverandøren av IKT-produkter, IKT-tjenester eller IKT-prosesser har ansvar for å vurdere, og IKT-produkter, IKT-tjenester eller IKT-prosesser som er sertifisert av en tredjepart.

81) Produsenten eller leverandøren av IKT-produkter, IKT-tjenester eller IKT-prosesser som utfører en egenvurdering av samsvar, bør kunne utstede og undertegne EU-samsvarserklæringen som en del av prosedyren for samsvarsvurdering. En EU-samsvarserklæring er et dokument som fastslår at et bestemt IKT-produkt, en bestemt IKT-tjeneste eller en bestemt IKT-prosess er i samsvar med kravene i den europeiske cybersikkerhetssertifiseringsordningen. Ved å utstede og undertegne EU-samsvarserklæringen påtar produsenten eller leverandøren av IKT-produkter, IKT-tjenester eller IKT-prosesser seg ansvaret for at IKT-produktene, IKT-tjenestene eller IKT-prosessene oppfyller de lovfestede kravene i den europeiske cybersikkerhetssertifiseringsordningen. En kopi av EU-samsvarserklæringen bør framlegges for den nasjonale cybersikkerhetssertifiseringsmyndigheten og for ENISA.

82) Produsenter eller leverandører av IKT-produkter, IKT-tjenester eller IKT-prosesser bør gjøre EU-samsvarserklæringen, den tekniske dokumentasjonen og all annen relevant informasjon om IKT-produkters, IKT-tjenesters eller IKT-prosessers samsvar med en europeisk cybersikkerhetssertifiseringsordning tilgjengelig for den vedkommende nasjonale cybersikkerhetssertifiseringsmyndigheten i et tidsrom som er fastsatt i den relevante europeiske cybersikkerhetssertifiseringsordningen. Den tekniske dokumentasjonen bør presisere de kravene som gjelder ut fra ordningen, og bør omfatte utforming, framstilling og drift av IKT-produktet, IKT-tjenesten eller IKT-prosessen i den grad det er relevant for egenvurderingen av samsvar. Den tekniske dokumentasjonen bør utarbeides på en slik måte at det er mulig å vurdere om et IKT-produkt eller en IKT-tjeneste oppfyller kravene som gjelder ut fra denne ordningen.

83) I forvaltningen av den europeiske rammen for cybersikkerhetssertifisering tas det hensyn til medlemsstatenes deltakelse samt passende deltakelse av berørte parter, og Kommisjonens rolle i forbindelse med planlegging, framsettelse av forslag, anmodning, utarbeiding, vedtak og gjennomgåelse av europeiske cybersikkerhetssertifiseringsordninger fastsettes.

84) Kommisjonen bør, med støtte fra Den europeiske cybersikkerhetssertifiseringsgruppen (ECCG – European Cybersecurity Certification Group) og cybersikkerhetssertifiseringsgruppen for berørte parter og etter et åpent og omfattende samråd, utarbeide Unionens løpende arbeidsprogram for europeiske cybersikkerhetssertifiseringsordninger og offentliggjøre det i form av et ikke-bindende instrument. Unionens løpende arbeidsprogram bør være et strategisk dokument som gir særlig bransjen, nasjonale myndigheter og standardiseringsorganer mulighet til å forberede seg på framtidige europeiske cybersikkerhetssertifiseringsordninger. Unionens løpende arbeidsprogram bør omfatte en flerårig oversikt over anmodninger om forslag til ordninger som Kommisjonen har til hensikt å oppfordre ENISA til å utarbeide, på grunnlag av særlige forhold. Kommisjonen bør ta hensyn til Unionens løpende arbeidsprogram når den utarbeider sin løpende plan for IKT-standardisering og standardiseringsanmodninger til europeiske standardiseringsorganisasjoner. I lys av den raske innføringen og spredningen av ny teknologi, framkomsten av tidligere ukjente cybersikkerhetsrisikoer samt utviklingen i regelverket og markedet, bør Kommisjonen eller ECCG ha rett til å be ENISA om å utarbeide forslag til ordninger som ikke inngår i Unionens løpende arbeidsprogram. I slike tilfeller bør Kommisjonen og ECCG også vurdere nødvendigheten av en slik anmodning, samtidig som det tas hensyn til denne forordningens overordnede målsettinger og formål, og behovet for å sikre kontinuitet med hensyn til ENISAs planlegging og ressursbruk.

ENISA bør etter mottak av en slik anmodning så raskt som mulig utarbeide forslag til ordninger for særlige IKT-produkter, IKT-tjenester og IKT-prosesser. Kommisjonen bør vurdere de positive og negative konsekvensene av sin anmodning på det aktuelle markedet, særlig for SMB-er, innovasjon, hindringer for adgang til dette markedet og kostnader for sluttbrukere. Kommisjonen bør på grunnlag av forslaget til ordning utarbeidet av ENISA, gis myndighet til å vedta den europeiske cybersikkerhetssertifiseringsordningen ved hjelp av gjennomføringsrettsakter. Samtidig som det tas hensyn til de generelle formålene og sikkerhetsmålene i denne forordningen, bør de europeiske cybersikkerhets-sertifiseringsordningene som er vedtatt av Kommisjonen, angi et minstesett av elementer for den enkelte ordningens formål, omfang og funksjon. Disse elementene bør blant annet omfatte cybersikkerhetssertifiseringens omfang og formål, inkludert kategoriene av IKT-produkter, IKT-tjenester og IKT-prosesser som omfattes, den detaljerte spesifikasjonen av cybersikkerhetskravene, for eksempel ved henvisning til standarder eller tekniske spesifikasjoner, de særlige vurderingskriteriene og vurderingsmetodene, samt det tiltenkte tillitsnivået («grunnleggende», «betydelig» eller «høyt») og vurderingsnivåene dersom det er relevant. ENISA bør kunne avvise en anmodning fra ECCG. Slike beslutninger bør treffes av styret og være behørig begrunnet.

85) ENISA bør ha et nettsted med informasjon om og offentliggjøring av europeiske cybersikkerhetssertifiseringsordninger, som blant annet bør omfatte anmodningene om utarbeiding av et forslag til ordning samt tilbakemeldinger som er mottatt i forbindelse med samrådet som ENISA gjennomfører i forberedelsesfasen. Nettstedet bør også inneholde informasjon om europeiske cybersikkerhetssertifikater og EU-samsvarserklæringer utstedt på grunnlag av denne forordningen, inkludert informasjon om tilbakekalling og utløp av slike europeiske cybersikkerhetssertifikater og EU-samsvarserklæringer. Nettstedet bør også angi de nasjonale cybersikkerhetssertifiseringsordningene som er blitt erstattet av en europeisk cybersikkerhetssertifiseringsordning.

86) Tillitsnivået for en europeisk sertifiseringsordning utgjør grunnlaget for tillit til at et IKT-produkt, en IKT-tjeneste eller en IKT-prosess oppfyller sikkerhetskravene i en bestemt europeisk cybersikkerhetssertifiseringsordning. For å sikre konsekvens i den europeiske rammen for cybersikkerhetssertifisering bør en europeisk cybersikkerhets-sertifiseringsordning kunne fastsette tillitsnivåer for europeiske cybersikkerhetssertifikater og EU-samsvarserklæringer utstedt innenfor rammen av ordningen. Hvert europeisk cybersikkerhetssertifikat kan vise til ett av tillitsnivåene «grunnleggende», «betydelig» eller «høyt», mens EU-samsvarserklæringen bare kan vise til tillitsnivået «grunnleggende». Tillitsnivåene vil innebære en tilsvarende nøyaktighet og grundighet i vurderingen av IKT-produktene, IKT-tjenestene eller IKT-prosessene og vil fastsettes ved henvisning til tekniske spesifikasjoner, standarder og prosedyrer knyttet til disse, inkludert tekniske kontroller, som har som formål å begrense eller forebygge hendelser. Hvert tillitsnivå bør være konsekvent på tvers av de ulike sektorområdene der det benyttes sertifisering.

87) En europeisk cybersikkerhetssertifiseringsordning kan angi flere vurderingsnivåer avhengig av hvor nøyaktig og grundig den benyttede vurderingsmetoden er. Vurderingsnivåene bør tilsvare ett av tillitsnivåene og bør knyttes til en egnet kombinasjon av tillitskomponenter. For alle tillitsnivåer bør IKT-produktet, IKT-tjenesten eller IKT-prosessen inneholde en rekke sikre funksjoner, som angitt i ordningen, som kan omfatte: en sikker «klar til bruk»-konfigurasjon, en signert kode, sikker oppdatering og mekanismer for begrensning av misbruk og full beskyttelse av stack- eller heap-minne. Disse funksjonene bør utarbeides og vedlikeholdes ved hjelp av sikkerhetsfokuserte utviklingsmetoder og tilhørende verktøyer for å sikre at effektive mekanismer for programvare og maskinvare er innarbeidet på pålitelig vis.

88) For tillitsnivået «grunnleggende» bør vurderingen minst bygge på følgende tillitskomponenter: Vurderingen bør minst omfatte en gjennomgåelse av den tekniske dokumentasjonen for IKT-produktet, IKT-tjenesten eller IKT-prosessen utført av samsvarsvurderingsorganet. Dersom sertifiseringen omfatter IKT-prosesser, bør prosessen som brukes til å utforme, utvikle og vedlikeholde et IKT-produkt eller en IKT-tjeneste, også omfattes av den tekniske undersøkelsen. Om en europeisk cybersikkerhetssertifiseringsordning gir mulighet for egenvurdering av samsvar, bør det være tilstrekkelig at produsenten eller leverandøren av IKT-produkter, IKT-tjenester eller IKT-prosesser har utført en egenvurdering av IKT-produktenes, IKT-tjenestenes eller IKT-prosessenes samsvar med sertifiseringsordningen.

89) For tillitsnivået «betydelig» bør vurderingen, i tillegg til kravene til tillitsnivået «grunnleggende», minst bygge på en kontroll av samsvar mellom IKT-produktets, IKT-tjenestens eller IKT-prosessens sikkerhetsfunksjoner og den tekniske dokumentasjonen.

90) For tillitsnivået «høyt» bør vurderingen, i tillegg til kravene til tillitsnivået «betydelig», minst bygge på en effektivitetstest som vurderer motstandsdyktigheten av IKT-produktets, IKT-tjenestens eller IKT-prosessens sikkerhetsfunksjoner mot grundig forberedte cyberangrep utført av personer med betydelige ferdigheter og ressurser.

91) Det bør fortsatt være frivillig å benytte europeisk cybersikkerhetssertifisering og EU-samsvarserklæringer, med mindre annet er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett vedtatt i samsvar med unionsretten. I fravær av harmonisert unionsrett kan medlemsstatene vedta nasjonale tekniske forskrifter som fastsetter obligatorisk sertifisering innenfor rammen av en europeisk cybersikkerhetssertifiseringsordning i samsvar med europaparlaments- og rådsdirektiv (EU) 2015/1535([20]). Medlemsstatene kan også benytte europeisk cybersikkerhetssertifisering i forbindelse med offentlige innkjøp og europaparlaments- og rådsdirektiv 2014/24/EU([21]).

92) På enkelte områder kan det i framtiden bli nødvendig å innføre særlige krav til cybersikkerhet og gjøre cyber sikkerhetssertifisering obligatorisk for visse IKT-produkter, IKT-tjenester eller IKT-prosesser for å forbedre cybersikkerheten i Unionen. Kommisjonen bør regelmessig overvåke hvordan vedtatte europeiske ordninger for cybersikkerhet påvirker tilgjengeligheten av sikre IKT-produkter, IKT-tjenester og IKT-prosesser på det indre markedet, og bør regelmessig vurdere i hvor stor grad produsentene eller leverandørene av IKT-produkter, IKT-tjenester eller IKT-prosesser i Unionen bruker sertifiseringsordningene. Effektiviteten til de europeiske cybersikkerhetssertifiseringsordningene, og hvorvidt særlige ordninger bør gjøres obligatoriske, bør vurderes i lys av Unionens regelverk knyttet til cybersikkerhet, særlig direktiv (EU) 2016/1148, idet det tas hensyn til sikkerheten i nett- og informasjonssystemene som brukes av ytere av samfunnsviktige tjenester.

93) Europeiske cybersikkerhetssertifikater og EU-samsvarserklæringer bør hjelpe sluttbrukerne å foreta velbegrunnede valg. IKT-produkter, IKT-tjenester og IKT-prosesser som er sertifisert eller som det er utstedt en EU-samsvarserklæring for, bør derfor ledsages av strukturert informasjon som er tilpasset det forventede tekniske nivået hos den tiltenkte sluttbrukeren. All slik informasjon bør være tilgjengelig på internett, og eventuelt i fysisk form. Sluttbrukeren bør ha tilgang til opplysninger om sertifiseringsordningens referansenummer, tillitsnivået, beskrivelsen av cybersikkerhetsrisikoene knyttet til IKT-produktet, IKT-tjenesten eller IKT-prosessen, og den utstedende myndigheten eller det utstedende organet, eller bør kunne få en kopi av det europeiske cybersikkerhetssertifikatet. I tillegg bør sluttbrukeren informeres om støtterutinene for cybersikkerhet, det vil si hvor lenge sluttbrukeren kan forvente å motta cybersikkerhetsoppdateringer eller -korrigeringer fra produsenten eller leverandøren av IKT-produkter, IKT-tjenester eller IKT-prosesser. I relevante tilfeller bør det gis veiledning om tiltak eller innstillinger som sluttbrukeren kan iverksette for å opprettholde eller øke cybersikkerheten til IKT-produktet eller IKT-tjenesten, og om kontaktinformasjonen til ett felles kontaktpunkt for å rapportere om og få støtte ved cyberangrep (i tillegg til automatisk rapportering). Denne informasjonen bør oppdateres regelmessig og gjøres tilgjengelig på et nettsted med informasjon om europeiske cybersikkerhetssertifiseringsordninger.

94) For å nå målene i denne forordningen og unngå oppsplittingen av det indre markedet bør nasjonale ordninger eller prosedyrer for cybersikkerhetssertifisering av IKT-produkter, IKT-tjenester eller IKT-prosesser som omfattes av en europeisk cybersikkerhetssertifiseringsordning, opphøre å gjelde fra en dato fastsatt av Kommisjonen gjennom gjennomføringsrettsakter. Medlemsstatene bør dessuten ikke innføre nye nasjonale cybersikkerhetssertifiseringsordninger for IKT-produkter, IKT-tjenester eller IKT-prosesser som allerede omfattes av en eksisterende europeisk cybersikkerhetssertifiseringsordning. Medlemsstatene bør imidlertid ikke hindres i å vedta eller opprettholde nasjonale cybersikkerhetssertifiseringsordninger for formål knyttet til nasjonal sikkerhet. Medlemsstatene bør informere Kommisjonen og ECCG om eventuelle hensikter om å utarbeide nye nasjonale cybersikkerhetssertifiseringsordninger. Kommisjonen og ECCG bør vurdere hvordan de nye nasjonale cybersikkerhetssertifiseringsordningene påvirker et velfungerende indre marked, og i lys av en eventuell strategisk interesse i stedet kreve en europeisk cybersikkerhetssertifiseringsordning.

95) Europeiske cybersikkerhetssertifiseringsordninger har til hensikt å bidra til å harmonisere cybersikkerhetspraksis i Unionen. De må bidra til å øke cybersikkerhetsnivået i Unionen. Utformingen av de europeiske cybersikkerhetssertifiseringsordningene bør ta hensyn til og gjøre det mulig å utvikle innovasjoner på cybersikkerhetsområdet.

([20]) Europaparlaments- og rådsdirektiv (EU) 2015/1535 av 9. september 2015 om en informasjonsprosedyre for tekniske forskrifter og regler for informasjonssamfunnstjenester (EUT L 241 av 17.9.2015, s. 1).

([21]) Europaparlaments- og rådsdirektiv 2014/24/EU av 26. februar 2014 om offentlige innkjøp og om oppheving av direktiv 2004/18/EF (EUT L 94 av 28.3.2014, s. 65).

96) Europeiske cybersikkerhetssertifiseringsordninger bør ta hensyn til eksisterende metoder for utvikling av programvare og maskinvare, og særlig til hvordan hyppige programvare- eller fastvareoppdateringer påvirker individuelle europeiske cybersikkerhetssertifikater. Europeiske cybersikkerhetssertifiseringsordninger bør fastsette vilkårene for at en oppdatering kan kreve at et IKT-produkt, en IKT-tjeneste eller en IKT-prosess skal sertifiseres på nytt, eller at virkeområdet for et bestemt europeisk cybersikkerhetssertifikat skal reduseres, idet det tas hensyn til eventuelle negative virkninger av oppdateringen på overholdelsen av sikkerhetskravene i det sertifikatet.

97) Når en europeisk cybersikkerhetssertifiseringsordning er vedtatt, bør produsenter eller leverandører av IKT-produkter, IKT-tjenester eller IKT-prosesser kunne sende søknader om sertifisering av sine IKT-produkter eller IKT-tjenester til et valgfritt samsvarsvurderingsorgan hvor som helst i Unionen. Samsvarsvurderingsorganer bør akkrediteres av et nasjonalt akkrediteringsorgan dersom de oppfyller visse krav fastsatt i denne forordningen. Akkrediteringen bør utstedes for en periode på høyst fem år og bør fornyes på samme vilkår, forutsatt at samsvarsvurderingsorganet fortsatt oppfyller kravene. Nasjonale akkrediteringsorganer bør begrense, midlertidig oppheve eller tilbakekalle akkrediteringen av et samsvarsvurderingsorgan dersom vilkårene for akkreditering ikke eller ikke lenger oppfylles, eller dersom tiltak truffet av samsvarsvurderingsorganet er i strid med denne forordningen.

98) Henvisninger i nasjonal lovgivning til nasjonale standarder som har opphørt å ha virkning på grunn av ikrafttredelsen av en europeisk cybersikkerhetssertifiseringsordning, kan skape forvirring. Medlemsstatene bør derfor ta hensyn til vedtakelsen av en europeisk cybersikkerhetssertifiseringsordning i sin nasjonale lovgivning.

99) For å oppnå likeverdige standarder i hele Unionen, lette gjensidig anerkjennelse og fremme generell aksept av europeiske cybersikkerhetssertifikater og EU-samsvarserklæringer er det nødvendig å innføre et system for fagfellevurdering mellom nasjonale cybersikkerhetssertifiseringsmyndigheter. Fagfellevurdering bør omfatte prosedyrer for å føre tilsyn med at IKT-produkter, IKT-tjenester og IKT-prosesser er i samsvar med europeiske cybersikkerhetssertifikater, for å overvåke forpliktelsene til produsenter eller leverandører av IKT-produkter, IKT-tjenester eller IKT-prosesser som utfører egenvurdering av samsvar, og for å overvåke samsvarsvurderingsorganer samt om personalet i organer som utsteder sertifikater for tillitsnivået «høyt», har tilstrekkelig ekspertise. Kommisjonen bør ved hjelp av gjennomføringsrettsakter kunne opprette minst en femårsplan for fagfellevurderinger, samt fastsette kriterier og metoder for hvordan fagfellevurderingssystemet skal fungere.

100) Uten at det berører det generelle fagfellevurderingssystemet som skal innføres for alle nasjonale cybersikkerhets sertifiseringsmyndigheter innenfor den europeiske rammen for cybersikkerhetssertifisering, kan visse europeiske cybersikkerhetssertifiseringsordninger omfatte en ordning for fagfellevurdering for organer som utsteder europeiske cybersikkerhetssertifikater for IKT-produkter, IKT-tjenester og IKT-prosesser med tillitsnivået «høyt» under slike ordninger. ECCG bør støtte gjennomføringen av slike ordninger for fagfellevurdering. Fagfellevurderingene bør særlig vurdere om de berørte organene utfører sine oppgaver på en harmonisert måte, og kan omfatte klageordninger. Resultatene av fagfellevurderingene bør offentliggjøres. De berørte organene kan vedta hensiktsmessige tiltak for å tilpasse sin praksis og ekspertise tilsvarende.

