DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT

Prop. 109 LS

(2022–2023)

Proposisjon til Stortinget (forslag til lovvedtak og stortingsvedtak)

Lov om digital sikkerhet (digitalsikkerhetsloven) og samtykke til godkjenning av EØS-komiteens beslutninger nr. 21/2023 og 22/2023 om innlemmelse i EØS-avtalen av direktiv (EU) 2016/1148 og forordningene (EU) 2018/151 og (EU) 2019/881

DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT

Prop. 109 LS

(2022–2023)

Proposisjon til Stortinget (forslag til lovvedtak og stortingsvedtak)

Lov om digital sikkerhet (digitalsikkerhetsloven) og samtykke til godkjenning av EØS-komiteens beslutninger nr. 21/2023 og 22/2023 om innlemmelse i EØS-avtalen av direktiv (EU) 2016/1148 og forordningene (EU) 2018/151 og (EU) 2019/881

Innhold

DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT

Prop. 109 LS

(2022–2023)

Proposisjon til Stortinget (forslag til lovvedtak og stortingsvedtak)

Lov om digital sikkerhet (digitalsikkerhetsloven) og samtykke til godkjenning av EØS-komiteens beslutninger nr. 21/2023 og 22/2023 om innlemmelse i EØS-avtalen av direktiv (EU) 2016/1148 og forordningene (EU) 2018/151 og (EU) 2019/881

Tilråding fra Justis- og beredskapsdepartementet 5. mai 2023, godkjent i statsråd samme dag.
(Regjeringen Støre)

1 Hovedinnholdet i proposisjonen

Justis- og beredskapsdepartementet foreslår i denne proposisjonen en ny lov om digital sikkerhet. I tillegg bes det om Stortingets samtykke til godkjenning av to beslutninger i EØS-komiteen.

Loven bygger på Europaparlaments- og rådsdirektiv (EU) 2016/1148 av 6. juli 2016 om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i hele Unionen (NIS-direktivet). Direktivet og tilhørende gjennomføringsforordning 2018/151 om spesifisering av NIS-direktivet artikkel 16 nr. 1 og nr. 4 (gjennomføringsforordningen) ble besluttet tatt inn i EØS-avtalen 3. februar 2023.

Forslaget til lov om digital sikkerhet er ment å være i samsvar med NIS-direktivet og øvrige sammenlignbare lands nasjonale lovgivning på området.

Loven skal forplikte virksomheter som har en særlig viktig rolle for å opprettholde kritisk samfunnsmessig og økonomisk aktivitet, til å overholde digitale sikkerhetskrav og varsle om alvorlige digitale hendelser. Loven skal bidra med forebyggende sikkerhetstiltak som gjør en virksomhet bedre rustet til å stå imot angrep mot nettverks- og informasjonssystemer de er avhengige av. Videre skal loven sikre planer for håndtering av uønskede hendelser. Loven stiller overordnede krav til sikkerhet og varsling, og virkeområdet er kun angitt i form av hvilke sektorer den gjelder i. Dette forutsetter et underliggende regelverk med tydeligere avgrensinger og konkretiseringer.

Loven inneholder derfor en vid adgang til å fastsette nærmere bestemmelser i forskrift.

Loven etablerer rammeverk for tilsyn med virksomhetene og åpner for ileggelse av pålegg og eventuelt overtredelsesgebyr ved manglende oppfyllelse av pliktene. Myndighetene skal også ta imot varsler om alvorlige digitale hendelser. Departementet legger opp til at eksisterende myndighetsstruktur benyttes i størst mulig grad for å begrense behovet for nye kontaktpunkter for virksomhetene som blir underlagt regelverket, og for at myndigheter som allerede utfører oppgaver som ligner oppgaver denne loven pålegger dem, skal kunne samkjøre disse så langt det er mulig. Departementet mener videre at eksisterende myndigheter også bør føre tilsyn med virksomheter som per i dag ikke er underlagt tilsyn.

Europaparlaments- og rådsforordning (EU) 2019/881 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) ble også besluttet tatt inn i EØS-avtalen 3. februar 2023. Forordningen er planlagt inkorporert i forskrift til denne loven.

Norge deltok i beslutningene i EØS-komiteen med forbehold om Stortingets samtykke, jf. Grunnloven § 26 andre ledd. Det bes på denne bakgrunn om Stortingets samtykke til godkjenning av EØS-komiteens beslutninger om innlemmelse av rettsaktene.

2 Lovforslagets bakgrunn

2.1 Utviklingstendenser

Den omfattende digitaliseringen som preger samfunnsutviklingen er et viktig premiss for effektivisering av samfunnet, verdiskapning og økonomisk vekst. Digitale systemer er sentrale for alle samfunnsfunksjoner. Dersom de digitale systemene feiler, vil det kunne medføre store konsekvenser på alle nivåer i samfunnet. Digital sikkerhet er derfor helt avgjørende for å ivareta velferdssamfunnet, viktige samfunnsfunksjoner og nasjonale interesser. Digital sikkerhet er en avgjørende forutsetning for at digitaliseringen skal lykkes.