101) Medlemsstatene bør utpeke en eller flere nasjonale cybersikkerhetssertifiseringsmyndigheter som skal føre tilsyn med at forpliktelsene fastsatt i denne forordningen oppfylles. En nasjonal cybersikkerhetssertifiseringsmyndighet kan være en eksisterende eller en ny myndighet. En medlemsstat bør også, etter avtale med en annen medlemsstat, kunne utpeke en eller flere nasjonale cybersikkerhetssertifiseringsmyndigheter på den andre medlemsstatens territorium.

102) Nasjonale cybersikkerhetssertifiseringsmyndigheter bør særlig overvåke og håndheve forpliktelsene til produsenter eller leverandører av IKT-produkter, IKT-tjenester eller IKT-prosesser som er etablert på deres respektive territorier i forbindelse med EU-samsvarserklæringen, bistå de nasjonale akkrediteringsorganene med overvåking av og tilsyn med samsvarsvurderingsorganenes aktiviteter ved å stille ekspertise og relevant informasjon til rådighet for dem, gi samsvarsvurderingsorganene tillatelse til å utføre sine oppgaver dersom disse organene oppfyller ytterligere krav fastsatt i en europeisk cybersikkerhetssertifiseringsordning, og overvåke den relevante utviklingen på cybersikkerhetssertifiseringsområdet. Nasjonale cybersikkerhetssertifiseringsmyndigheter bør også behandle klager som er inngitt av fysiske eller juridiske personer i forbindelse med europeiske cybersikkerhetssertifikater utstedt av disse myndighetene eller i forbindelse med europeiske cybersikkerhetssertifikater utstedt av samsvarsvurderingsorganer, og dersom slike

sertifikater angir tillitsnivået «høyt», i relevant utstrekning undersøke klagens formål og informere klageren om forløpet og utfallet av undersøkelsen innen en rimelig frist. De nasjonale cybersikkerhetssertifiseringsmyndighetene bør dessuten samarbeide med andre nasjonale cybersikkerhetssertifiseringsmyndigheter eller andre offentlige myndigheter, blant annet ved å utveksle informasjon om mulig manglende samsvar mellom IKT-produkter, IKT-tjenester og IKT-prosesser og kravene i denne forordningen eller særlige europeiske cybersikkerhetssertifiseringsordninger. Kommisjonen bør lette denne utvekslingen av informasjon ved å gjøre tilgjengelig et generelt støttesystem for elektronisk informasjon, for eksempel informasjons- og kommunikasjonssystemet for markedstilsyn (ICSMS – Information and Communication System on Market Surveillance) og hurtigvarslingssystemet for farlige produkter som ikke er næringsmidler (RAPEX – Rapid Alert System for dangerous non-food products), som allerede brukes av markedstilsynsmyndighetene på grunnlag av forordning (EF) nr. 765/2008.

103) For å sikre en konsekvent bruk av den europeiske rammen for cybersikkerhetssertifisering bør det opprettes en ECCG som består av representanter for nasjonale cybersikkerhetssertifiseringsmyndigheter eller andre relevante nasjonale myndigheter. De viktigste oppgavene for ECCG bør være å gi råd til og bistå Kommisjonen i dens arbeid for å sikre konsekvent gjennomføring og bruk av den europeiske rammen for cybersikkerhetssertifisering, bistå og samarbeide tett med ENISA ved utarbeidingen av forslag til cybersikkerhetssertifiseringsordninger, i behørig begrunnede tilfeller be ENISA om å utarbeide et forslag til ordning, vedta uttalelser rettet til ENISA om forslag til ordninger og vedta uttalelser rettet til Kommisjonen om vedlikehold og gjennomgåelse av eksisterende europeiske cybersikkerhets-sertifiseringsordninger. ECCG bør lette utvekslingen av god praksis og ekspertise mellom de ulike nasjonale cybersikkerhetssertifiseringsmyndighetene som har ansvar for godkjenningen av samsvarsvurderingsorganer og utstedelsen av europeiske cybersikkerhetssertifikater.

104) For å øke bevisstheten om og få aksept for framtidige europeiske cybersikkerhetssertifiseringsordninger kan Kommisjonen utstede generelle eller sektorspesifikke retningslinjer for cybersikkerhet, for eksempel om god praksis for cybersikkerhet eller ansvarlig cybersikkerhetsatferd, som framhever de positive konsekvensene av å bruke sertifiserte IKT-produkter, IKT-tjenester og IKT-prosesser.

105) For ytterligere å lette handelen og erkjenne at IKT-forsyningskjedene er globale, kan avtaler om gjensidig anerkjennelse av europeiske cybersikkerhetssertifikater inngås av Unionen i samsvar med artikkel 218 i traktaten om Den europeiske unions virkemåte (TEUV). Kommisjonen kan, idet det tas hensyn til rådene fra ENISA og Den europeiske cybersikkerhetssertifiseringsgruppen, anbefale at det innledes relevante forhandlinger. Hver europeisk cybersikkerhets-sertifiseringsordning bør fastsette særlige vilkår for slike avtaler om gjensidig anerkjennelse med tredjeland.

106) For å sikre ensartede vilkår for gjennomføring av denne forordningen bør Kommisjonen gis gjennomføringsmyndighet. Denne myndigheten bør utøves i samsvar med europaparlaments- og rådsforordning (EU) nr. 182/2011([22]).

107) Undersøkelsesprosedyren bør brukes ved vedtakelse av gjennomføringsrettsakter om europeiske cybersikkerhets sertifiseringsordninger av IKT-produkter, IKT-tjenester eller IKT-prosesser, ved vedtakelse av gjennomføringsrettsakter om ordninger for ENISAs gjennomføring av undersøkelser, ved vedtakelse av gjennomføringsrettsakter om en plan for fagfellevurdering av nasjonale cybersikkerhetssertifiseringsmyndigheter, samt vedtakelse av gjennomføringsrettsakter om vilkår, formater og prosedyrer for meldinger om akkrediterte samsvarsvurderingsorganer fra de nasjonale cybersikkerhetssertifiseringsmyndighetene til Kommisjonen.

108) ENISAs arbeid bør vurderes regelmessig og på en uavhengig måte. Vurderingen bør ta hensyn til ENISAs mål, arbeidsmetoder og oppgavenes relevans, særlig oppgavene knyttet til det driftsmessige samarbeidet på unionsplan. Denne vurderingen bør også vurdere konsekvensene, virkningen og effektiviteten av den europeiske rammen for cybersikkerhetssertifisering. Ved en gjennomgåelse bør Kommisjonen vurdere hvordan ENISAs rolle som et referansepunkt for rådgivning og ekspertise kan styrkes, og bør også vurdere muligheten for at ENISA kan støtte vurderingen av tredjelands IKT-produkter, IKT-tjenester og IKT-prosesser som ikke overholder unionsreglene, når slike produkter, tjenester og prosesser innføres til Unionen.

([22]) Europaparlaments- og rådsforordning (EU) nr. 182/2011 av 16. februar 2011 om fastsettelse av allmenne regler og prinsipper for medlemsstatenes kontroll med Kommisjonens utøvelse av sin gjennomføringsmyndighet (EUT L 55 av 28.2.2011, s. 13).

109) Ettersom målene for denne forordningen ikke i tilstrekkelig grad kan nås av medlemsstatene og derfor på grunn av deres omfang og virkninger bedre kan nås på unionsplan, kan Unionen treffe tiltak i samsvar med nærhetsprinsippet som fastsatt i artikkel 5 i traktaten om Den europeiske union. I samsvar med forholdsmessighetsprinsippet fastsatt i nevnte artikkel går denne forordningen ikke lenger enn det som er nødvendig for å nå disse målene.

110) Forordning (EU) nr. 526/2013 bør oppheves.

VEDTATT DENNE FORORDNINGEN:

AVDELING I

ALMINNELIGE BESTEMMELSER

Artikkel 1

Formål og virkeområde

1. For å sikre at det indre markedet fungerer på en tilfredsstillende måte og samtidig oppnå et høyt nivå av cybersikkerhet, cyberrobusthet og tillit i Unionen, fastsetter denne forordningen

a) mål, oppgaver og organisatoriske spørsmål knyttet til ENISA (Den europeiske unions cybersikkerhetsbyrå), og

b) en ramme for innføring av europeiske cybersikkerhetssertifiseringsordninger for å sikre et tilstrekkelig nivå av cybersikkerhet for IKT-produkter, IKT-tjenester og IKT-prosesser i Unionen, samt for å unngå oppsplittingen av det indre markedet med hensyn til cybersikkerhetssertifiseringsordninger i Unionen.

Rammen nevnt i første ledd bokstav b) får anvendelse uten at det berører særlige bestemmelser i andre unionsrettsakter om frivillig eller obligatorisk sertifisering.

2. Denne forordningen berører ikke medlemsstatenes myndighetsområder med hensyn til aktiviteter som gjelder offentlig sikkerhet, forsvar, nasjonal sikkerhet og statens aktiviteter på det strafferettslige området.

Artikkel 2

Definisjoner

I denne forordningen menes med

1) «cybersikkerhet» de aktivitetene som er nødvendige for å beskytte nett- og informasjonssystemer, brukerne av slike systemer og andre personer som berøres av cybertrusler,

2) «nett- og informasjonssystem» et nett- og informasjonssystem som definert i artikkel 4 nr. 1 i direktiv (EU) 2016/1148,

3) «nasjonal strategi for sikkerhet i nett- og informasjonssystemer» en nasjonal strategi for sikkerhet i nett- og informasjonssystemer som definert i artikkel 4 nr. 3 i direktiv (EU) 2016/1148,

4) «yter av samfunnsviktige tjenester» en yter av samfunnsviktige tjenester som definert i artikkel 4 nr. 4 i direktiv (EU) 2016/1148,

5) «tilbyder av digitale tjenester» en tilbyder av digitale tjenester som definert i artikkel 4 nr. 6 i direktiv (EU) 2016/1148,

6) «hendelse» en hendelse som definert i artikkel 4 nr. 7 i direktiv (EU) 2016/1148,

7) «hendelseshåndtering» en hendelseshåndtering som definert i artikkel 4 nr. 8 i direktiv (EU) 2016/1148,

8) «cybertrussel» enhver potensiell omstendighet, hendelse eller handling som kan skade, forstyrre eller på annen negativ måte påvirke nett- og informasjonssystemer, brukerne av slike systemer og andre personer,

9) «europeisk cybersikkerhetssertifiseringsordning» et omfattende sett av regler, tekniske krav, standarder og prosedyrer som er fastsatt på unionsplan, og som gjelder for sertifisering eller samsvarsvurdering av særlige IKT-produkter, IKT-tjenester eller IKT-prosesser,

10) «nasjonal cybersikkerhetssertifiseringsordning» et omfattende sett av regler, tekniske krav, standarder og prosedyrer som er utarbeidet og vedtatt av en nasjonal offentlig myndighet, og som gjelder for sertifisering eller samsvarsvurdering av IKT-produkter, IKT-tjenester og IKT-prosesser som omfattes av den særlige ordningen,

11) «europeisk cybersikkerhetssertifikat» et dokument utstedt av et relevant organ, som bekrefter at et bestemt IKT-produkt, en bestemt IKT-tjeneste eller en bestemt IKT-prosess er blitt vurdert med hensyn til om de oppfyller særlige sikkerhetskrav fastsatt i en europeisk cybersikkerhetssertifiseringsordning,

12) «IKT-produkt» et element eller en gruppe av elementer i et nett- eller informasjonssystem,

13) «IKT-tjeneste» en tjeneste som helt eller hovedsakelig består av overføring, lagring, innhenting eller behandling av informasjon ved hjelp av nett- og informasjonssystemer,

14) «IKT-prosess» et sett av aktiviteter som utføres for å utforme, utvikle, levere eller vedlikeholde et IKT-produkt eller en IKT-tjeneste,

15) «akkreditering» en akkreditering som definert i artikkel 2 nr. 10 i forordning (EF) nr. 765/2008,

16) «nasjonalt akkrediteringsorgan» et nasjonalt akkrediteringsorgan som definert i artikkel 2 nr. 11 i forordning (EF) nr. 765/2008,

17) «samsvarsvurdering» en samsvarsvurdering som definert i artikkel 2 nr. 12 i forordning (EF) nr. 765/2008,

18) «samsvarsvurderingsorgan» et samsvarsvurderingsorgan som definert i artikkel 2 nr. 13 i forordning (EF) nr. 765/2008,

19) «standard» en standard som definert i artikkel 2 nr. 1 i forordning (EU) nr. 1025/2012,

20) «teknisk spesifikasjon» et dokument som fastsetter de tekniske kravene som skal oppfylles av, eller prosedyrer for samsvarsvurdering knyttet til, et IKT-produkt, en IKT-tjeneste eller en IKT-prosess,

21) «tillitsnivå» et grunnlag for tillit til at et IKT-produkt, en IKT-tjeneste eller en IKT-prosess oppfyller sikkerhetskravene i en bestemt europeisk cybersikkerhetssertifiseringsordning, som angir på hvilket nivå et IKT-produkt, en IKT-tjeneste eller en IKT-prosess er blitt vurdert, men måler ikke i seg selv det aktuelle IKT-produktets, IKT-tjenestens eller IKT-prosessens sikkerhet,

22) «egenvurdering av samsvar» et tiltak som utføres av en produsent eller en leverandør av IKT-produkter, IKT-tjenester eller IKT-prosesser, som vurderer om disse IKT-produktene, IKT-tjenestene eller IKT-prosessene oppfyller kravene i en spesifikk europeisk cybersikkerhetssertifiseringsordning.

AVDELING II

ENISA (DEN EUROPEISKE UNIONS CYBERSIKKERHETSBYRÅ)

KAPITTEL I

Mandat og mål

Artikkel 3

Mandat

1. ENISA skal utføre de oppgavene det er pålagt ved denne forordningen for å oppnå et høyt felles nivå av cybersikkerhet i hele Unionen, blant annet ved aktivt å støtte medlemsstater, Unionens institusjoner, organer, kontorer og byråer med å forbedre cybersikkerheten. ENISA skal fungere som et referansepunkt for rådgivning og ekspertise på området cybersikkerhet for Unionens institusjoner, organer, kontorer og byråer samt for andre berørte parter i Unionen.

ENISA skal bidra til å redusere oppsplittingen av det indre markedet ved å utføre de oppgavene det er pålagt gjennom denne forordningen.

2. ENISA skal utføre de oppgavene det er pålagt gjennom unionsrettsakter som fastsetter tiltak for tilnærming av de av medlemsstatenes lover og forskrifter som gjelder cybersikkerhet.

3. ENISA skal ved utførelsen av sine oppgaver opptre uavhengig og samtidig unngå dobbeltarbeid i medlemsstaten og ta hensyn til eksisterende ekspertise i medlemsstaten.

4. ENISA skal utvikle sine egne ressurser, inkludert teknisk og menneskelig kapasitet og kompetanse, som er nødvendige for å utføre de oppgavene det er pålagt gjennom denne forordningen.

Artikkel 4

Mål

1. ENISA skal være et kompetansesenter for cybersikkerhet i kraft av sin uavhengighet, den vitenskapelige og tekniske kvaliteten på rådene og bistanden det gir, opplysningene det leverer, åpenheten omkring dets driftsprosedyrer og arbeidsmetoder samt hvor aktsomt det utfører sine oppgaver.

2. ENISA skal bistå Unionens institusjoner, organer, kontorer og byråer samt medlemsstatene med å utvikle og gjennomføre Unionens politikk knyttet til cybersikkerhet, inkludert sektorpolitikk i forbindelse med cybersikkerhet.

3. ENISA skal støtte kapasitetsoppbygging og beredskap i hele Unionen ved å bistå Unionens institusjoner, organer, kontorer og byråer samt medlemsstatene og berørte parter i privat og offentlig sektor for å øke beskyttelsen av deres nett- og informasjonssystemer, utvikle og forbedre cyberrobusthet og beredskapsressurser, og utvikle ferdigheter og kompetanse på cybersikkerhetsområdet.

4. ENISA skal fremme samarbeid, inkludert informasjonsutveksling og samordning på unionsplan, mellom medlemsstatene, Unionens institusjoner, organer, kontorer og byråer samt relevante berørte parter i privat og offentlig sektor i spørsmål som gjelder cybersikkerhet.

5. ENISA skal bidra til å øke cybersikkerhetskapasiteten på unionsplan for å støtte medlemsstatenes tiltak for å forebygge og reagere på cybertrusler, særlig ved grensekryssende hendelser.

6. ENISA skal fremme bruken av europeisk cybersikkerhetssertifisering med henblikk på å unngå oppsplittingen av det indre markedet. ENISA skal bidra til innføring og opprettholdelse av en europeisk ramme for cybersikkerhetssertifisering i samsvar med avdeling III i denne forordningen, med sikte på å øke gjennomsiktigheten for cybersikkerhet i forbindelse med IKT-produkter, IKT-tjenester og IKT-prosesser, og dermed styrke tilliten til det digitale indre markedet og dets konkurranseevne.

7. ENISA skal fremme et høyt nivå av bevissthet om cybersikkerhet, inkludert cyberhygiene og cyberkompetanse hos borgere, organisasjoner og foretak.

KAPITTEL II

Oppgaver

Artikkel 5

Utvikling og gjennomføring av Unionens politikk og unionsretten

ENISA skal bidra til utviklingen og gjennomføringen av Unionens politikk og unionsretten ved å

1) bistå og gi råd om utvikling og gjennomgåelse av Unionens politikk og unionsretten på cybersikkerhetsområdet og om sektorspesifikke politikk- og lovgivningsinitiativer i spørsmål som gjelder cybersikkerhet, særlig ved å framlegge uavhengige uttalelser og analyser samt utføre forberedende arbeid,

2) bistå medlemsstatene med å gjennomføre Unionens politikk og unionsretten i forbindelse med cybersikkerhet på en konsekvent måte, særlig i forbindelse med direktiv (EU) 2016/1148, blant annet ved å avgi uttalelser, utstede retningslinjer, gi råd og beste praksis om emner som risikohåndtering, hendelsesrapportering og informasjonsutveksling, samt ved å lette utvekslingen av beste praksis mellom vedkommende myndigheter i forbindelse med dette,

3) bistå medlemsstatene og Unionens institusjoner, organer, kontorer og byråer med å utvikle og fremme politikk på cybersikkerhetsområdet som gjelder opprettholdelse av den generelle tilgjengeligheten av eller integriteten til den offentlige kjernen av det åpne internettet,

4) bidra til arbeidet i samarbeidsgruppen i samsvar med artikkel 11 i direktiv (EU) 2016/1148 ved å yte ekspertise og gi bistand,

5) støtte

   a) utviklingen og gjennomføringen av Unionens politikk på området elektronisk identitet og tillitstjenester, særlig ved å bidra med rådgivning og utstedelse av tekniske retningslinjer, samt ved å lette utvekslingen av beste praksis mellom vedkommende myndigheter,

   b) fremmingen av et høyere nivå av sikkerhet i elektronisk kommunikasjon, blant annet ved å bidra med rådgivning og ekspertise, samt ved å lette utvekslingen av beste praksis mellom vedkommende myndigheter,

   c) medlemsstatene ved gjennomføringen av spesifikke cybersikkerhetsaspekter av Unionens politikk og unionsretten om vern av personopplysninger og personvern, blant annet ved å gi råd til Det europeiske personvernråd på anmodning,

6) støtte den regelmessige gjennomgåelsen av Unionens politiske aktiviteter ved å utarbeide en årsrapport om status for gjennomføringen av de respektive rettslige rammene med hensyn til

   a) opplysninger om medlemsstatenes meldinger om hendelser fra de felles kontaktpunktene til samarbeidsgruppen i samsvar med artikkel 10 nr. 3 i direktiv (EU) 2016/1148,

   b) sammendrag av meldinger om brudd på sikkerheten eller tap av integritet som mottas fra tilbydere av tillitstjenester, og som framlegges for ENISA av tilsynsorganene i samsvar med artikkel 19 nr. 3 i europaparlaments- og rådsforordning (EU) nr. 910/2014([23]),

   c) meldinger om sikkerhetshendelser som overføres av tilbydere av offentlige elektroniske kommunikasjonsnett eller offentlig tilgjengelige elektroniske kommunikasjonstjenester, som framlegges for ENISA av vedkommende myndigheter i samsvar med artikkel 40 i direktiv (EU) 2018/1972.

([23]) Europaparlaments- og rådsforordning (EU) nr. 910/2014 av 23. juli 2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked og om oppheving av direktiv 1999/93/EF (EUT L 257 av 28.8.2014, s. 73).

Artikkel 6

Kapasitetsoppbygging

1. ENISA skal bistå

a) medlemsstatene i arbeidet med å forbedre evnen til å forebygge, påvise og analysere cybertrusler og cyberhendelser, og forbedre kapasiteten til å reagere på slike cybertrusler og cyberhendelser ved å gi dem kunnskap og ekspertise,

b) medlemsstatene og Unionens institusjoner, organer, kontorer og byråer med å fastsette og gjennomføre politikk for offentliggjøring av sårbarheter på frivillig grunnlag,

c) Unionens institusjoner, organer, kontorer og byråer i arbeidet med å forbedre evnen til å forebygge, påvise og analysere cybertrusler og cyberhendelser, og forbedre kapasiteten til å reagere på slike cybertrusler og cyberhendelser, særlig gjennom hensiktsmessig støtte til CERT-EU,

d) medlemsstatene med å opprette nasjonale CSIRT-enheter når det bes om det i samsvar med artikkel 9 nr. 5 i direktiv 2016/1148,

e) medlemsstatene med å utarbeide nasjonale strategier for sikkerhet i nett- og informasjonssystemer når det bes om det i samsvar med artikkel 7 nr. 2 i direktiv (EU) 2016/1148, og fremme spredningen av disse strategiene og merke seg framskrittene i gjennomføringen av dem i hele Unionen med henblikk på å fremme beste praksis,

f) Unionens institusjoner med å utarbeide og gjennomgå Unionens strategier for cybersikkerhet, fremme spredningen av dem og følge framskrittene i gjennomføringen av dem,

g) nasjonale CSIRT-enheter og Unionens CSIRT-enheter med å øke sin kapasitet, blant annet ved å fremme dialog og utveksling av informasjon, for å sikre at hver CSIRT-enhet, ut fra den nyeste tekniske utviklingen, har felles minstekrav til kapasiteten og følger beste praksis,

h) medlemsstatene ved regelmessig og minst annethvert år å organisere cybersikkerhetsøvelsene på unionsplan nevnt i artikkel 7 nr. 5, og ved å utarbeide politiske anbefalinger på grunnlag av vurderingen av øvelsene og erfaringene fra dem,

i) relevante offentlige organer ved å tilby opplæring i cybersikkerhet, eventuelt i samarbeid med berørte parter,

j) samarbeidsgruppen med å utveksle beste praksis, særlig med hensyn til medlemsstatenes identifikasjon av ytere av samfunnsviktige tjenester, i samsvar med artikkel 11 nr. 3 bokstav l) i direktiv (EU) 2016/1148, inkludert i forbindelse med gjensidig avhengighet over landegrensene, vedrørende risikoer og hendelser.

2. ENISA skal støtte informasjonsutveksling i og mellom sektorer, særlig i sektorene oppført i vedlegg II til direktiv (EU) 2016/1148, ved å gjøre tilgjengelig beste praksis og gi veiledning om tilgjengelige verktøyer og prosedyrer samt om hvordan reguleringsmessige spørsmål knyttet til informasjonsutveksling kan løses.

Artikkel 7

Driftsmessig samarbeid på unionsplan

1. ENISA skal støtte det driftsmessige samarbeidet mellom medlemsstatene, Unionens institusjoner, organer, kontorer og byråer og mellom berørte parter.

2. ENISA skal samarbeide på driftsmessig nivå og opprette synergier med Unionens institusjoner, organer, kontorer og byråer, inkludert CERT-EU, med de tjenestene som håndterer datakriminalitet og tilsynsmyndighetene som håndterer personvern og vern av personopplysninger, for å behandle spørsmål av felles interesse, blant annet ved å

a) utveksle fagkunnskap og beste praksis,

b) gi råd og utstede retningslinjer om relevante spørsmål knyttet til cybersikkerhet,

c) innføre praktiske ordninger for utføring av bestemte oppgaver, etter samråd med Kommisjonen.

3. ENISA skal ivareta sekretariatfunksjonene for CSIRT-nettet i samsvar med artikkel 12 nr. 2 i direktiv (EU) 2016/1148, og skal i denne egenskapen aktivt støtte informasjonsutvekslingen og samarbeidet mellom nettverkets medlemmer.

4. ENISA skal støtte medlemsstatene i det driftsmessige samarbeidet i CSIRT-nettet ved

a) å gi råd om hvordan de kan forbedre sin kapasitet til å forebygge, påvise og reagere på hendelser og, på anmodning fra en eller flere medlemsstater, gi råd i forbindelse med en bestemt cybertrussel,

b) på anmodning fra en eller flere medlemsstater, å bistå ved vurderingen av hendelser som har en betydelig eller vesentlig innvirkning, ved å levere ekspertise og lette den tekniske håndteringen av slike hendelser, blant annet særlig ved å støtte frivillig utveksling av relevant informasjon og tekniske løsninger mellom medlemsstatene,

c) å analysere sårbarheter og hendelser på grunnlag av offentlig tilgjengelig informasjon eller informasjon som medlemsstatene har framlagt frivillig for dette formålet, og

d) på anmodning fra en eller flere medlemsstater, å gi støtte til tekniske undersøkelser i ettertid i forbindelse med hendelser som har en betydelig eller vesentlig innvirkning som definert i direktiv (EU) 2016/1148.

Ved gjennomføring av disse oppgavene skal ENISA og CERT-EU samarbeide på en strukturert måte for å dra nytte av synergier og unngå dobbeltarbeid.

5. ENISA skal regelmessig organisere cybersikkerhetsøvelser på unionsplan og bistå medlemsstatene og Unionens institusjoner, organer, kontorer og byråer med å organisere cybersikkerhetsøvelser på anmodning fra dem. Slike cybersikkerhetsøvelser på unionsplan kan omfatte tekniske, driftsmessige eller strategiske elementer. ENISA skal annethvert år organisere en omfattende øvelse i stor skala.

Når det er hensiktsmessig skal ENISA også bidra til og hjelpe til med å organisere sektorvise cybersikkerhetsøvelser sammen med relevante organisasjoner som også deltar i cybersikkerhetsøvelser på unionsplan.

6. ENISA skal i nært samarbeid med medlemsstatene utarbeide en regelmessig, detaljert teknisk situasjonsrapport om cybersikkerhet i EU, om hendelser og cybertrusler basert på offentlig tilgjengelig informasjon, sin egen analyse og rapporter som deles av blant annet medlemsstatenes CSIRT-enheter eller de felles kontaktpunktene opprettet ved direktiv (EU) 2016/1148, begge på frivillig grunnlag, EC3 og CERT-EU.

7. ENISA skal bidra til å utvikle en samordnet innsats på unions- og medlemsstatsplan i forbindelse med omfattende grensekryssende hendelser eller kriser knyttet til cybersikkerhet, hovedsakelig ved å

a) samle og analysere rapporter fra nasjonale kilder som er offentlig tilgjengelige eller deles på frivillig grunnlag, med sikte på å bidra til å skape en felles situasjonsbevissthet,

b) sikre en effektiv informasjonsflyt og foreslå eskaleringsordninger mellom CSIRT-nettet og de tekniske og politiske beslutningstakerne på unionsplan,

c) på anmodning lette den tekniske håndteringen av slike hendelser eller kriser, blant annet særlig ved å støtte frivillig utveksling av tekniske løsninger mellom medlemsstatene,

d) støtte Unionens institusjoner, organer, kontorer og byråer og på anmodning medlemsstatene i kommunikasjonen til offentligheten om slike hendelser eller kriser,

e) teste samarbeidsplanene for å reagere på slike hendelser eller kriser på unionsplan og på anmodning støtte medlemsstatene med å teste slike planer på nasjonalt plan.

Artikkel 8

Marked, cybersikkerhetssertifisering og standardisering

1. ENISA skal støtte og fremme utviklingen og gjennomføringen av Unionens politikk for cybersikkerhetssertifisering av IKT-produkter, IKT-tjenester og IKT-prosesser, som fastsatt i avdeling III i denne forordningen, ved å

a) fortløpende overvåke utviklingen innen beslektede standardiseringsområder og anbefale egnede tekniske spesifikasjoner til bruk i utviklingen av europeiske cybersikkerhetssertifiseringsordninger i henhold til artikkel 54 nr. 1 bokstav c) dersom det ikke finnes standarder,

b) utarbeide forslag til europeiske cybersikkerhetssertifiseringsordninger («forslag til ordninger») for IKT-produkter, IKT-tjenester og IKT-prosesser i samsvar med artikkel 49,

c) vurdere vedtatte europeiske cybersikkerhetssertifiseringsordninger i samsvar med artikkel 49 nr. 8.

d) delta i fagfellevurderinger i samsvar med artikkel 59 nr. 4,

e) bistå Kommisjonen med å ivareta sekretariatfunksjonene for ECCG i samsvar med artikkel 62 nr. 5.

2. ENISA skal ivareta sekretariatfunksjonene for cybersikkerhetssertifiseringsgruppen for berørte parter i samsvar med artikkel 22 nr. 4.

3. ENISA skal sammenstille og offentliggjøre retningslinjer og utvikle god praksis med hensyn til cybersikkerhetskravene til IKT-produkter, IKT-tjenester og IKT-prosesser, i samarbeid med nasjonale cybersikkerhetssertifiseringsmyndigheter og bransjen på en formell, strukturert og gjennomsiktig måte.

4. ENISA skal bidra til kapasitetsoppbygging i forbindelse med vurderings- og sertifiseringsprosesser ved å sammenstille og utstede retningslinjer samt gi støtte til medlemsstatene når de ber om det.

5. ENISA skal lette opprettelsen og innføringen av europeiske og internasjonale standarder for risikohåndtering og for sikkerheten til IKT-produkter, IKT-tjenester og IKT-prosesser.

6. ENISA skal i samarbeid med medlemsstatene og bransjen utarbeide råd og retningslinjer for de tekniske områdene i tilknytning til sikkerhetskrav for ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester, samt for allerede eksisterende standarder, inkludert medlemsstatenes nasjonale standarder, på grunnlag av artikkel 19 nr. 2 i direktiv (EU) 2016/1148.

7. ENISA skal utføre og formidle regelmessige analyser av de viktigste tendensene på markedet for cybersikkerhet, både på etterspørsels- og tilbudssiden, med sikte på å fremme cybersikkerhetsmarkedet i Unionen.

Artikkel 9

Kunnskap og informasjon

ENISA skal

a) utføre analyser av ny teknologi og framlegge emnespesifikke vurderinger av de forventede samfunnsmessige, rettslige, økonomiske og reguleringsmessige konsekvensene av teknologiske innovasjoner innen cybersikkerhet,

b) utføre langsiktige strategiske analyser av cybertrusler og cyberhendelser for å identifisere nye tendenser og bidra til å forebygge hendelser,

c) i samarbeid med eksperter fra medlemsstatenes myndigheter og relevante berørte parter gi råd og veiledning og utveksle beste praksis for sikkerheten i nett- og informasjonssystemer, særlig med hensyn til sikkerheten i infrastrukturer som støtter sektorene oppført i vedlegg II til direktiv (EU) 2016/1148, og de som brukes av tilbyderne av digitale tjenester oppført i vedlegg III til det direktivet,

d) gjennom en egen portal samle, organisere og gjøre tilgjengelig for offentligheten informasjon om cybersikkerhet gitt av Unionens institusjoner, organer, kontorer og byråer, og informasjon om cybersikkerhet gitt på frivillig grunnlag av medlemsstatene og berørte parter i privat og offentlig sektor,

e) samle inn og analysere offentlig tilgjengelig informasjon om betydelige hendelser og utarbeide rapporter for å gi veiledning til borgere, organisasjoner og foretak i hele Unionen.

Artikkel 10

Bevisstgjøring og utdanning

ENISA skal

a) øke offentlighetens bevissthet om cybersikkerhetsrisikoer og gi veiledning om god praksis for den enkelte bruker rettet mot borgere, organisasjoner og foretak, inkludert cyberhygiene og cyberkompetanse,

b) i samarbeid med medlemsstatene, Unionens institusjoner, organer, kontorer og byråer og bransjen organisere regelmessige informasjonskampanjer for å øke cybersikkerheten og dens synlighet i Unionen, og oppmuntre til en bred offentlig debatt,

c) bistå medlemsstatene i arbeidet med å øke bevisstheten om cybersikkerhet og fremme utdanning i cybersikkerhet,

d) støtte nærmere samordning og utveksling av beste praksis mellom medlemsstatene når det gjelder bevissthet om og utdanning i cybersikkerhet.

Artikkel 11

Forskning og innovasjon

I forbindelse med forskning og innovasjon skal ENISA

a) gi råd til Unionens institusjoner, organer, kontorer og byråer og medlemsstatene om forskningsbehov og prioriteringer på cybersikkerhetsområdet for å gjøre det mulig å reagere effektivt på foreliggende og nye risikoer og cybertrusler, blant annet om ny og framvoksende informasjons- og kommunikasjonsteknologi, og for å bruke risikoforebyggende teknologi på en effektiv måte,

b) i tilfeller der Kommisjonen har gitt ENISA relevant myndighet til det, delta i gjennomføringsfasen av programmer for finansiering av forskning og innovasjon, eller som støttemottaker,

c) bidra til det strategiske forsknings- og innovasjonsprogrammet på unionsplan på cybersikkerhetsområdet.

Artikkel 12

Internasjonalt samarbeid

ENISA skal bidra til Unionens innsats for å samarbeide med tredjestater og internasjonale organisasjoner samt innenfor relevante rammer for internasjonalt samarbeid for å fremme internasjonalt samarbeid om cybersikkerhetsspørsmål, ved å

a) delta som observatør og delta i organiseringen av internasjonale øvelser når det er hensiktsmessig, og analysere og rapportere til styret om resultatet av slike øvelser,

b) på anmodning fra Kommisjonen lette utvekslingen av beste praksis,

c) på anmodning fra Kommisjonen stille ekspertise til rådighet for Kommisjonen,

d) gi råd og støtte til Kommisjonen i spørsmål som gjelder avtaler om gjensidig anerkjennelse av cybersikkerhetssertifikater med tredjeland, i samarbeid med ECCG, som er opprettet i samsvar med artikkel 62.

KAPITTEL III

Organisering av ENISA

Artikkel 13

ENISAs struktur

ENISAs administrasjons- og ledelsesstruktur skal bestå av

a) et styre,

b) styrets arbeidsutvalg,

c) en daglig leder,

d) en rådgivende gruppe for ENISA,

e) et nettverk av nasjonale kontaktpersoner.

Avsnitt 1

Styret

Artikkel 14

Styrets sammensetning

1. Styret skal bestå av ett medlem utnevnt av hver medlemsstat og to medlemmer av Kommisjonen. Alle medlemmer skal ha stemmerett.

2. Hvert medlem av styret skal ha et varamedlem. Varamedlemmet skal representere medlemmet når medlemmet ikke er til stede.

3. Styremedlemmer og deres varamedlemmer skal utnevnes på bakgrunn av sine kunnskaper på cybersikkerhetsområdet, idet det tas hensyn til deres relevante ledelses-, administrasjons- og budsjettferdigheter. For å sikre kontinuitet i styrets arbeid skal Kommisjonen og medlemsstatene bestrebe seg på å begrense utskiftingen av sine representanter i styret. Kommisjonen og medlemsstatene skal ta sikte på å oppnå en jevn kjønnsfordeling i styret.

4. Mandatperioden for styremedlemmene og deres varamedlemmer skal være fire år. Denne perioden kan fornyes.

Artikkel 15

Styrets funksjoner

1. Styret skal

a) fastsette de generelle retningslinjene for driften av ENISA og sikre at ENISA utfører sine oppgaver i samsvar med reglene og prinsippene i denne forordningen; det skal også sikre at ENISAs arbeid er i samsvar med virksomhet som utøves av medlemsstatene og på unionsplan,

b) vedta ENISAs utkast til det samlede programdokumentet nevnt i artikkel 24 før det framlegges for Kommisjonen til uttalelse,

c) vedta ENISAs samlede programdokument idet det tas hensyn til Kommisjonens uttalelse,

d) føre tilsyn med gjennomføringen av den flerårige og årlige programplanleggingen som inngår i det samlede programdokumentet,

e) vedta ENISAs årsbudsjett og utøve andre funksjoner i forbindelse med ENISAs budsjett i samsvar med kapittel IV,

f) vurdere og vedta den konsoliderte årsrapporten om ENISAs aktiviteter, inkludert regnskapene og en beskrivelse av hvordan ENISA har oppfylt sine ytelsesindikatorer, framlegge både årsrapporten og vurderingen av denne for Europaparlamentet, Rådet, Kommisjonen og Revisjonsretten senest 1. juli det påfølgende året samt offentliggjøre årsrapporten,

g) vedta de finansielle reglene som får anvendelse på ENISA, i samsvar med artikkel 32,

h) vedta en strategi for bedrageribekjempelse som står i forhold til risikoen for bedrageri, der det tas hensyn til en nytte- og kostnadsanalyse av tiltakene som skal gjennomføres,

i) vedta regler for forebygging og håndtering av interessekonflikter blant styremedlemmene,

j) sikre tilstrekkelig oppfølging av resultatene og anbefalingene fra undersøkelsene til Det europeiske kontor for bedrageribekjempelse (OLAF) og fra ulike interne eller eksterne revisjonsrapporter og vurderinger,

k) vedta sin forretningsorden, inkludert regler for midlertidige beslutninger om delegering av særlige oppgaver i samsvar med artikkel 19 nr. 7,

l) med hensyn til ENISAs personale utøve den myndigheten som ut fra Den europeiske unions vedtekter for tjenestemenn og tjenestevilkårene for andre ansatte i Unionen («vedtektene for tjenestemenn» og «tjenestevilkårene for andre ansatte»), fastsatt i forordning (EØF, Euratom, EKSF) nr. 259/68([24]), er tillagt ansettelsesmyndigheten og den myndigheten som har fullmakt til å inngå arbeidsavtaler («ansettelsesmyndighetens myndighet») i samsvar med nr. 2 i denne artikkelen,

m) vedta regler for å gjennomføre vedtektene for tjenestemenn og tjenestevilkårene for andre ansatte i samsvar med prosedyren i artikkel 110 i vedtektene for tjenestemenn,

n) utnevne den daglige lederen og, dersom det er relevant, forlenge vedkommendes mandatperiode eller avskjedige vedkommende fra sin stilling i samsvar med artikkel 36,

o) utnevne en regnskapsfører, som kan være Kommisjonens regnskapsfører, som skal være helt uavhengig i utførelsen av sine oppgaver,

p) treffe alle beslutninger om opprettelsen av ENISAs interne strukturer og, om nødvendig, endringer av disse, idet det tas hensyn til ENISAs aktivitetsbehov samt forsvarlig budsjettstyring,

q) godkjenne opprettelse av samarbeidsavtaler i samsvar med artikkel 7,

r) godkjenne opprettelse eller inngåelse av samarbeidsavtaler i samsvar med artikkel 42.