Den sikkerhetspolitiske situasjonen i verden er i endring, noe som påvirker det nasjonale trusselbildet og skaper sikkerhetsmessige utfordringer. Med komplekse trusler og verdikjeder blir det avgjørende med helhetlige sikkerhetstiltak og at myndighetene har mulighet til å følge opp og kontrollere at tiltak gjennomføres. De siste årene er det gjennomført flere utredninger og utarbeidet politiske dokumenter om digital sikkerhet, blant annet NOU 2015: 13 *Digital sårbarhet – sikkert samfunn,* Meld. St. 38 (2016–2017) *IKT-sikkerhet – et felles ansvar*, NOU 2018: 14 *IKT-sikkerhet i alle ledd* og nå sist i Meld. St. 9 (2022–2023) *Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet – Så åpent som mulig, så sikkert som nødvendig*. Analysene som inngår i eller ligger til grunn for disse utredningene viser gjennomgående at utfordringene innenfor digital sikkerhet går på tvers av virksomheter, sektorer og landegrenser.

Nasjonal strategi for digital sikkerhet angir mål og prioriteringer som skal ligge til grunn for myndighetenes arbeid med digital sikkerhet. Strategien vektlegger behovet for en målrettet norsk deltagelse i det internasjonale samarbeidet for å styrke den globale digitale sikkerheten. Strategien understøttes av en egen tiltaksoversikt.

IKT-sikkerhetsutvalgets utredning NOU 2018: 14 *IKT-sikkerhet i alle ledd* ble overlevert til Justis- og beredskapsdepartementet 3. desember 2018. Ett av hovedtemaene i utredningen omhandler regulering av digital sikkerhet i norsk rett. Utvalget ble bedt om å vurdere om dagens regulering er hensiktsmessig for å oppnå forsvarlig digital sikkerhet. Utvalget uttaler i denne sammenheng at Norge har en mangelfull regulering av IKT-sikkerhet, og anbefaler derfor at det utarbeides en ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning.

I stortingsmelding Meld. St. 9 (2022–2023) *Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet – Så åpent som mulig, så sikkert som nødvendig* uttaler regjeringen at de ønsker å bruke regulering som virkemiddel på områder innen digital sikkerhet der det gir klare nytteeffekter. Sikkerhetsloven regulerer digital sikkerhet innenfor sitt virkeområde. I meldingen er det varslet at regjeringen vurderer å fremme et forslag til ny lov om digital sikkerhet. Sentralt i dette er ansvarliggjøring av virksomheter innenfor samfunnsområder som har en særlig viktig rolle for opprettholdelsen av samfunnsmessig og økonomisk aktivitet, og å sikre gjennomføring av nasjonale råd og anbefalinger. Revisjonsrapporter fra EU-kommisjonen samt utviklingstrekk og erfaringer fra både Norge og andre EØS-stater vil spille en viktig rolle for hvordan regjeringen ønsker å videreutvikle loven.

Denne loven vil legge til rette for gjennomføringen av NIS-direktivet i norsk rett. Den vil også være et utgangspunkt for videre kravstilling og regulering innen digital sikkerhet. For å synliggjøre fremtidige ambisjoner om videreutvikling av regelverket, har departementet valgt å endre tittelen på loven sammenlignet med høringsnotatet fra «lov om sikkerhet i nettverk og informasjonssystemer», til «lov om digital sikkerhet».

2.2 Begrepsbruk

Det benyttes ulike begreper om digital sikkerhet i forskjellige bransjer og profesjoner. Eksempler er IKT-sikkerhet, cybersikkerhet, digital sikkerhet, informasjonssikkerhet og datasikkerhet. Begrepene er, med nyanseforskjeller, å betrakte som synonymer.

Justis- og beredskapsdepartementet har siden 2013 hatt samordningsansvaret for IKT-sikkerhet i sivil sektor, og gjennomgående brukt begrepet IKT-sikkerhet. Begrepet IKT-sikkerhet oppleves imidlertid av mange som problematisk da det anses å være teknisk orientert som typisk henvender seg til en virksomhets IT-avdeling og ikke til en virksomhets ledelse. Cybersikkerhet er også til dels problematisk da det ikke uten videre er intuitivt hva som inngår i begrepet, og at det ikke er et godt norsk begrep.

I denne proposisjonen benyttes «digital sikkerhet» gjennomgående om beskyttelse av «alt» som er sårbart fordi det er koblet til eller på annen måte avhengig av informasjons- og kommunikasjonsteknologi. Begrepet brukes synonymt med begrepene IKT-sikkerhet og cybersikkerhet. Begrepsvalget er i tråd med *Nasjonal strategi for digital sikkerhet*. Begrepet er lett forståelig, fremtidsrettet og i tråd med faguttrykkene for området ellers, slik som digitale angrep, digitale sårbarheter og digitale utfordringer.