2. Styret skal i samsvar med artikkel 110 i vedtektene for tjenestemenn vedta en beslutning med hjemmel i artikkel 2 nr. 1 i vedtektene for tjenestemenn og artikkel 6 i tjenestevilkårene for andre ansatte, som delegerer den relevante ansettelses-myndigheten til daglig leder og fastsetter vilkårene for når denne delegeringen av myndighet kan avbrytes. Daglig leder kan videredelegere denne myndigheten.

([24]) EUT L 56 av 4.3.1968, s. 1.

3. Styret kan, dersom særlige omstendigheter krever det, treffe en beslutning om å midlertidig avbryte delegeringen av ansettelsesmyndigheten til daglig leder og en eventuell videredelegering av denne myndigheten fra daglig leders side, og utøve denne myndigheten selv eller delegere den til ett av sine medlemmer eller til en annen ansatt enn den daglige lederen.

Artikkel 16

Styrets leder

Styret skal med to tredels flertall velge en leder og en nestleder blant sine medlemmer. Deres mandatperiode skal være fire år, og kan fornyes én gang. Dersom deres medlemskap i styret opphører i løpet av mandatperioden, opphører deres mandatperiode automatisk samtidig. Nestlederen skal automatisk ta lederens plass dersom lederen er forhindret fra å ivareta sine plikter.

Artikkel 17

Styrets møter

1. Styrelederen skal innkalle til styremøtene.

2. Styret skal ha minst to ordinære møter i året. Det skal også ha ekstraordinære møter på anmodning fra lederen, på anmodning fra Kommisjonen eller på anmodning fra minst en tredel av medlemmene.

3. Den daglige lederen skal delta på styrets møter, men skal ikke ha stemmerett.

4. Medlemmer av ENISAs rådgivende gruppe kan delta på styremøtene etter invitasjon fra lederen, men skal ikke ha stemmerett.

5. Styremedlemmene og deres varamedlemmer kan, med forbehold for styrets forretningsorden, bistås på styremøtene av rådgivere eller eksperter.

6. ENISA skal ivareta sekretariatfunksjonene for styret.

Artikkel 18

Styrets avstemningsregler

1. Styret skal treffe sine beslutninger med flertall blant sine medlemmer.

2. Det kreves to tredels flertall blant styremedlemmene for å vedta det samlede programdokumentet og årsbudsjettet samt for å utnevne, forlenge mandatperioden for og avsette den daglige lederen.

3. Hvert medlem skal ha én stemme. Ved et medlems fravær skal vedkommendes varamedlem ha rett til å utøve medlemmets stemmerett.

4. Styrets leder skal delta i avstemningene.

5. Den daglige lederen skal ikke delta i avstemningene.

6. I styrets forretningsorden skal det fastsettes mer detaljerte avstemningsregler, særlig for når et medlem kan handle på vegne av et annet medlem.

Avsnitt 2

Styrets arbeidsutvalg

Artikkel 19

Styrets arbeidsutvalg

1. Styret skal bistås av et arbeidsutvalg.

2. Styrets arbeidsutvalg skal

a) forberede beslutninger som skal vedtas av styret,

b) sammen med styret sikre tilstrekkelig oppfølging av resultatene og anbefalingene fra undersøkelsene til OLAF og fra ulike interne eller eksterne revisjonsrapporter og vurderinger,

c) uten at det berører den daglige lederens ansvarsområder som fastsatt i artikkel 20, bistå og gi råd til den daglige lederen ved gjennomføringen av styrets beslutninger om administrative og budsjettmessige spørsmål i samsvar med artikkel 20.

3. Styrets arbeidsutvalg skal bestå av fem medlemmer. Medlemmene av styrets arbeidsutvalg skal utnevnes blant medlemmene av styret. Ett av medlemmene skal være styrets leder, som også kan lede styrets arbeidsutvalg, og et annet medlem skal være en av representantene for Kommisjonen. Utnevnelsen av medlemmene av styrets arbeidsutvalg skal ta sikte på å oppnå en jevn kjønnsfordeling i styret. Den daglige lederen skal delta på møtene i styrets arbeidsutvalg, men skal ikke ha stemmerett.

4. Mandatperioden for medlemmene av styrets arbeidsutvalg skal være to år. Denne perioden kan fornyes.

5. Styrets arbeidsutvalg skal møtes minst én gang hver tredje måned. Arbeidsutvalgets leder skal innkalle til ytterligere møter på anmodning fra utvalgets medlemmer.

6. Styret skal vedta forretningsordenen for styrets arbeidsutvalg.

7. Dersom det er nødvendig av hasteårsaker, kan styrets arbeidsutvalg treffe visse midlertidige beslutninger på vegne av styret, særlig i spørsmål som gjelder den administrative ledelsen, inkludert midlertidig oppheving av delegeringen av ansettelsesmyndighetens myndighet og budsjettspørsmål. Slike midlertidige beslutninger skal snarest meddeles styret. Styret skal deretter beslutte om den midlertidige beslutningen skal godkjennes eller avvises senest tre måneder etter at beslutningen ble truffet. Styrets arbeidsutvalg skal ikke treffe beslutninger på vegne av styret som krever godkjenning av et flertall på to tredeler av styrets medlemmer.

Avsnitt 3

Daglig leder

Artikkel 20

Den daglige lederens oppgaver

1. ENISA skal ledes av sin daglige leder, som skal være uavhengig i utførelsen av sine oppgaver. Den daglige lederen skal være ansvarlig overfor styret.

2. Den daglige lederen skal på anmodning rapportere til Europaparlamentet om utøvelsen av sitt arbeid. Rådet kan be den daglige lederen om å rapportere om utøvelsen av sitt arbeid.

3. Den daglige lederen skal ha ansvar for

a) den daglige administrasjonen av ENISA,

b) å gjennomføre beslutningene truffet av styret,

c) å utarbeide utkastet til det samlede programdokumentet og framlegge det for styret for godkjenning før det framlegges for Kommisjonen,

d) å gjennomføre det samlede programdokumentet og rapportere til styret om dette,

e) å utarbeide den konsoliderte årsrapporten om ENISAs aktiviteter, inkludert gjennomføringen av ENISAs årlige arbeidsprogram, og framlegge den for styret for vurdering og vedtakelse,

f) å utarbeide en handlingsplan for oppfølging av konklusjonene i etterfølgende vurderinger og framlegge en framdrifts-rapport for Kommisjonen annethvert år,

g) å utarbeide en handlingsplan for oppfølging av konklusjonene i interne og eksterne revisjonsrapporter, samt undersøkelser utført av OLAF, og framlegge en framdriftsrapport annethvert år for Kommisjonen og regelmessig for styret,

h) å utarbeide et utkast til de finansielle reglene som får anvendelse på ENISA, som nevnt i artikkel 32,

i) å utarbeide et utkast til overslag over inntekter og utgifter for ENISA og gjennomføre ENISAs budsjett,

j) å verne Unionens økonomiske interesser gjennom tiltak for å forebygge bedrageri, korrupsjon og annen ulovlig virksomhet, gjennom effektiv kontroll og, dersom uregelmessigheter avdekkes, gjennom inndrivelse av urettmessig utbetalte beløp samt, når det er hensiktsmessig, gjennom administrative og økonomiske sanksjoner som er virkningsfulle, står i forhold til overtredelsen og virker avskrekkende,

k) å utarbeide en strategi for bedrageribekjempelse for ENISA og framlegge den for styret for godkjenning,

l) å opprette og opprettholde kontakt med næringslivet og forbrukersammenslutninger for å sikre en løpende dialog med berørte parter,

m) å utveksle synspunkter og informasjon regelmessig med Unionens institusjoner, organer, kontorer og byråer om deres aktiviteter på cybersikkerhetsområdet for å sikre at Unionens politikk utvikles og gjennomføres på en konsekvent måte,

n) å utføre andre oppgaver som den daglige lederen er pålagt ved denne forordningen.

4. Når det er nødvendig og innenfor rammen av ENISAs mål og oppgaver, kan den daglige lederen opprette midlertidige arbeidsgrupper sammensatt av eksperter, inkludert eksperter fra medlemsstatenes vedkommende myndigheter. Den daglige lederen skal informere styret om dette på forhånd. Prosedyrene for å fastsette særlig sammensetningen av disse arbeidsgruppene, den daglige lederens utpeking av eksperter og arbeidsgruppenes arbeid skal angis i ENISAs interne driftsregler.

5. Når det er nødvendig for at ENISA skal kunne utføre sine oppgaver på en effektiv måte og på grunnlag av en hensiktsmessig nytte- og kostnadsanalyse, kan den daglige lederen beslutte å opprette ett eller flere lokale kontorer i en eller flere medlemsstater. Før det besluttes å opprette et lokalt kontor, skal den daglige lederen innhente uttalelse fra de berørte medlemsstatene, inkludert den medlemsstaten der ENISA har sitt sete, og innhente forhåndssamtykke fra Kommisjonen og styret. Ved uenighet under samrådsprosessen mellom den daglige lederen og de berørte medlemsstatene, skal spørsmålet framlegges for Rådet til drøfting. Det samlede antallet ansatte ved alle lokale kontorer skal begrenses til et minimum og skal ikke overstige 40 % av ENISAs samlede antall ansatte i den medlemsstaten der ENISA har sitt sete. Antallet ansatte ved hvert lokale kontor skal ikke overstige 10 % av ENISAs samlede antall ansatte i den medlemsstaten der ENISA har sitt sete.

I beslutningen om å opprette et lokalt kontor skal omfanget av aktivitetene som skal utføres, angis, på en slik måte at unødvendige kostnader og overlapping av ENISAs administrative funksjoner unngås.

Avsnitt 4

ENISAs rådgivende gruppe, cybersikkerhetssertifiseringsgruppen for berørte parter og nettverket av nasjonale kontaktpersoner

Artikkel 21

ENISAs rådgivende gruppe

1. Styret skal, etter forslag fra den daglige lederen, på en gjennomsiktig måte opprette ENISAs rådgivende gruppe sammensatt av anerkjente eksperter som representerer berørte parter, for eksempel IKT-bransjen, leverandører av elektroniske kommunikasjonsnett eller -tjenester som er tilgjengelige for offentligheten, SMB-er, ytere av samfunnsviktige tjenester, forbrukergrupper, eksperter på cybersikkerhetsområdet fra høyskoler og universiteter og representanter for nasjonale reguleringsmyndigheter som er meddelt i samsvar med direktiv (EU) 2018/1972/EF, europeiske standardiseringsorganisasjoner samt rettshåndhevende myndigheter og tilsynsmyndigheter for personvern. Styret skal ta sikte på å oppnå en hensiktsmessig kjønnsfordeling og geografisk fordeling samt en fordeling mellom de forskjellige gruppene av berørte parter.

2. Prosedyrene for ENISAs rådgivende gruppe, særlig når det gjelder gruppens sammensetning, forslaget fra den daglige lederen nevnt i nr. 1, antallet og utnevnelsen av gruppens medlemmer og den rådgivende gruppens arbeid skal angis i ENISAs interne driftsregler og offentliggjøres.

3. ENISAs rådgivende gruppe skal ledes av den daglige lederen eller av en person som den daglige lederen utpeker i hvert enkelt tilfelle.

4. Mandatperioden for medlemmene av ENISAs rådgivende gruppe skal være to og et halvt år. Medlemmer av styret skal ikke være medlemmer av ENISAs rådgivende gruppe. Eksperter fra Kommisjonen og medlemsstatene har rett til å være til stede på møtene i ENISAs rådgivende gruppe og delta i gruppens arbeid. Representanter for andre organer som den daglige lederen anser som relevante, men som ikke er medlemmer av ENISAs rådgivende gruppe, kan inviteres til å være til stede på møtene i ENISAs rådgivende gruppe og delta i gruppens arbeid.

5. ENISAs rådgivende gruppe skal gi råd til ENISA om utførelsen av dets oppgaver, med unntak av anvendelsen av bestemmelsene i avdeling III i denne forordningen. Den skal særlig gi den daglige lederen råd om utarbeidingen av et forslag til ENISAs årlige arbeidsprogram og om hvordan kommunikasjonen sikres med berørte parter i alle spørsmål som gjelder det årlige arbeidsprogrammet.

6. ENISAs rådgivende gruppe skal regelmessig informere styret om sine aktiviteter.

Artikkel 22

Cybersikkerhetssertifiseringsgruppe for berørte parter

1. Det skal opprettes en cybersikkerhetssertifiseringsgruppe for berørte parter.

2. Cybersikkerhetssertifiseringsgruppen for berørte parter skal bestå av medlemmer som velges blant anerkjente eksperter som representerer de relevante berørte partene. Kommisjonen skal, etter en gjennomsiktig og åpen innbydelse etter et forslag fra ENISA, velge ut medlemmer av cybersikkerhetssertifiseringsgruppen for berørte parter, idet det sikres en passende fordeling mellom de ulike gruppene av berørte parter, samt en hensiktsmessig kjønnsfordeling og geografisk fordeling.

3. Cybersikkerhetssertifiseringsgruppen for berørte parter skal

a) gi Kommisjonen råd i strategiske spørsmål om den europeiske rammen for cybersikkerhetssertifisering,

b) på anmodning gi ENISA råd i generelle og strategiske spørsmål om ENISAs oppgaver i tilknytning til markedet, cybersikkerhetssertifisering og standardisering,

c) bistå Kommisjonen ved utarbeidingen av Unionens løpende arbeidsprogram som nevnt i artikkel 47,

d) avgi uttalelse om Unionens løpende arbeidsprogram i samsvar med artikkel 47 nr. 4, og

e) i hastetilfeller gi Kommisjonen og ECCG råd om behovet for ytterligere sertifiseringsordninger som ikke omfattes av Unionens løpende arbeidsprogram, som angitt i artikkel 47 og 48.

4. Sertifiseringsgruppen for berørte parter skal ledes i fellesskap av representantene for Kommisjonen og ENISA, og dens sekretariatfunksjoner skal ivaretas av ENISA.

Artikkel 23

Nettverk av nasjonale kontaktpersoner

1. Styret skal etter forslag fra den daglige lederen opprette et nettverk av nasjonale kontaktpersoner som består av representanter for alle medlemsstater (nasjonale kontaktpersoner). Hver medlemsstat skal oppnevne én representant til nettverket av nasjonale kontaktpersoner. Møtene i nettverket av nasjonale kontaktpersoner kan holdes i ulike ekspert-sammensetninger.

2. Det nasjonale nettverket av kontaktpersoner skal særlig fremme utvekslingen av informasjon mellom ENISA og medlemsstatene, og støtte ENISA i formidlingen av dets aktiviteter, resultater og anbefalinger til relevante berørte parter i hele Unionen.

3. Nasjonale kontaktpersoner skal fungere som et kontaktpunkt på nasjonalt plan for å lette samarbeidet mellom ENISA og nasjonale eksperter i forbindelse med gjennomføringen av ENISAs årlige arbeidsprogram.

4. De nasjonale kontaktpersonene skal ha et nært samarbeid med de respektive medlemsstatenes representanter i styret, men selve nettverket av nasjonale kontaktpersoner skal ikke utføre arbeid som overlapper arbeidet i styret eller andre fora i Unionen.

5. Funksjonene og prosedyrene til nettverket av nasjonale kontaktpersoner skal angis i ENISAs interne driftsregler og offentliggjøres.

Avsnitt 5

Drift

Artikkel 24

Samlet programdokument

1. ENISA skal utøve sin virksomhet i samsvar med det samlede programdokumentet som inneholder dets årlige og flerårige programplanlegging, og som skal inneholde alle planlagte aktiviteter.

2. Hvert år skal den daglige lederen utarbeide et utkast til et samlet programdokument som inneholder årlig og flerårig programplanlegging med de tilsvarende planene for finansielle ressurser og menneskelige ressurser i samsvar med artikkel 32 i delegert kommisjonsforordning (EU) nr. 1271/2013([25]), samtidig som det tas hensyn til retningslinjene fastsatt av Kommisjonen.

3. Senest 30. november hvert år skal styret vedta det samlede programdokumentet nevnt i nr. 1 og oversende det til Europaparlamentet, Rådet og Kommisjonen senest 31. januar det påfølgende året, sammen med eventuelle senere oppdaterte versjoner av dette dokumentet.

4. Det samlede programdokumentet skal bli endelig etter at Unionens alminnelige budsjett er endelig vedtatt, og skal om nødvendig justeres.

([25]) Delegert kommisjonsforordning (EU) nr. 1271/2013 av 30. september 2013 om det finansielle rammereglement for organene nevnt i artikkel 208 i europaparlaments- og rådsforordning (EU, Euratom) nr. 966/2012 (EUT L 328 av 7.12.2013, s. 42).

5. Det årlige arbeidsprogrammet skal inneholde detaljerte mål og forventede resultater, inkludert ytelsesindikatorer. Det skal også inneholde en beskrivelse av tiltakene som skal finansieres, og en angivelse av de finansielle og menneskelige ressursene som er avsatt til hvert tiltak, i samsvar med prinsippene om aktivitetsbasert budsjettering og ledelse. Det årlige arbeidsprogrammet skal være i samsvar med det flerårige arbeidsprogrammet nevnt i nr. 7. Det skal klart angi hvilke oppgaver som er tilføyd, endret eller slettet i forhold til det foregående regnskapsåret.

6. Styret skal endre det vedtatte årlige arbeidsprogrammet dersom ENISA tildeles en ny oppgave. Alle vesentlige endringer av det årlige arbeidsprogrammet skal vedtas etter samme framgangsmåte som det opprinnelige årlige arbeidsprogrammet. Styret kan delegere myndigheten til å foreta ikke-vesentlige endringer i det årlige arbeidsprogrammet til den daglige lederen.

7. Det flerårige arbeidsprogrammet skal angi den overordnede strategiske programplanleggingen, inkludert mål, forventede resultater og ytelsesindikatorer. Det skal også inneholde informasjon om ressursplanlegging, inkludert flerårig budsjett og personale.

8. Ressursplanleggingen skal oppdateres årlig. Den strategiske programplanleggingen skal oppdateres ved behov, særlig for å ta høyde for resultatet av vurderingen nevnt i artikkel 67.

Artikkel 25

Interesseerklæring

1. Medlemmer av styret, den daglige lederen og tjenestemenn som medlemsstatene midlertidig stiller til rådighet, skal hver og en avgi en forpliktelseserklæring og en erklæring om hvorvidt det foreligger eller ikke foreligger direkte eller indirekte interesser som kan anses å påvirke deres uavhengighet. Erklæringene skal være nøyaktige og fullstendige, avgis skriftlig hvert år og oppdateres ved behov.

2. Medlemmer av styret, den daglige lederen og eksterne eksperter som deltar i midlertidige arbeidsgrupper, skal hver og en, nøyaktig og fullstendig og senest ved begynnelsen av hvert møte, redegjøre for eventuelle interesser som vil kunne anses å påvirke deres uavhengighet med hensyn til punktene på dagsordenen, og skal avstå fra å delta i drøftinger og avstemninger om slike punkter.

3. ENISA skal i sine interne driftsregler fastsette hvordan reglene om interesseerklæringer nevnt i nr. 1 og 2 skal gjennomføres i praksis.

Artikkel 26

Innsyn

1. ENISA skal utføre sitt arbeid med en høy grad av innsyn og i samsvar med artikkel 28.

2. ENISA skal sikre at offentligheten og eventuelle berørte parter får hensiktsmessig, objektiv, pålitelig og lett tilgjengelig informasjon, særlig med hensyn til resultatene av dets arbeid. Det skal også offentliggjøre interesseerklæringer avgitt i samsvar med artikkel 25.

3. Styret kan etter forslag fra den daglige lederen tillate berørte parter å delta som observatører i forbindelse med visse deler av ENISAs aktiviteter.

4. ENISA skal i sine interne driftsregler fastsette hvordan innsynsreglene nevnt i nr. 1 og 2 skal gjennomføres i praksis.

Artikkel 27

Fortrolighet

1. Med forbehold for artikkel 28 skal ENISA ikke bringe videre til tredjeparter opplysninger som det behandler eller mottar, og som det foreligger en begrunnet anmodning om helt eller delvis fortrolig behandling av.

2. Styremedlemmene, den daglige lederen, medlemmene av ENISAs rådgivende gruppe, eksterne eksperter som deltar i midlertidige arbeidsgrupper, og ENISAs personale, inkludert tjenestemenn som midlertidig stilles til rådighet av medlemsstatene, skal være underlagt taushetsplikt som fastsatt i artikkel 339 i TEUV, selv etter at deres funksjoner har opphørt.

3. ENISA skal i sine interne driftsregler fastsette hvordan fortrolighetsreglene nevnt i nr. 1 og 2 skal gjennomføres i praksis.

4. Dersom det er nødvendig for utførelsen av ENISAs oppgaver, skal styret beslutte å tillate ENISA å håndtere gradert informasjon. I så fall skal ENISA, etter avtale med Kommisjonens kontorer, vedta sikkerhetsregler som bygger på sikkerhetsprinsippene i kommisjonsbeslutning (EU, Euratom) 2015/443([26]) og kommisjonsbeslutning (EU, Euratom) 2015/444([27]). Disse sikkerhetsreglene skal omfatte bestemmelser om utveksling, behandling og lagring av gradert informasjon.

Artikkel 28

Tilgang til dokumenter

1. Forordning (EF) nr. 1049/2001 får anvendelse på dokumenter som ENISA innehar.

2. Styret skal innen 28. desember 2019 vedta gjennomføringsregler for forordning (EF) nr. 1049/2001.

3. Beslutninger truffet av ENISA i henhold til artikkel 8 i forordning (EF) nr. 1049/2001 kan klages inn for Det europeiske ombud i samsvar med artikkel 228 i TEUV eller for Den europeiske unions domstol i samsvar med artikkel 263 i TEUV.

KAPITTEL IV

Opprettelse av ENISAs budsjett og budsjettets struktur

Artikkel 29

Opprettelse av ENISAs budsjett

1. Den daglige lederen skal hvert år sette opp et utkast til overslag over ENISAs inntekter og utgifter for det kommende regnskapsåret, og oversende det til styret sammen med et utkast til en stillingsoversikt. Inntekter og utgifter skal være i balanse.

2. Styret skal hvert år, på grunnlag av utkastet til overslag, utarbeide et overslag over ENISAs inntekter og utgifter for det kommende regnskapsåret.

3. Styret skal senest 31. januar hvert år sende dette overslaget, som skal være en del av utkastet til det samlede programdokumentet, til Kommisjonen og de tredjelandene som Unionen har inngått avtaler med som nevnt i artikkel 42 nr. 2.

4. På grunnlag av dette overslaget skal Kommisjonen innta i forslaget til Unionens alminnelige budsjett de overslagene den anser som nødvendige for stillingsoversikten og det bidraget som skal ytes over Unionens alminnelige budsjett, og framlegge dette for Europaparlamentet og Rådet i samsvar med artikkel 314 i TEUV.

5. Europaparlamentet og Rådet skal godkjenne bevilgningene i form av bidraget fra Unionen til ENISA.

6. Europaparlamentet og Rådet skal vedta ENISAs stillingsoversikt.

([26]) Kommisjonsbeslutning (EU, Euratom) 2015/443 av 13. mars 2015 om sikkerhet i Kommisjonen (EUT L 72 av 17.3.2015, s. 41).
([27]) Kommisjonsbeslutning (EU, Euratom) 2015/444 av 13. mars 2015 om sikkerhetsregler for vern av graderte EU-opplysninger (EUT L 72 av 17.3.2015, s. 53).

7. Styret skal vedta ENISAs budsjett sammen med det samlede programdokumentet. ENISAs budsjett blir endelig etter at Unionens alminnelige budsjett er endelig vedtatt. Styret skal om nødvendig justere ENISAs budsjett og det samlede programdokumentet i samsvar med Unionens alminnelige budsjett.

Artikkel 30

Struktur for ENISAs budsjett

1. Uten at det berører andre ressurser skal ENISAs inntekter bestå av

a) et bidrag fra Unionens alminnelige budsjett,

b) inntekter avsatt til særlige utgiftsposter i samsvar med de finansielle reglene nevnt i artikkel 32,

c) unionsfinansiering i form av delegeringsavtaler eller ad hoc-tilskudd i samsvar med de finansielle reglene nevnt i artikkel 32 og med bestemmelsene i de relevante instrumentene som støtter Unionens politikk,

d) bidrag fra tredjestater som deltar i ENISAs arbeid i samsvar med artikkel 42,

e) eventuelle frivillige bidrag fra medlemsstatene i form av penger eller naturalytelser.

Medlemsstater som gir frivillige bidrag i henhold til første ledd bokstav e), skal ikke kreve noen særlige rettigheter eller tjenester som et resultat av dette.

2. ENISAs utgifter skal omfatte utgifter til personale, administrativ og teknisk bistand, infrastruktur og drift samt utgifter i forbindelse med kontrakter inngått med tredjeparter.

Artikkel 31

Gjennomføring av ENISAs budsjett

1. Den daglige lederen skal være ansvarlig for gjennomføringen av ENISAs budsjett.

2. Kommisjonens interne revisor skal ha samme fullmakter overfor ENISA som overfor Kommisjonens kontorer.

3. ENISAs regnskapsfører skal sende det foreløpige regnskapet for regnskapsåret (år N) til Kommisjonens regnskapsfører og til Revisjonsretten senest 1. mars i det påfølgende regnskapsåret (år N + 1).

4. Etter mottak av Revisjonsrettens merknader om ENISAs foreløpige regnskap i henhold til artikkel 246 i europaparlaments- og rådsforordning (EU, Euratom) 2018/1046([28]), skal ENISAs regnskapsfører på eget ansvar stille opp ENISAs endelige regnskap og framlegge det for styret for uttalelse.

5. Styret skal avgi en uttalelse om ENISAs endelige regnskap.

6. Senest 31. mars i år N + 1 skal den daglige lederen oversende rapporten om budsjett- og økonomistyringen til Europaparlamentet, Rådet, Kommisjonen og Revisjonsretten.

7. Senest 31. juli i år N + 1 skal ENISAs regnskapsfører oversende ENISAs endelige regnskap til Europaparlamentet, Rådet, Kommisjonens regnskapsfører og Revisjonsretten sammen med styrets uttalelse.

([28]) Europaparlaments- og rådsforordning (EU, Euratom) 2018/1046 av 18. juli 2018 om finansielle regler for Unionens alminnelige budsjett, om endring av forordning (EU) nr. 1296/2013, (EU) nr. 1301/2013, (EU) nr. 1303/2013, (EU) nr. 1304/2013, (EU) nr. 1309/2013, (EU) nr. 1316/2013, (EU) nr. 223/2014, (EU) nr. 283/2014 og beslutning nr. 541/2014/EU og om oppheving av forordning (EU, Euratom) nr. 966/2012 (EUT L 193 av 30.7.2018, s. 1).

8. ENISAs regnskapsfører skal på samme dato som oversendelsen av ENISAs endelige regnskap, også sende en erklæring som omfatter dette endelige regnskapet, med kopi til Kommisjonens regnskapsfører.

9. Senest 15. november i år N + 1 skal den daglige lederen offentliggjøre ENISAs endelige regnskap i *Den europeiske unions tidende*.

10. Senest 30. september i år N + 1 skal den daglige lederen sende Revisjonsretten et svar på dens merknader og også sende en kopi av dette svaret til styret og Kommisjonen.

11. Den daglige lederen skal framlegge for Europaparlamentet, på anmodning fra dette, all informasjon som er nødvendig for at framgangsmåten for meddelelse av ansvarsfrihet for det aktuelle regnskapsåret skal kunne gjennomføres på en tilfredsstillende måte, i samsvar med artikkel 261 nr. 3 i forordning (EU, Euratom) 2018/1046.

12. Etter rekommandasjon fra Rådet skal Europaparlamentet før 15. mai i år N + 2 meddele den daglige lederen ansvarsfrihet for gjennomføringen av budsjettet for år N.

Artikkel 32

Finansielle regler

De finansielle reglene som får anvendelse på ENISA, skal vedtas av styret etter samråd med Kommisjonen. De skal ikke avvike fra delegert forordning (EU) nr. 1271/2013, med mindre ENISAs drift særlig krever et slikt avvik og Kommisjonen på forhånd har gitt sitt samtykke.

Artikkel 33

Bedrageribekjempelse

1. For å fremme bekjempelsen av bedrageri, korrupsjon og andre ulovlige handlinger i henhold til europaparlaments- og rådsforordning (EU, Euratom) nr. 883/2013([29]) skal ENISA senest 28. desember 2019 tiltre den tverrinstitusjonelle avtalen av 25. mai 1999 mellom Europaparlamentet, Rådet for Den europeiske union og Kommisjonen for De europeiske fellesskap om interne undersøkelser som foretas av Det europeiske kontor for bedrageribekjempelse (OLAF)([30]). ENISA skal vedta egnede bestemmelser som får anvendelse på alle ansatte i ENISA, ved å bruke malen i vedlegget til nevnte avtale.

2. Revisjonsretten skal ha myndighet til å utføre revisjon, på grunnlag av dokumenter og kontroller på stedet, hos alle tilskuddsmottakere, leverandører og underleverandører som har mottatt unionsmidler fra ENISA.

3. OLAF kan i samsvar med bestemmelsene og framgangsmåtene i forordning (EU, Euratom) nr. 883/2013 og rådsforordning (Euratom, EF) nr. 2185/96([31]), foreta undersøkelser, inkludert kontroller og inspeksjoner på stedet, for å påvise om det har forekommet bedrageri, korrupsjon eller annen ulovlig virksomhet som berører Unionens økonomiske interesser, i forbindelse med et tilskudd eller en kontrakt som er finansiert av ENISA.

4. Uten at det berører nr. 1, 2 og 3 skal ENISAs samarbeidsavtaler med tredjeland og internasjonale organisasjoner, kontrakter, tilskuddsavtaler og tilskuddsbeslutninger inneholde bestemmelser som uttrykkelig gir Revisjonsretten og OLAF myndighet til å utføre slike revisjoner og undersøkelser i samsvar med deres respektive myndigheter.

([29]) Europaparlaments- og rådsforordning (EU, Euratom) nr. 883/2013 av 11. september 2013 om undersøkelser som foretas av Det europeiske kontor for bedrageribekjempelse (OLAF), og om oppheving av europaparlaments- og rådsforordning (EF) nr. 1073/1999 og rådsforordning (Euratom) nr. 1074/1999 (EUT L 248 av 18.9.2013, s. 1).

([30]) EFT L 136 av 31.5.1999, s. 15.

([31]) Rådsforordning (EF, Euratom) nr. 2185/96 av 11. november 1996 om kontroll og inspeksjon på stedet som foretas av Kommisjonen for å verne De europeiske fellesskaps økonomiske interesser mot bedrageri og andre uregelmessigheter (EFT L 292 av 15.11.1996, s. 2).

KAPITTEL V

Personale

Artikkel 34

Alminnelige bestemmelser

Vedtektene for tjenestemenn og tjenestevilkårene for andre ansatte samt reglene som er vedtatt ved avtale mellom Unionens institusjoner for å gjennomføre vedtektene for tjenestemenn og tjenestevilkårene for andre ansatte, får anvendelse på ENISAs personale.

Artikkel 35

Privilegier og immunitet

Protokoll nr. 7 om Den europeiske unions privilegier og immunitet, som er vedlagt TEU og TEUV, får anvendelse på ENISA og dets personale.

Artikkel 36

Daglig leder

1. Den daglige lederen skal ansettes midlertidig i ENISA i samsvar med artikkel 2 bokstav a) i tjenestevilkårene for andre ansatte.

2. Den daglige lederen skal utnevnes av styret fra en liste over kandidater som Kommisjonen har foreslått, etter en åpen utvelgingsprosess med innsynsmulighet.

3. Når arbeidsavtalen med den daglige lederen inngås, skal ENISA representeres av styrets leder.

4. Før utnevnelsen skal kandidaten som styret har valgt, oppfordres til å avgi en erklæring til den relevante komiteen i Europaparlamentet og svare på medlemmenes spørsmål.

5. Den daglige lederens mandatperiode skal være fem år. Ved utgangen av denne perioden skal Kommisjonen foreta en vurdering av den daglige lederens utførelse av arbeidsoppgavene og av ENISAs framtidige oppgaver og utfordringer.

6. Styret skal treffe beslutning om utnevnelse av, forlengelse av mandatperioden for eller avsetting av den daglige lederen i samsvar med artikkel 18 nr. 2.

7. Styret kan på forslag fra Kommisjonen, idet det tas hensyn til vurderingen nevnt i nr. 5, forlenge den daglige lederens mandatperiode én gang med fem år.

8. Styret skal informere Europaparlamentet dersom det har til hensikt å forlenge den daglige lederens mandatperiode. Innen tre måneder før en slik forlengelse og dersom det blir bedt om det, skal den daglige lederen avgi en erklæring til den relevante komiteen i Europaparlamentet og svare på medlemmenes spørsmål.

9. Dersom en daglig leders mandatperiode er blitt forlenget, kan vedkommende ikke delta i en ny utvelgingsprosess til samme stilling.

10. Den daglige lederen kan avsettes bare etter en beslutning truffet av styret etter forslag fra Kommisjonen.

Artikkel 37

Nasjonale eksperter som stilles til rådighet og annet personale

1. ENISA kan benytte seg av nasjonale eksperter som stilles til rådighet eller annet personale som ikke er ansatt av ENISA. Vedtektene for tjenestemenn og tjenestevilkårene for andre ansatte får ikke anvendelse på slikt personale.

2. Styret skal treffe en beslutning om fastsettelse av regler for nasjonale eksperter som stilles til rådighet for ENISA.

KAPITTEL VI

Alminnelige bestemmelser for ENISA

Artikkel 38

ENISAs rettslige status

1. ENISA skal være et unionsorgan og er et eget rettssubjekt.

2. I hver medlemsstat skal ENISA ha den mest omfattende rettslige handleevnen som en juridisk person kan ha i henhold til nasjonal rett. Det kan særlig erverve og avhende løsøre og fast eiendom og være part i en rettssak.

3. ENISA skal være representert ved sin daglige leder.

Artikkel 39

ENISAs ansvar

1. ENISAs ansvar i kontraktsforhold er underlagt den loven som gjelder for den aktuelle kontrakten.

2. Den europeiske unions domstol skal ha myndighet til å treffe beslutning i henhold til en voldgiftsklausul i en kontrakt inngått av ENISA.

3. Ved ansvar utenfor kontraktsforhold skal ENISA erstatte skader som dets personale volder når de utfører sine oppgaver, i samsvar med de alminnelige rettsprinsippene som er felles for medlemsstatenes rettssystemer.

4. Den europeiske unions domstol har myndighet til å avgjøre tvister om erstatning for skader som nevnt i nr. 3.

5. Det personlige ansvaret til ENISAs personale overfor ENISA skal reguleres ved de relevante vilkårene som gjelder for ENISAs personale.

Artikkel 40

Språkordning

1. Rådsforordning nr. 1([32]) får anvendelse på ENISA. Medlemsstatene og andre organer som er utpekt av medlemsstatene, kan henvende seg til ENISA og motta svar på det av de offisielle språkene i Unionens institusjoner som de selv velger.

2. Oversettelsestjenestene som er nødvendige for ENISAs arbeid, skal utføres av Oversettelsessenteret for Den europeiske unions organer.

Artikkel 41

Vern av personopplysninger

1. ENISAs behandling av personopplysninger skal være underlagt forordning (EU) 2018/1725.

2. Styret skal vedta gjennomføringsregler som nevnt i artikkel 45 nr. 3 i forordning (EU) 2018/1725. Styret kan vedta ytterligere tiltak som er nødvendige for ENISAs anvendelse av forordning (EU) 2018/1725.

([32]) Rådsforordning nr. 1 om fastsettelse av reglene for bruk av språk for Det europeiske økonomiske fellesskap (EFT 17 av 6.10.1958, s. 385/58).

Artikkel 42

Samarbeid med tredjestater og internasjonale organisasjoner

1. I den grad det er nødvendig for å nå målene fastsatt i denne forordningen, kan ENISA samarbeide med de vedkommende myndighetene i tredjeland eller med internasjonale organisasjoner, eller begge. ENISA kan for dette formålet opprette samarbeidsavtaler med myndighetene i tredjeland og internasjonale organisasjoner, med forbehold for forhåndsgodkjenning fra Kommisjonen. Disse samarbeidsavtalene skal ikke medføre rettslige forpliktelser for Unionen og dens medlemsstater.

2. ENISA skal være åpent for deltakelse fra tredjeland som har inngått avtaler med Unionen om dette. I samsvar med de relevante bestemmelsene i avtalene skal det utarbeides samarbeidsavtaler som blant annet angir arten og omfanget av disse tredjelandenes deltakelse i ENISAs arbeid, samt på hvilken måte deltakelsen skal skje, inkludert bestemmelser om deltakelse i ENISAs initiativer, om finansielle bidrag og om personale. Når det gjelder personalspørsmål skal disse samarbeidsavtalene under alle omstendigheter være i samsvar med vedtektene for tjenestemenn og tjenestevilkårene for andre ansatte.

3. Styret skal vedta en strategi for forbindelser med tredjeland og internasjonale organisasjoner når det gjelder saker som hører inn under ENISAs myndighetsområde. Kommisjonen skal sikre at ENISA arbeider innenfor rammen av sitt mandat og den eksisterende institusjonelle rammen ved å inngå passende samarbeidsavtaler med den daglige lederen.

Artikkel 43

Sikkerhetsregler for vern av sensitiv ikke-gradert informasjon og gradert informasjon

Etter samråd med Kommisjonen skal ENISA vedta sikkerhetsregler som bygger på sikkerhetsprinsippene i Kommisjonens sikkerhetsregler for vern av sensitiv ikke-gradert informasjon og EUCI, som fastsatt i beslutning (EU, Euratom) 2015/443 og 2015/444. ENISAs sikkerhetsregler skal omfatte bestemmelser om utveksling, behandling og lagring av slik informasjon.

Artikkel 44

Vertsstatsavtale og driftsforhold

1. De nødvendige bestemmelsene med hensyn til lokalene og ressursene som skal stilles til rådighet for ENISA i vertsstaten samt de særlige reglene i vertsstaten som får anvendelse på den daglige lederen, medlemmene av styret, ENISAs personale og deres familiemedlemmer, skal fastsettes i en vertsstatsavtale mellom ENISA og vertsstaten, som er inngått etter at styret har godkjent den.

2. ENISAs vertsstat skal sørge for best mulige vilkår for å sikre at ENISA fungerer på en tilfredsstillende måte, idet det tas hensyn til beliggenheten, tilbud om tilfredsstillende utdanningsinstitusjoner for de ansattes barn samt tilstrekkelig tilgang til arbeidsmarkedet, trygdeordninger og helsetilbud for de ansattes barn og ektefeller.

Artikkel 45

Administrativ kontroll

ENISAs drift skal underlegges tilsyn av Det europeiske ombud i samsvar med artikkel 228 i TEUV.

AVDELING III

RAMME FOR CYBERSIKKERHETSSERTIFISERING

Artikkel 46

Europeisk ramme for cybersikkerhetssertifisering

1. Den europeiske rammen for cybersikkerhetssertifisering skal opprettes for å bedre vilkårene for det indre markedets virkemåte ved å øke cybersikkerhetsnivået i Unionen og muliggjøre en harmonisert tilnærming på unionsplan til europeiske cybersikkerhetssertifiseringsordninger, med sikte på å skape et digitalt indre marked for IKT-produkter, IKT-tjenester og IKT-prosesser.

2. Den europeiske rammen for cybersikkerhetssertifisering skal fastsette en mekanisme for opprettelse av europeiske cybersikkerhetssertifiseringsordninger og for å sikre at IKT-produkter, IKT-tjenester og IKT-prosesser som er vurdert i samsvar med slike ordninger, oppfyller særlige sikkerhetskrav som har som mål å beskytte tilgjengeligheten, autentisiteten, integriteten eller fortroligheten til lagrede, overførte eller behandlede data eller til funksjoner eller tjenester som tilbys i eller er tilgjengelige via disse produktene, tjenestene og prosessene gjennom hele deres livssyklus.

Artikkel 47

Unionens løpende arbeidsprogram for europeisk cybersikkerhetssertifisering

1. Kommisjonen skal offentliggjøre Unionens løpende arbeidsprogram for europeisk cybersikkerhetssertifisering (heretter kalt «Unionens løpende arbeidsprogram») som skal angi de strategiske prioriteringene for framtidige europeiske cybersikkerhetssertifiseringsordninger.

2. Unionens løpende arbeidsprogram skal særlig omfatte en liste over IKT-produkter, IKT-tjenester og IKT-prosesser eller kategorier av disse som kan ha fordel av å omfattes av en europeisk cybersikkerhetssertifiseringsordning.

3. Inkludering av bestemte IKT-produkter, IKT-tjenester og IKT-prosesser eller kategorier av disse i Unionens løpende arbeidsprogram skal begrunnes med ett eller flere av følgende forhold:

a) Tilgjengeligheten og utviklingen av nasjonale cybersikkerhetssertifiseringsordninger som omfatter en bestemt kategori av IKT-produkter, IKT-tjenester eller IKT-prosesser, særlig når det gjelder risikoen for fragmentering.

b) Relevant unionsrett eller unionspolitikk, eller medlemsstatenes nasjonale rett eller politikk.

c) Etterspørselen på markedet.

d) Utviklingen i trusselbildet på cyberområdet.

e) Anmodning om utarbeiding av et spesifikt forslag til ordning fra ECCG.

4. Kommisjonen skal ta behørig hensyn til uttalelsene fra ECCG og sertifiseringsgruppen for berørte parter om utkastet til Unionens løpende arbeidsprogram.

5. Det første av Unionens løpende arbeidsprogrammer skal offentliggjøres innen 28. juni 2020. Unionens løpende arbeidsprogram skal oppdateres minst en gang hvert tredje år og oftere om nødvendig.

Artikkel 48

Anmodning om en europeisk cybersikkerhetssertifiseringsordning

1. Kommisjonen kan be ENISA om å utarbeide et forslag til ordning eller gjennomgå en eksisterende europeisk cybersikkerhetssertifiseringsordning på grunnlag av Unionens løpende arbeidsprogram.

2. I behørig begrunnede tilfeller kan Kommisjonen eller ECCG be ENISA om å utarbeide et forslag til ordning eller gjennomgå en eksisterende europeisk cybersikkerhetssertifiseringsordning som ikke inngår i Unionens løpende arbeidsprogram. Unionens løpende arbeidsprogrammer skal oppdateres i samsvar med dette.

Artikkel 49

Utarbeiding, vedtakelse og revidering av en europeisk cybersikkerhetssertifiseringsordning

1. Etter en anmodning fra Kommisjonen i samsvar med artikkel 48 skal ENISA utarbeide et forslag til ordning som oppfyller kravene i artikkel 51, 52 og 54.

2. Etter en anmodning fra ECCG i samsvar med artikkel 48 nr. 2 kan ENISA utarbeide et forslag til ordning som oppfyller kravene i artikkel 51, 52 og 54. Dersom ENISA avviser en slik anmodning, skal det begrunne sin avvisning. Alle beslutninger om avvisning av en slik anmodning skal treffes av styret.

3. Under utarbeidingen av et forslag til ordning, skal ENISA rådføre seg med alle relevante berørte parter gjennom en formell, åpen, gjennomsiktig og inkluderende samrådsprosess.

4. For hvert forslag til ordning skal ENISA opprette en midlertidig arbeidsgruppe i samsvar med artikkel 20 nr. 4 for å gi ENISA konkrete råd og bidra med ekspertise.

5. ENISA skal ha et nært samarbeid med ECCG. ECCG skal gi ENISA bistand og ekspertrådgivning i forbindelse med utarbeidingen av forslaget til ordning og vedta en uttalelse om forslaget til ordning.

6. ENISA skal ta størst mulig hensyn til uttalelsen fra ECCG før forslaget til ordning som er utarbeidet i samsvar med nr. 3, 4 og 5, oversendes til Kommisjonen. ECCGs uttalelse skal ikke være bindende for ENISA, og fravær av en slik uttalelse skal heller ikke hindre ENISA i å oversende forslaget til ordning til Kommisjonen.

7. Kommisjonen kan, på grunnlag av forslaget til ordning utarbeidet av ENISA, vedta gjennomføringsrettsakter for en europeisk cybersikkerhetssertifiseringsordning for IKT-produkter, IKT-tjenester og IKT-prosesser som oppfyller kravene i artikkel 51, 52 og 54. Disse gjennomføringsrettsaktene skal vedtas i samsvar med undersøkelsesprosedyren nevnt i artikkel 66 nr. 2.

8. ENISA skal minst hvert femte år vurdere hver vedtatt europeisk cybersikkerhetssertifiseringsordning, samtidig som det tas hensyn til tilbakemeldingene fra berørte parter. Om nødvendig kan Kommisjonen eller ECCG be ENISA om å starte prosessen med å utarbeide et revidert forslag til ordning i samsvar med artikkel 48 og denne artikkelen.

Artikkel 50

Nettsted for europeiske cybersikkerhetssertifiseringsordninger

1. ENISA skal ha et eget nettsted som informerer om og offentliggjør europeiske cybersikkerhetssertifiseringsordninger, europeiske cybersikkerhetssertifikater og EU-samsvarserklæringer, inkludert informasjon om europeiske cybersikkerhets-sertifiseringsordninger som ikke lenger er gyldige, inndratte og utløpte europeiske cybersikkerhetssertifikater og EU-samsvarserklæringer, og datalagre med lenker til cybersikkerhetsinformasjon som er gitt i samsvar med artikkel 55.

2. Dersom det er relevant skal nettstedet nevnt i nr. 1 også angi de nasjonale cybersikkerhetssertifiseringsordningene som er blitt erstattet av en europeisk cybersikkerhetssertifiseringsordning.

Artikkel 51

Sikkerhetsmål for europeiske cybersikkerhetssertifiseringsordninger

En europeisk cybersikkerhetssertifiseringsordning skal være utformet for å oppnå, etter hva som er relevant, minst følgende sikkerhetsmål:

a) Å beskytte data som lagres, overføres eller på annen måte behandles mot utilsiktet eller uautorisert lagring, behandling, tilgang eller offentliggjøring i hele livssyklusen til IKT-produktet, IKT-tjenesten eller IKT-prosessen.

b) Å beskytte data som lagres, overføres eller på annen måte behandles mot utilsiktet eller uautorisert tilintetgjøring, tap eller endring eller manglende tilgjengelighet i hele livssyklusen til IKT-produktet, IKT-tjenesten eller IKT-prosessen.

c) At personer med fullmakt, programmer eller maskiner bare kan få tilgang til dataene, tjenestene eller funksjonene som omfattes av deres tilgangsrettigheter.

d) Å identifisere og dokumentere kjente avhengigheter og sårbarheter.

e) Å registrere hvilke data, tjenester eller funksjoner som noen har hatt tilgang til, brukt eller på annen måte behandlet, på hvilke tidspunkter og av hvem.

f) Å gjøre det mulig å kontrollere hvilke data, tjenester eller funksjoner som noen har hatt tilgang til, brukt eller på annen måte behandlet, på hvilke tidspunkter og av hvem.

g) Å verifisere at IKT-produkter, IKT-tjenester og IKT-prosesser ikke inneholder kjente sårbarheter.

h) Å gjenopprette tilgjengeligheten av og tilgangen til data, tjenester og funksjoner i rett tid dersom det oppstår en fysisk eller teknisk hendelse.

i) At IKT-produkter, IKT-tjenester og IKT-prosesser er sikre som standard og gjennom innebygd sikkerhet.

j) At IKT-produkter, IKT-tjenester og IKT-prosesser leveres med oppdatert programvare og maskinvare som ikke inneholder offentlig kjente sårbarheter, og med mekanismer for sikre oppdateringer.

Artikkel 52

Tillitsnivåer for europeiske cybersikkerhetssertifiseringsordninger

1. En europeisk cybersikkerhetssertifiseringsordning kan angi ett eller flere av følgende tillitsnivåer for IKT-produkter, IKT-tjenester og IKT-prosesser: «grunnleggende», «betydelig» eller «høyt». Tillitsnivået skal stå i forhold til det risikonivået som er knyttet til den tiltenkte bruken av IKT-produktet, IKT-tjenesten eller IKT-prosessen hva angår sannsynligheten for og virkningen av en hendelse.

2. Europeiske cybersikkerhetssertifikater og EU-samsvarserklæringer skal vise til alle tillitsnivåer angitt i den europeiske cybersikkerhetssertifiseringsordningen som det europeiske cybersikkerhetssertifikatet eller EU-samsvarserklæringen utstedes på grunnlag av.

3. Sikkerhetskravene som svarer til hvert tillitsnivå, skal fastsettes i den relevante europeiske cybersikkerhets-sertifiseringsordningen, inkludert de tilsvarende sikkerhetsfunksjonene og den tilsvarende nøyaktigheten og grundigheten i vurderingen som IKT-produktet, IKT-tjenesten eller IKT-prosessen skal gjennomgå.

4. Sertifikatet eller EU-samsvarserklæringen skal vise til tekniske spesifikasjoner, standarder og prosedyrer knyttet til dette, inkludert tekniske kontroller, som har som formål å redusere risikoen for eller hindre cybersikkerhetshendelser.

5. Et europeisk cybersikkerhetssertifikat eller en EU-samsvarserklæring som viser til tillitsnivået «grunnleggende», skal gi forsikring om at de IKT-produktene, IKT-tjenestene og IKT-prosessene som sertifikatet eller EU-samsvarserklæringen er utstedt for, oppfyller de tilsvarende sikkerhetskravene, inkludert sikkerhetsfunksjoner, og at de er blitt vurdert på et nivå som har som formål å minimere de kjente grunnleggende risikoene for hendelser og cyberangrep. Vurderingene som skal gjennomføres, skal minst omfatte en gjennomgåelse av den tekniske dokumentasjonen. Dersom en slik gjennomgåelse ikke er hensiktsmessig, skal det utføres en alternativ vurdering med tilsvarende virkning.

6. Et europeisk cybersikkerhetssertifikat som viser til tillitsnivået «betydelig», skal gi forsikring om at de IKT-produktene, IKT-tjenestene og IKT-prosessene som sertifikatet er utstedt for, oppfyller de tilsvarende sikkerhetskravene, inkludert sikkerhetsfunksjoner, og at de er blitt vurdert på et nivå som har som formål å minimere de kjente grunnleggende cybersikkerhetsrisikoene, og risikoen for hendelser og cyberangrep utført av aktører med begrensede ferdigheter og ressurser. Vurderingene som skal gjennomføres, skal minst omfatte følgende: en gjennomgåelse for å påvise fravær av offentlig kjente sårbarheter og testing for å påvise at IKT-produktene, IKT-tjenestene eller IKT-prosessene ivaretar de nødvendige sikkerhetsfunksjonene på korrekt måte. Dersom slike vurderinger ikke er hensiktsmessige, skal det utføres en alternativ vurdering med tilsvarende virkning.

7. Et europeisk cybersikkerhetssertifikat som viser til tillitsnivået «høyt», skal gi forsikring om at de IKT-produktene, IKT-tjenestene og IKT-prosessene som sertifikatet er utstedt for, oppfyller de tilsvarende sikkerhetskravene, inkludert sikkerhetsfunksjoner, og at de er blitt vurdert på et nivå som har som formål å minimere risikoen for avanserte cyberangrep utført av aktører med betydelige ferdigheter og ressurser. Vurderingene som skal gjennomføres, skal minst omfatte følgende: en gjennomgåelse for å påvise fravær av offentlig kjente sårbarheter, testing for å påvise at IKT-produktene, IKT-tjenestene eller IKT-prosessene ivaretar de nødvendige sikkerhetsfunksjonene med den nyeste teknologien, samt en vurdering av deres motstandsdyktighet mot kompetente angripere ved hjelp av inntrengingstester. Dersom slike vurderinger ikke er hensiktsmessige, skal det utføres alternative vurderinger med tilsvarende virkning.

8. En europeisk cybersikkerhetssertifiseringsordning kan fastsette flere vurderingsnivåer avhengig av hvor nøyaktig og grundig den benyttede vurderingsmetoden er. Hvert vurderingsnivå skal tilsvare ett av tillitsnivåene og skal defineres gjennom en egnet kombinasjon av tillitskomponenter.

Artikkel 53

Egenvurdering av samsvar

1. En europeisk cybersikkerhetssertifiseringsordning kan gi produsenten eller leverandøren av IKT-produkter, IKT-tjenester eller IKT-prosesser mulighet til å utføre en egenvurdering av samsvar på eget ansvar. Egenvurdering av samsvar bør bare tillates i forbindelse med IKT-produkter, IKT-tjenester eller IKT-prosesser med lav risiko som tilsvarer tillitsnivået «grunnleggende».

2. Produsenten eller leverandøren av IKT-produkter, IKT-tjenester eller IKT-prosesser kan utstede en EU-samsvarserklæring hvor det angis at de kravene som er fastsatt i ordningen, er oppfylt. Ved å utstede en slik erklæring påtar produsenten eller leverandøren av IKT-produkter, IKT-tjenester eller IKT-prosesser seg ansvaret for at IKT-produktene, IKT-tjenestene eller IKT-prosessene oppfyller kravene fastsatt i den ordningen.

3. Produsenten eller leverandøren av IKT-produkter, IKT-tjenester eller IKT-prosesser skal gjøre EU-samsvarserklæringen, den tekniske dokumentasjonen og all annen relevant informasjon om IKT-produkters og IKT-tjenesters samsvar med ordningen tilgjengelig for den nasjonale cybersikkerhetssertifiseringsmyndigheten nevnt i artikkel 58 i tidsrommet fastsatt i den tilsvarende europeiske cybersikkerhetssertifiseringsordningen. En kopi av EU-samsvarserklæringen skal framlegges for den nasjonale cybersikkerhetssertifiseringsmyndigheten og for ENISA.

4. Utstedelsen av en EU-samsvarserklæring er frivillig, med mindre annet er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett.

5. EU-samsvarserklæringer skal anerkjennes i alle medlemsstater.

Artikkel 54

Elementer i europeiske cybersikkerhetssertifiseringsordninger

1. En europeisk cybersikkerhetssertifiseringsordning skal minst omfatte følgende elementer:

a) Sertifiseringsordningens formål og omfang, inkludert typene eller kategoriene av IKT-produkter, IKT-tjenester og IKT-prosesser som omfattes av ordningen.

b) En klar beskrivelse av formålet med ordningen og hvordan de valgte standardene, vurderingsmetodene og tillitsnivåene samsvarer med behovene til de tiltenkte brukerne av ordningen.

c) Henvisninger til de internasjonale, europeiske eller nasjonale standardene som følges ved vurderingen, eller, dersom slike standarder ikke er tilgjengelige eller ikke er hensiktsmessige, til tekniske spesifikasjoner som oppfyller kravene i vedlegg II til forordning (EU) nr. 1025/2012, eller, dersom slike spesifikasjoner ikke er tilgjengelige, til tekniske spesifikasjoner eller andre cybersikkerhetskrav som er definert i den europeiske cybersikkerhetssertifiseringsordningen.

d) Dersom det er relevant, ett eller flere tillitsnivåer.

e) En angivelse av om egenvurdering av samsvar er tillatt innenfor rammen av ordningen.

f) Dersom det er relevant, særlige eller ytterligere krav som gjelder for samsvarsvurderingsorganer for å sikre at de har teknisk kompetanse til å vurdere cybersikkerhetskravene.

g) De særlige vurderingskriteriene og -metodene som skal brukes, inkludert typer av vurdering, for å vise at sikkerhetsmålene nevnt i artikkel 51 er nådd.

h) Dersom det er relevant, opplysninger som er nødvendige for sertifiseringen og som en søker skal framlegge for eller på annen måte gjøre tilgjengelige for samsvarsvurderingsorganene.

i) Dersom ordningen fastsetter bruk av merker eller etiketter, vilkårene for bruk av slike merker eller etiketter.

j) Reglene for å kontrollere at IKT-produkter, IKT-tjenester og IKT-prosesser oppfyller kravene i de europeiske cybersikkerhetssertifikatene eller EU-samsvarserklæringene, inkludert ordninger for å vise at de angitte cybersikkerhets-kravene fortsatt er oppfylt.

k) Dersom det er relevant, vilkårene for utstedelse, opprettholdelse, videreføring og fornyelse av de europeiske cybersikkerhetssertifikatene samt vilkårene for utvidelse eller reduksjon av sertifiseringens omfang.

l) Reglene om konsekvensene for IKT-produkter, IKT-tjenester og IKT-prosesser som er sertifisert eller som det er utstedt en EU-samsvarserklæring for, men som ikke oppfyller kravene i ordningen.

m) Reglene for hvordan tidligere uoppdagede sårbarheter knyttet til cybersikkerhet i IKT-produkter, IKT-tjenester og IKT-prosesser skal rapporteres og håndteres.

n) Dersom det er relevant, reglene for hvordan samsvarsvurderingsorganer skal oppbevare dokumentasjon.

o) Identifisering av nasjonale eller internasjonale cybersikkerhetssertifiseringsordninger som omfatter samme type eller kategorier av IKT-produkter, IKT-tjenester og IKT-prosesser, sikkerhetskrav, vurderingskriterier og -metoder samt tillitsnivåer.

p) Innholdet i og formatet for de europeiske cybersikkerhetssertifikatene og EU-samsvarserklæringene som skal utstedes.

q) Tidsrommet der EU-samsvarserklæringen, den tekniske dokumentasjonen og all annen relevant informasjon skal gjøres tilgjengelig av produsenten eller leverandøren av IKT-produkter, IKT-tjenester eller IKT-prosesser.

r) Den lengste gyldighetsperioden for europeiske cybersikkerhetssertifikater utstedt i samsvar med ordningen.

s) Politikk for offentliggjøring av europeiske cybersikkerhetssertifikater som er utstedt, endret eller trukket tilbake i samsvar med ordningen.

t) Vilkår for gjensidig anerkjennelse av sertifiseringsordninger med tredjeland.

u) Dersom det er relevant, reglene for en eventuell ordning for fagfellevurdering som er opprettet ved ordningen for de myndighetene eller organene som utsteder europeiske cybersikkerhetssertifikater med tillitsnivået «høyt» i samsvar med artikkel 56 nr. 6. Slike ordninger skal ikke berøre fagfellevurderingen fastsatt i artikkel 59.

v) Formatet og prosedyrene som skal følges av produsenter eller leverandører av IKT-produkter, IKT-tjenester eller IKT-prosesser når de leverer og oppdaterer tilleggsinformasjonen om cybersikkerhet i samsvar med artikkel 55.

2. De angitte kravene i den europeiske cybersikkerhetssertifiseringsordningen skal være i samsvar med alle gjeldende lovfestede krav, særlig krav som følger av harmonisert unionsrett.

3. Dersom det er fastsatt i en bestemt unionsrettsakt, kan et sertifikat eller en EU-samsvarserklæring utstedt i samsvar med en europeisk cybersikkerhetssertifiseringsordning brukes til å vise en formodning om samsvar med kravene i den aktuelle rettsakten.

4. I fravær av harmonisert unionsrett kan medlemsstatenes nasjonale rett også fastsette at en europeisk cybersikkerhets-sertifiseringsordning kan brukes til å etablere formodningen om samsvar med lovfestede krav.

Artikkel 55

Tilleggsinformasjon om cybersikkerhet for sertifiserte IKT-produkter, IKT-tjenester og IKT-prosesser

1. Produsenten eller leverandøren av IKT-produkter, IKT-tjenester eller IKT-prosesser som er sertifisert, eller av IKT-produkter, IKT-tjenester og IKT-prosesser som det er utstedt en EU-samsvarserklæring for, skal offentliggjøre følgende tilleggsinformasjon om cybersikkerhet:

a) Veiledning og anbefalinger for å bistå sluttbrukerne med sikker konfigurasjon, installasjon, ibruktaking, drift og vedlikehold av IKT-produktene eller IKT-tjenestene.

b) Tidsrommet der sluttbrukerne vil bli tilbudt sikkerhetsstøtte, særlig når det gjelder tilgjengeligheten av cybersikkerhets-relaterte oppdateringer.

c) Kontaktinformasjon til produsenten eller leverandøren og aksepterte metoder for mottak av informasjon om sårbarheter fra sluttbrukere og sikkerhetsforskere.

d) En henvisning til nettbaserte datalagre med liste over offentliggjorte sårbarheter knyttet til IKT-produktet, IKT-tjenesten eller IKT-prosessen og til eventuell relevant cybersikkerhetsrådgivning.

2. Informasjonen nevnt i nr. 1 skal være tilgjengelig i elektronisk form og skal fortsatt være tilgjengelig og oppdateres om nødvendig minst inntil det tilsvarende europeiske cybersikkerhetssertifikatet eller den tilsvarende EU-samsvarserklæringen utløper.

Artikkel 56

Cybersikkerhetssertifisering

1. IKT-produkter, IKT-tjenester og IKT-prosesser som er sertifisert i samsvar med en europeisk cybersikkerhets sertifiseringsordning som er vedtatt i samsvar med artikkel 49, skal formodes å oppfylle kravene i den ordningen.

2. Cybersikkerhetssertifiseringen skal være frivillig, med mindre annet er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett.

3. Kommisjonen skal regelmessig vurdere effektiviteten og bruken av de vedtatte europeiske cybersikkerhets-sertifiseringsordningene og hvorvidt en bestemt europeisk cybersikkerhetssertifiseringsordning skal gjøres obligatorisk gjennom relevant unionsrett for å sikre et tilstrekkelig cybersikkerhetsnivå for IKT-produkter, IKT-tjenester og IKT-prosesser i Unionen og forbedre det indre markedets virkemåte. Den første av disse vurderingene skal utføres innen 31. desember 2023, og påfølgende vurderinger skal deretter utføres minst annethvert år. Kommisjonen skal på grunnlag av resultatene av disse vurderingene identifisere de IKT-produktene, IKT-tjenestene og IKT-prosessene som omfattes av en eksisterende sertifiseringsordning, og som skal omfattes av en obligatorisk sertifiseringsordning.

Kommisjonen skal prioritere å fokusere på sektorene oppført i vedlegg II til direktiv (EU) 2016/1148, som skal vurderes senest to år etter vedtakelsen av den første europeiske cybersikkerhetssertifiseringsordningen.

Ved utarbeidingen av vurderingen skal Kommisjonen

a) ta hensyn til virkningen av tiltakene på produsentene eller leverandørene av slike IKT-produkter, IKT-tjenester eller IKT-prosesser og på brukerne med hensyn til kostnadene av disse tiltakene og de samfunnsmessige eller økonomiske fordelene som følge av det forventede økte sikkerhetsnivået for de aktuelle IKT-produktene, IKT-tjenestene eller IKT-prosessene,

b) ta hensyn til eksistensen og gjennomføringen av relevant nasjonal rett i medlemsstatene og i tredjeland,

c) gjennomføre en åpen, gjennomsiktig og inkluderende samrådsprosess med alle berørte parter og medlemsstater,

d) ta hensyn til eventuelle gjennomføringsfrister, overgangstiltak og overgangsperioder, særlig med hensyn til tiltakets mulige innvirkning på produsentene eller leverandørene av IKT-produkter, IKT-tjenester eller IKT-prosesser, inkludert SMB-er,

e) foreslå den raskeste og mest effektive måten som overgangen fra frivillige til obligatoriske sertifiseringsordninger kan gjennomføres på.

4. Samsvarsvurderingsorganene nevnt i artikkel 60 skal utstede europeiske cybersikkerhetssertifikater i samsvar med denne artikkelen som viser til tillitsnivået «grunnleggende» eller «betydelig» på grunnlag av kriterier som inngår i den europeiske cybersikkerhetssertifiseringsordningen som Kommisjonen har vedtatt i samsvar med artikkel 49.

5. Som unntak fra nr. 4 kan en europeisk cybersikkerhetssertifiseringsordning i behørig begrunnede tilfeller fastsette at europeiske cybersikkerhetssertifikater som følger av ordningen, bare skal utstedes av et offentlig organ. Et slik organ skal være ett av følgende:

a) En nasjonal cybersikkerhetssertifiseringsmyndighet som nevnt i artikkel 58 nr. 1.

b) Et offentlig organ som er akkreditert som et samsvarsvurderingsorgan i samsvar med artikkel 60 nr. 1.

6. Dersom en europeisk cybersikkerhetssertifiseringsordning vedtatt i samsvar med artikkel 49 krever tillitsnivået «høyt», skal det europeiske cybersikkerhetssertifikatet innenfor rammen av ordningen bare utstedes av en nasjonal cybersikkerhets-sertifiseringsmyndighet eller, i følgende tilfeller, av et samsvarsvurderingsorgan:

a) Etter forhåndsgodkjenning fra den nasjonale cybersikkerhetssertifiseringsmyndigheten for hvert enkelt europeisk cybersikkerhetssertifikat utstedt av et samsvarsvurderingsorgan.

b) På grunnlag av den nasjonale cybersikkerhetssertifiseringsmyndighetens generelle delegering av oppgaven med å utstede slike europeiske cybersikkerhetssertifikater til et samsvarsvurderingsorgan.

7. Den fysiske eller juridiske personen som framlegger IKT-produkter, IKT-tjenester eller IKT-prosesser for sertifisering, skal gjøre all informasjon som er nødvendig for å utføre sertifiseringen, tilgjengelig for den nasjonale cybersikkerhets-sertifiseringsmyndigheten nevnt i artikkel 58, dersom denne myndigheten er det organet som utsteder det europeiske cybersikkerhetssertifikatet, eller for samsvarsvurderingsorganet nevnt i artikkel 60.

8. Innehaveren av et europeisk cybersikkerhetssertifikat skal informere myndigheten eller organet nevnt i nr. 7 om eventuelle senere påviste sårbarheter eller uregelmessigheter med hensyn til sikkerheten til det sertifiserte IKT-produktet, den sertifiserte IKT-tjenesten eller den sertifiserte IKT-prosessen som kan påvirke oppfyllelsen av kravene knyttet til sertifiseringen. Denne myndigheten eller dette organet skal oversende denne informasjonen uten unødig opphold til den berørte nasjonale cybersikkerhetssertifiseringsmyndigheten.

9. Et europeisk cybersikkerhetssertifikat skal utstedes for det tidsrommet som er fastsatt i den europeiske cyber sikkerhetssertifiseringsordningen, og kan fornyes forutsatt at de relevante kravene fortsatt er oppfylt.

10. Et europeisk cybersikkerhetssertifikat utstedt på grunnlag av denne artikkelen skal anerkjennes i alle medlemsstater.

Artikkel 57

Nasjonale cybersikkerhetssertifiseringsordninger og cybersikkerhetssertifikater

1. Uten at det berører nr. 3 i denne artikkelen, skal nasjonale cybersikkerhetssertifiseringsordninger og de tilknyttede prosedyrene for IKT-produkter, IKT-tjenester og IKT-prosesser som omfattes av en europeisk cybersikkerhets-sertifiseringsordning, opphøre å ha virkning fra datoen fastsatt i gjennomføringsrettsakten vedtatt i samsvar med artikkel 49 nr. 7. Nasjonale cybersikkerhetssertifiseringsordninger og tilknyttede prosedyrer for IKT-produkter, IKT-tjenester og IKT-prosesser som ikke omfattes av en europeisk cybersikkerhetssertifiseringsordning, skal fortsatt bestå.

2. Medlemsstatene skal ikke innføre nye nasjonale cybersikkerhetssertifiseringsordninger for IKT-produkter, IKT-tjenester og IKT-prosesser som allerede omfattes av en gjeldende europeisk cybersikkerhetssertifiseringsordning.

3. Eksisterende sertifikater som ble utstedt i samsvar med nasjonale cybersikkerhetssertifiseringsordninger, og som omfattes av en europeisk cybersikkerhetssertifiseringsordning, skal forbli gyldige fram til sin utløpsdato.

4. For å unngå oppsplitting av det indre markedet skal medlemsstatene informere Kommisjonen og ECCG dersom de har til hensikt å utarbeide nye nasjonale cybersikkerhetssertifiseringsordninger.

Artikkel 58

Nasjonale cybersikkerhetssertifiseringsmyndigheter

1. Hver medlemsstat skal utpeke en eller flere nasjonale cybersikkerhetssertifiseringsmyndigheter på sitt territorium eller, etter avtale med en annen medlemsstat, utpeke en eller flere nasjonale cybersikkerhetssertifiseringsmyndigheter som er etablert i den andre medlemsstaten, til å ha ansvar for tilsynsoppgavene i den utpekende medlemsstaten.

2. Hver medlemsstat skal informere Kommisjonen om identiteten til de utpekte nasjonale cybersikkerhets sertifiseringsmyndighetene. Dersom en medlemsstat utpeker mer enn én myndighet, skal den også informere Kommisjonen om hvilke oppgaver hver av disse myndighetene har fått tildelt.

3. Uten at det berører artikkel 56 nr. 5 bokstav a) og artikkel 56 nr. 6 skal hver nasjonal cybersikkerhets sertifiseringsmyndighet være uavhengig av de enhetene den fører tilsyn med når det gjelder organisering, beslutninger om finansiering, juridisk struktur og beslutningstaking.

4. Medlemsstatene skal sikre at aktivitetene til de nasjonale cybersikkerhetssertifiseringsmyndighetene i forbindelse med utstedelsen av europeiske cybersikkerhetssertifikater nevnt i artikkel 56 nr. 5 bokstav a) og i artikkel 56 nr. 6 er strengt atskilt fra deres tilsynsaktiviteter som fastsatt i denne artikkelen, og at disse aktivitetene utføres uavhengig av hverandre.

5. Medlemsstatene skal sikre at de nasjonale cybersikkerhetssertifiseringsmyndighetene har tilstrekkelige ressurser til å utøve sine myndigheter og utføre sine oppgaver på en effektiv og formålstjenlig måte.

6. For å sikre en effektiv gjennomføring av denne forordningen er det hensiktsmessig at nasjonale cybersikkerhets-sertifiseringsmyndigheter deltar i ECCG på en aktiv, effektiv, formålstjenlig og sikker måte.

7. Nasjonale cybersikkerhetssertifiseringsmyndigheter skal

a) føre tilsyn med og håndheve regler som inngår i europeiske cybersikkerhetssertifiseringsordninger i samsvar med artikkel 54 nr. 1 bokstav j) for å kontrollere at IKT-produkter, IKT-tjenester og IKT-prosesser oppfyller kravene i de europeiske cybersikkerhetssertifikatene som er utstedt på deres respektive territorier, i samarbeid med andre vedkommende markedstilsynsmyndigheter,

b) kontrollere at produsentene eller leverandørene av IKT-produkter, IKT-tjenester eller IKT-prosesser som er etablert på deres respektive territorier, oppfyller og håndhever sine forpliktelser og utfører egenvurdering av samsvar, og særlig kontrollere at produsentene eller leverandørene nevnt i artikkel 53 nr. 2 og 3 og i den tilsvarende europeiske cybersikkerhetssertifiseringsordningen oppfyller og håndhever sine forpliktelser,

c) uten at det berører artikkel 60 nr. 3 aktivt bistå og støtte de nasjonale akkrediteringsorganene med å kontrollere og føre tilsyn med samsvarsvurderingsorganenes aktiviteter for denne forordningens formål,

d) kontrollere og føre tilsyn med aktivitetene til de offentlige organene nevnt i artikkel 56 nr. 5,

e) der det er relevant, godkjenne samsvarsvurderingsorganer i samsvar med artikkel 60 nr. 3 og begrense, midlertidig oppheve eller trekke tilbake eksisterende godkjenning dersom samsvarsvurderingsorganene overtrer kravene i denne forordningen,

f) behandle klager fra fysiske eller juridiske personer i forbindelse med europeiske cybersikkerhetssertifikater utstedt av nasjonale cybersikkerhetssertifiseringsmyndigheter eller europeiske cybersikkerhetssertifikater utstedt av samsvarsvurderingsorganer i samsvar med artikkel 56 nr. 6 eller i forbindelse med EU-samsvarserklæringer utstedt i samsvar med artikkel 53, og skal i relevant omfang undersøke klagens formål og informere klageren om forløpet og utfallet av undersøkelsen innen en rimelig frist,

g) å framlegge en årlig sammendragsrapport om de aktivitetene som er utført ifølge bokstav b), c) og d) i dette nummer eller ifølge nr. 8, for ENISA og ECCG,

h) samarbeide med andre nasjonale cybersikkerhetssertifiseringsmyndigheter eller andre offentlige myndigheter, blant annet ved å utveksle informasjon om mulig manglende samsvar mellom IKT-produkter, IKT-tjenester og IKT-prosesser og kravene i denne forordningen eller kravene i særlige europeiske cybersikkerhetssertifiseringsordninger, og

i) overvåke den relevante utviklingen på cybersikkerhetssertifiseringsområdet.

8. Hver nasjonal cybersikkerhetssertifiseringsmyndighet skal minst ha myndighet til å

a) be samsvarsvurderingsorganer, innehavere av europeiske cybersikkerhetssertifikater og utstedere av EU-samsvarserklæringer om å framlegge all informasjon myndigheten trenger for å utføre sine oppgaver,

b) utføre undersøkelser i form av revisjoner av samsvarsvurderingsorganer, innehavere av europeiske cybersikkerhetssertifikater og utstedere av EU-samsvarserklæringer for å kontrollere at de overholder bestemmelsene i denne avdelingen,

c) treffe egnede tiltak i samsvar med nasjonal rett for å sikre at samsvarsvurderingsorganer, innehavere av europeiske cybersikkerhetssertifikater og utstedere av EU-samsvarserklæringer overholder bestemmelsene i denne forordningen eller i en europeisk cybersikkerhetssertifiseringsordning,

d) få adgang til lokalene hos samsvarsvurderingsorganer eller innehavere av europeiske cybersikkerhetssertifikater, for å gjennomføre undersøkelser i samsvar med unionsretten eller medlemsstatenes prosessrett,

e) i samsvar med nasjonal rett trekke tilbake europeiske cybersikkerhetssertifikater utstedt av nasjonale cybersikkerhetssertifiseringsmyndigheter eller europeiske cybersikkerhetssertifikater utstedt av samsvarsvurderingsorganer i samsvar med artikkel 56 nr. 6, dersom slike sertifikater ikke overholder bestemmelsene i denne forordningen eller i en europeisk cybersikkerhetssertifiseringsordning,

f) ilegge sanksjoner i samsvar med nasjonal rett som fastsatt i artikkel 65, og kreve at overtredelsene av forpliktelsene i denne forordningen umiddelbart opphører.

9. Nasjonale cybersikkerhetssertifiseringsmyndigheter skal samarbeide med hverandre og med Kommisjonen, særlig ved å utveksle informasjon, erfaring og god praksis med hensyn til cybersikkerhetssertifisering og tekniske spørsmål som gjelder cybersikkerhet for IKT-produkter, IKT-tjenester og IKT-prosesser.

Artikkel 59

Fagfellevurdering

1. For å oppnå likeverdige standarder i hele Unionen med hensyn til europeiske cybersikkerhetssertifikater og EU-samsvarserklæringer skal nasjonale cybersikkerhetssertifiseringsmyndigheter fagfellevurderes.

2. Fagfellevurderingen skal utføres på grunnlag av forsvarlige og gjennomsiktige vurderingskriterier og prosedyrer, særlig for strukturelle krav, krav til menneskelige ressurser og prosesser samt fortrolighet og klager.

3. Fagfellevurderingen skal vurdere

a) dersom det er relevant, om aktivitetene til de nasjonale cybersikkerhetssertifiseringsmyndighetene i forbindelse med utstedelsen av europeiske cybersikkerhetssertifikater nevnt i artikkel 56 nr. 5 bokstav a) og i artikkel 56 nr. 6 er strengt atskilt fra deres tilsynsaktiviteter som fastsatt i artikkel 58, og om disse aktivitetene utføres uavhengig av hverandre,

b) prosedyrene for å føre tilsyn med og håndheve reglene for å kontrollere at IKT-produkter, IKT-tjenester og IKT-prosesser overholder europeiske cybersikkerhetssertifikater i samsvar med artikkel 58 nr. 7 bokstav a),

c) prosedyrene for å overvåke og håndheve forpliktelsene til produsenter eller leverandører av IKT-produkter, IKT-tjenester eller IKT-prosesser i samsvar med artikkel 58 nr. 7 bokstav b),

d) prosedyrene for å overvåke, godkjenne og føre tilsyn med samsvarsvurderingsorganenes aktiviteter,

e) dersom det er relevant, om personalet hos myndighetene eller organene som utsteder sertifikater med tillitsnivået «høyt» i samsvar med artikkel 56 nr. 6, har den nødvendige ekspertisen.

4. Fagfellevurdering skal utføres av minst to nasjonale cybersikkerhetssertifiseringsmyndigheter fra andre medlemsstater og Kommisjonen og skal utføres minst hvert femte år. ENISA kan delta i fagfellevurderingen.

5. Kommisjonen kan vedta gjennomføringsrettsakter som fastsetter en plan for fagfellevurdering som dekker et tidsrom på minst fem år, og kriteriene for sammensetningen av gruppen som skal utføre fagfellevurderingen, metoden som skal brukes i fagfellevurderingen, samt tidsplanen, hyppigheten og andre oppgaver i forbindelse med den. Når Kommisjonen vedtar disse gjennomføringstiltakene, skal den ta behørig hensyn til ECCGs synspunkter. Disse gjennomføringsrettsaktene skal vedtas i samsvar med undersøkelsesprosedyren nevnt i artikkel 66 nr. 2.

6. Resultatene av fagfellevurderinger skal undersøkes av ECCG, som skal utarbeide sammendrag som kan offentliggjøres, og ved behov utstede retningslinjer eller anbefalinger om tiltak som de berørte enhetene skal treffe.

Artikkel 60

Samsvarsvurderingsorganer

1. Samsvarsvurderingsorganene skal akkrediteres av de nasjonale akkrediteringsorganene som er utpekt i samsvar med forordning (EF) nr. 765/2008. Slik akkreditering skal utstedes bare dersom samsvarsvurderingsorganet oppfyller kravene i vedlegget til denne forordningen.

2. Dersom et europeisk cybersikkerhetssertifikat utstedes av en nasjonal cybersikkerhetssertifiseringsmyndighet i samsvar med artikkel 56 nr. 5 bokstav a) og artikkel 56 nr. 6, skal sertifiseringsorganet til den nasjonale cybersikkerhetssertifiseringsmyndigheten akkrediteres som et samsvarsvurderingsorgan i samsvar med nr. 1 i denne artikkelen.

3. Dersom europeiske cybersikkerhetssertifiseringsordninger fastsetter særlige eller ytterligere krav i samsvar med artikkel 54 nr. 1 bokstav f), skal bare samsvarsvurderingsorganer som oppfyller disse kravene, ha godkjenning fra den nasjonale cybersikkerhetssertifiseringsmyndigheten til å utføre oppgaver innenfor rammen av slike ordninger.

4. Akkrediteringen nevnt i nr. 1 skal utstedes til samsvarsvurderingsorganene for en periode på høyst fem år og kan fornyes på samme vilkår, forutsatt at samsvarsvurderingsorganet fortsatt oppfyller kravene i denne artikkelen. Nasjonale akkrediteringsorganer skal treffe alle egnede tiltak innenfor en rimelig frist for å begrense, midlertidig oppheve eller tilbakekalle akkrediteringen av et samsvarsvurderingsorgan utstedt i henhold til nr. 1 dersom vilkårene for akkreditering ikke eller ikke lenger oppfylles, eller dersom tiltak truffet av samsvarsvurderingsorganet er i strid med denne forordningen.

Artikkel 61

Melding

1. For hver europeisk cybersikkerhetssertifiseringsordning skal de nasjonale cybersikkerhetssertifiseringsmyndighetene informere Kommisjonen om hvilke samsvarsvurderingsorganer som er akkreditert, og, dersom det er relevant, godkjent i samsvar med artikkel 60 nr. 3 til å utstede europeiske cybersikkerhetssertifikater på angitte tillitsnivåer som nevnt i artikkel 52. De nasjonale cybersikkerhetssertifiseringsmyndighetene skal uten unødig opphold informere Kommisjonen om eventuelle senere endringer av dem.

2. Ett år etter ikrafttredelsen av en europeisk cybersikkerhetssertifiseringsordning skal Kommisjonen offentliggjøre en liste over samsvarsvurderingsorganer som er meldt innenfor rammen av ordningen, i *Den europeiske unions tidende*.

3. Dersom Kommisjonen mottar en melding etter utløpet av perioden nevnt i nr. 2, skal den offentliggjøre endringene av listen over meldte samsvarsvurderingsorganer i *Den europeiske unions tidende* innen to måneder etter datoen for mottak av meldingen.

4. En nasjonal cybersikkerhetssertifiseringsmyndighet kan be Kommisjonen om å fjerne et samsvarsvurderingsorgan som er meldt av medlemsstaten, fra listen nevnt i nr. 2. Kommisjonen skal offentliggjøre de aktuelle endringene i den nevnte listen i *Den europeiske unions tidende* innen én måned etter datoen for mottak av den nasjonale cybersikkerhetssertifiseringsmyndighetens anmodning.

5. Kommisjonen kan vedta gjennomføringsrettsakter som fastsetter vilkår, formater og prosedyrer for meldinger nevnt i nr. 1 i denne artikkelen. Disse gjennomføringsrettsaktene skal vedtas i samsvar med undersøkelsesprosedyren nevnt i artikkel 66 nr. 2.

Artikkel 62

Europeisk cybersikkerhetssertifiseringsgruppe

1. Det skal opprettes en europeisk cybersikkerhetssertifiseringsgruppe («ECCG»).

2. ECCG skal bestå av representanter for nasjonale cybersikkerhetssertifiseringsmyndigheter eller representanter for andre vedkommende nasjonale myndigheter. Et medlem av ECCG skal ikke representere mer enn to medlemsstater.

3. Berørte parter og relevante tredjeparter kan innbys til å delta på ECCGs møter og delta i gruppens arbeid.

4. ECCG skal ha til oppgave

a) å gi råd til og bistå Kommisjonen i dens arbeid for å sikre konsekvent gjennomføring og bruk av denne avdelingen, særlig for Unionens løpende arbeidsprogram, politiske spørsmål om cybersikkerhetssertifisering, samordning av politikken og utarbeiding av europeiske cybersikkerhetssertifiseringsordninger,

b) å bistå, gi råd til og samarbeide med ENISA i forbindelse med utarbeidingen av et forslag til ordning i samsvar med artikkel 49,

c) å vedta en uttalelse om forslag til ordning utarbeidet av ENISA i samsvar med artikkel 49,

d) å be ENISA om å utarbeide et forslag til ordning i samsvar med artikkel 48 nr. 2,

e) å vedta uttalelser rettet til Kommisjonen om vedlikehold og gjennomgåelse av eksisterende europeiske cybersikkerhets sertifiseringsordninger,

f) å undersøke den relevante utviklingen på området cybersikkerhetssertifisering og å utveksle informasjon og god praksis om cybersikkerhetssertifiseringsordninger,

g) å fremme samarbeidet mellom nasjonale cybersikkerhetssertifiseringsmyndigheter innenfor rammen av denne avdelingen gjennom kapasitetsoppbygging og utveksling av informasjon, særlig ved å utarbeide metoder for effektiv utveksling av informasjon om spørsmål som gjelder cybersikkerhetssertifisering,

h) å støtte gjennomføringen av ordninger for fagfellevurdering i samsvar med reglene fastsatt i en europeisk cyber sikkerhetssertifiseringsordning i samsvar med artikkel 54 nr. 1 bokstav u),

i) å lette tilpasningen av europeiske cybersikkerhetssertifiseringsordninger til internasjonalt anerkjente standarder, blant annet ved å gjennomgå eksisterende europeiske cybersikkerhetssertifiseringsordninger og eventuelt gi anbefalinger til ENISA om å samarbeide med relevante internasjonale standardiseringsorganisasjoner for å håndtere utilstrekkeligheter eller mangler i tilgjengelige internasjonalt anerkjente standarder.

5. Kommisjonen skal med bistand fra ENISA lede ECCG, og Kommisjonen skal ivareta sekretariatfunksjonene for ECCG i samsvar med artikkel 8 nr. 1 bokstav e).

Artikkel 63

Rett til å klage

1. Fysiske og juridiske personer skal ha rett til å klage til utstederen av et europeisk cybersikkerhetssertifikat eller, dersom klagen gjelder et europeisk cybersikkerhetssertifikat utstedt av et samsvarsvurderingsorgan som handler i samsvar med artikkel 56 nr. 6, til den berørte nasjonale cybersikkerhetssertifiseringsmyndigheten.

2. Myndigheten eller organet som klagen inngis til, skal informere klageren om saksforløpet og om beslutningen som er truffet, samt om retten til effektive rettsmidler nevnt i artikkel 64.

Artikkel 64

Rett til effektive rettsmidler

1. Uten hensyn til eventuelle administrative rettsmidler eller annen ikke-rettslig prøving skal fysiske og juridiske personer ha rett til effektive rettsmidler ved

a) beslutninger truffet av myndigheten eller organet nevnt i artikkel 63 nr. 1, inkludert om det er relevant, i forbindelse med urettmessig utstedelse, manglende utstedelse eller anerkjennelse av et europeisk cybersikkerhetssertifikat som disse fysiske og juridiske personene innehar,

b) en manglende reaksjon på en klage inngitt til myndigheten eller organet nevnt i artikkel 63 nr. 1.

2. Saker i medfør av denne artikkelen skal bringes inn for domstolene i medlemsstaten der myndigheten eller organet som rettsmidlet søkes brukt mot, befinner seg.

Artikkel 65

Sanksjoner

Medlemsstatene skal fastsette regler for sanksjoner ved overtredelser av denne avdelingen og ved overtredelser av europeiske cybersikkerhetssertifiseringsordninger, og skal treffe alle nødvendige tiltak for å sikre at sanksjonene gjennomføres. De fastsatte sanksjonene skal være virkningsfulle, stå i forhold til overtredelsen og virke avskrekkende. Medlemsstatene skal umiddelbart informere Kommisjonen om disse bestemmelsene og tiltakene og informere den om eventuelle senere endringer som påvirker dem.

AVDELING IV

SLUTTBESTEMMELSER

Artikkel 66

Komitéprosedyre

1. Kommisjonen skal bistås av en komité. Nevnte komité skal være en komité som definert i forordning (EU) nr. 182/2011.

2. Når det vises til dette nummeret, får artikkel 5 nr. 4 bokstav b) i forordning (EU) nr. 182/2011 anvendelse.

Artikkel 67

Vurdering og gjennomgåelse

1. Innen 28. juni 2024 og deretter hvert femte år skal Kommisjonen vurdere konsekvensene, virkningen og effektiviteten av ENISAs arbeid og dets arbeidsmetoder, det eventuelle behovet for å endre ENISAs mandat og de økonomiske følgene av en slik endring. Vurderingen skal ta hensyn til alle tilbakemeldinger mottatt av ENISA om dets aktiviteter. Dersom Kommisjonen anser at fortsatt drift av ENISA ikke lenger er berettiget i lys av de målene, det mandatet og de oppgavene det har fått tildelt, kan Kommisjonen foreslå at denne forordningen endres med hensyn til bestemmelsene knyttet til ENISA.

2. Vurderingen skal også undersøke konsekvensene, virkningen og effektiviteten av bestemmelsene i avdeling III i denne forordningen med hensyn til målene om å sikre et tilstrekkelig cybersikkerhetsnivå for IKT-produkter, IKT-tjenester og IKT-prosesser i Unionen og forbedre det indre markedets virkemåte.

3. Vurderingen skal undersøke om grunnleggende cybersikkerhetskrav for tilgang til det indre markedet er nødvendige for å hindre at IKT-produkter, IKT-tjenester og IKT-prosesser som ikke oppfyller grunnleggende cybersikkerhetskrav, kommer inn på markedet i Unionen.

4. Kommisjonen skal innen 28. juni 2024 og deretter hvert femte år framlegge en rapport om vurderingen sammen med sine konklusjoner til Europaparlamentet, Rådet og styret. Resultatene i rapporten skal offentliggjøres.

Artikkel 68

Oppheving og etterfølgelse

1. Forordning (EU) nr. 526/2013 oppheves med virkning fra 27. juni 2019.

2. Henvisninger til forordning (EU) nr. 526/2013 og til ENISA som opprettet ved den forordningen skal forstås som henvisninger til denne forordningen og til ENISA som opprettet ved denne forordningen.

3. ENISA som opprettet ved denne forordningen etterfølger ENISA som opprettet ved forordning (EU) nr. 526/2013, med hensyn til alle eierskap, avtaler, rettslige forpliktelser, arbeidsavtaler, økonomiske forpliktelser og ethvert økonomisk ansvar. Alle beslutninger truffet av styret og styrets arbeidsutvalg i samsvar med forordning (EU) nr. 526/2013 skal fortsatt være gyldige, forutsatt at de er i samsvar med denne forordningen.

4. ENISA skal opprettes for et ubegrenset tidsrom fra 27. juni 2019.

5. Den daglige lederen som er utnevnt i samsvar med artikkel 24 nr. 4 i forordning (EU) nr. 526/2013, skal fortsette som og utøve sine oppgaver som daglig leder som nevnt i artikkel 20 i denne forordningen i den gjenværende delen av den daglige lederens mandatperiode. De andre vilkårene i vedkommendes avtale skal ikke endres.

6. Medlemmene av styret og deres varamedlemmer utnevnt i samsvar med artikkel 6 i forordning (EU) nr. 526/2013 skal fortsette som styremedlemmer og ivareta styrets funksjoner som nevnt i artikkel 15 i denne forordningen i den gjenværende delen av sin mandatperiode.

Artikkel 69

Ikrafttredelse

1. Denne forordningen trer i kraft den 20. dagen etter at den er kunngjort i *Den europeiske unions tidende*.

2. Artikkel 58, 60, 61, 63, 64 og 65 får anvendelse fra 28. juni 2021.

Denne forordningen er bindende i alle deler og kommer direkte til anvendelse i alle medlemsstater.

Utferdiget i Strasbourg 17. april 2019.

For Europaparlamentet	*For Rådet*
A. TAJANI	G. CIAMBA
President	*Formann*

VEDLEGG

KRAV SOM SAMSVARSVURDERINGSORGANER SKAL OPPFYLLE

Samsvarsvurderingsorganer som ønsker å bli akkreditert, skal oppfylle følgende krav:

1. Et samsvarsvurderingsorgan skal opprettes i samsvar med nasjonal rett og være et rettssubjekt.

2. Et samsvarsvurderingsorgan skal være et tredjepartsorgan som er uavhengig av den organisasjonen eller de IKT-produktene, IKT-tjenestene eller IKT-prosessene det vurderer.

3. Et organ som tilhører en næringslivs- eller yrkesorganisasjon som representerer foretak som deltar i utforming, produksjon, levering, montering, bruk eller vedlikehold av IKT-produkter, IKT-tjenester eller IKT-prosesser som organet vurderer, kan anses å være et samsvarsvurderingsorgan, forutsatt at det er påvist at organet er uavhengig, og at det ikke foreligger interessekonflikter.

4. Samsvarsvurderingsorganene, deres øverste ledelse og de personene som har ansvar for å utføre samsvarsvurderingene, skal ikke være konstruktør, produsent, leverandør, installatør, kjøper, eier, bruker eller vedlikeholder av IKT-produktene, IKT-tjenestene eller IKT-prosessene de vurderer, og skal heller ikke være representant for noen av disse partene. Dette forbudet skal ikke hindre bruk av vurderte IKT-produkter som er nødvendige for samsvarsvurderingsorganets arbeid, eller bruk av slike IKT-produkter til personlige formål.

5. Samsvarsvurderingsorganene, deres øverste ledelse og de personene som har ansvar for å utføre samsvarsvurderingene, skal ikke være direkte involvert i utforming, produksjon eller konstruksjon, markedsføring, installasjon, bruk eller vedlikehold av de IKT-produktene, IKT-tjenestene eller IKT-prosessene de vurderer, og skal heller ikke representere parter som deltar i slike aktiviteter. Samsvarsvurderingsorganene, deres øverste ledelse og de personene som har ansvar for å utføre samsvarsvurderingene, skal ikke delta i noen aktiviteter som kan være i strid med deres uavhengighet eller integritet i forbindelse med samsvarsvurderingen. Dette forbudet gjelder særlig rådgivningstjenester.

6. Dersom et samsvarsvurderingsorgan eies eller drives av en offentlig enhet eller en offentlig institusjon, skal det sikres og dokumenteres at det er uavhengig og at det ikke foreligger interessekonflikter mellom den nasjonale cybersikkerhets-sertifiseringsmyndigheten og samsvarsvurderingsorganet.

7. Samsvarsvurderingsorganene skal sikre at deres datterforetaks eller underleverandørers aktiviteter ikke påvirker fortroligheten, objektiviteten eller upartiskheten med hensyn til organenes samsvarsvurdering.

8. Samsvarsvurderingsorganer og deres personale skal utøve sin samsvarsvurdering med største faglige integritet og ha den nødvendige tekniske kompetansen på det aktuelle området, og de skal ikke utsettes for noen form for press eller påvirkning, særlig av økonomisk art, som kan påvirke deres skjønn eller resultatene av deres samsvarsvurdering, inkludert press og påvirkning av økonomisk art, særlig ikke fra personer eller grupper av personer som har en interesse i resultatene av disse aktivitetene.

9. Et samsvarsvurderingsorgan skal kunne utføre alle de samsvarsvurderingsoppgavene som det er pålagt ifølge denne forordningen, uansett om disse oppgavene utføres av samsvarsvurderingsorganet selv eller på dets vegne og ansvar. Enhver bruk av underleverandører og ethvert samråd med eksternt personale skal behørig dokumenteres, det skal ikke involvere mellommenn, og det skal være gjenstand for en skriftlig avtale som blant annet omfatter fortrolighet og interessekonflikter. Det aktuelle samsvarsvurderingsorganet skal ha det fulle ansvaret for oppgavene som utføres.

10. Et samsvarsvurderingsorgan skal til enhver tid og for hver prosedyre for samsvarsvurdering og hver type, kategori eller underkategori av IKT-produkter, IKT-tjenester eller IKT-prosesser, ha følgende til rådighet:

    a) Personale med teknisk kunnskap og tilstrekkelig og relevant erfaring til å utføre samsvarsvurderingsoppgavene.

    b) Beskrivelser av prosedyrer for samsvarsvurdering som sikrer gjennomsiktighet og mulighet til å gjenta disse prosedyrene. Organet skal ha egnede retningslinjer og prosedyrer for å skille mellom oppgaver det utfører som et meldt organ i samsvar med artikkel 61, og dets andre aktiviteter.

c) Prosedyrer for utøvelsen av aktiviteter som tar behørig hensyn til foretakets størrelse, hvilken sektor det opererer innenfor, dets struktur, hvor kompleks de aktuelle IKT-produktenes, IKT-tjenestenes eller IKT-prosessenes teknologi er, samt produksjonsprosessens masse- eller seriepreg.

11. Et samsvarsvurderingsorgan skal ha de midlene som er nødvendige for å utføre tekniske og administrative oppgaver i forbindelse med samsvarsvurderingen, og det skal ha tilgang til alt nødvendig utstyr og nødvendige innretninger.

12. Personalet med ansvar for å utføre samsvarsvurderinger skal ha

a) solid teknisk og yrkesrettet opplæring som omfatter alle aktiviteter i forbindelse med samsvarsvurdering,

b) tilstrekkelig kunnskap om kravene som gjelder for de samsvarsvurderingene de utfører, og den nødvendige myndigheten til å utføre disse vurderingene,

c) nødvendig kunnskap om og forståelse av gjeldende krav og prøvingsstandarder,

d) nødvendige ferdigheter til å utarbeide sertifikater, protokoller og rapporter som viser at vurderingene er utført.

13. Det skal sikres at samsvarsvurderingsorganene, deres øverste ledelse og de personene som har ansvar for å foreta samsvarsvurderingene, og eventuelle underleverandører, er upartiske.

14. Godtgjøringen til et samsvarsvurderingsorgans øverste ledelse og til de personene som har ansvar for å foreta samsvarsvurderingene, skal ikke være avhengig av antall vurderinger som foretas, eller av resultatet av disse vurderingene.

15. Samsvarsvurderingsorganer skal tegne ansvarsforsikring med mindre medlemsstaten påtar seg erstatningsansvaret i samsvar med nasjonal rett eller medlemsstaten selv er direkte ansvarlig for samsvarsvurderingen.

16. Samsvarsvurderingsorganet og dets personale, komiteer, datterforetak, underleverandører og eventuelle tilknyttede organer eller personale i et samsvarsvurderingsorgans eksterne organer skal ivareta fortroligheten og overholde taushetsplikten med hensyn til all informasjon de innhenter når de utfører sine samsvarsvurderingsoppgaver i samsvar med denne forordningen eller alle internrettslige bestemmelser som gjennomfører den, unntatt når offentliggjøring kreves i samsvar med unionsretten eller medlemsstatenes nasjonale rett som slike personer er underlagt, og unntatt overfor vedkommende myndigheter i de medlemsstatene der aktivitetene utføres. Immaterialrettigheter skal vernes. Samsvarsvurderingsorganet skal ha innført dokumenterte prosedyrer med hensyn til kravene i dette nummeret.

17. Med unntak av nr. 16 skal kravene i dette vedlegget ikke være til hinder for at et samsvarsvurderingsorgan og en person som søker om sertifisering, eller som vurderer å søke om sertifisering, kan utveksle teknisk informasjon og veiledning med hensyn til regelverket.

18. Samsvarsvurderingsorganene skal opptre i samsvar med sammenhengende, rettferdige og rimelige vilkår, idet det tas hensyn til interessene til SMB-er når det gjelder gebyrer.

19. Samsvarsvurderingsorganer skal oppfylle kravene i den relevante standarden som er blitt harmonisert i samsvar med forordning (EF) nr. 765/2008 for akkreditering av samsvarsvurderingsorganer som utfører sertifisering av IKT-produkter, IKT-tjenester eller IKT-prosesser.

20. Samsvarsvurderingsorganene skal sikre at prøvingslaboratoriene som benyttes til samsvarsvurdering, oppfyller kravene i den relevante standarden som er blitt harmonisert i samsvar med forordning (EF) nr. 765/2008 for akkreditering av laboratorier som utfører prøving.