Cybersikkerhetsforordningen benytter gjennomgående begrepet cybersikkerhet. I forordningen artikkel 2 nr. 1 defineres cybersikkerhet som «de aktivitetene som er nødvendige for å beskytte nett- og informasjonssystemer, brukerne av slike systemer og andre personer som berøres av cybertrusler». Forordningen regulerer blant annet cybersikkerhetssertifisering. For å klargjøre lovens elementer som peker tilbake på cybersikkerhetsforordningen, foreslås det at lovbestemmelsen som gir hjemmel til å gjennomføre forordningen benytter «sikkerhetssertifisering av IKT-produkter, IKT-tjenester og IKT-prosesser».

2.3 NIS-direktivet

2.3.1 Innledning

Direktiv (EU) 2016/1148 (NIS-direktivet) ble vedtatt i EU 6. juli 2016 og har som formål å styrke den digitale sikkerheten i EØS. Bakgrunnen for forslaget var at det, innen EU, ikke har vært implementert tilstrekkelige og helhetlige beskyttelsestiltak for å oppnå god nok sikkerhet i nettverks- og informasjonssystemer som er særlig viktige for det indre markeds funksjon. Statene har ulik kvalitet på de beskyttelsestiltak som er implementert, hvilket medfører en fragmentert tilnærming på EU-nivå.

NIS-direktivet omfatter utvalgte virksomheter som leverer tjenester som er viktige for å opprettholde et velfungerende samfunn og næringsliv. Virksomhetene som omfattes av direktivet får i hovedsak to forpliktelser. De skal gjennomføre sikkerhetstiltak som står i et rimelig forhold til den risikoen virksomheten står overfor og de skal varsle om alvorlige digitale hendelser.

Virksomhetene faller i to kategorier. For det første tilbydere av samfunnsviktige tjenester innenfor samfunnssektorene energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur. For det andre tilbydere av digitale tjenester, nærmere bestemt nettbaserte markedsplasser, nettbaserte søkemotorer og skytjenester.

Det stilles strengere krav til sikkerhet for tilbydere av samfunnsviktige tjenester enn for tilbydere av digitale tjenester. En konkretisering av kravene for sistnevnte kategori følger av gjennomføringsforordningen. Dette omtales nærmere i punkt 6 om krav til sikkerhet.

NIS-direktivet gir statene rom for nasjonal tilpasning på flere områder. Direktivet setter minimumskrav til statene når det gjelder både virkeområde og sikkerhetskrav. Det er for eksempel opp til den enkelte stat å inkludere flere samfunnssektorer og å stille strengere sikkerhetskrav enn det som følger av direktivet. Det er imidlertid ikke rom for å inkludere færre samfunnssektorer eller å stille mindre strenge krav.

EU-land har gjennomført direktivet på ulike måter. I Sverige trådte *lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster* i kraft 1. august 2018. I all hovedsak gjelder loven de delene av NIS-direktivet som retter seg mot tilbydere av samfunnsviktige og digitale tjenester. I Danmark er NIS-direktivet implementert gjennom reguleringer i den enkelte sektor. *Lov nr. 437 av 8 mai 2018 om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter m.v.* trådte i kraft 10. mai 2018. Dette lovforslaget implementerer de deler av direktivet som stiller sikkerhetskrav til samtrafikkpunkter. I Storbritannia trådte *The Network and Information Systems Regulations 2018 No. 506* i kraft 10. mai 2018. Regelverket gjelder alle direktivets krav, både de som retter seg mot tilbydere av samfunnsviktige og digitale tjenester, og krav som retter seg mot myndighetene.

I november 2022 vedtok EU direktiv (EU) 2022/2555, et nytt direktiv som opphever NIS1 (NIS2-direktivet). Direktivet er foreløpig ikke tatt inn i EØS-avtalen. Direktivets virkeområde er utvidet ved å legge til nye sektorer, og ved å innføre et størrelsestak slik at alle mellomstore og store bedrifter i utvalgte sektorer omfattes av virkeområdet. Skillet mellom tilbydere av samfunnsviktige tjenester og tilbydere av digitale

tjenester videreføres ikke. Virksomheter blir klassifisert ut fra deres betydning og delt inn i kategorier som henholdsvis grunnleggende og viktige, og underlagt forskjellige tilsynsregimer.

NIS2-direktivet styrker sikkerhetskravene til tilbyderne med en minimumsliste over grunntiltak som må anvendes, og gir mer presise bestemmelser for varsling av hendelser. I tillegg adresseres sikkerheten i forsyningskjeder og leverandørforhold. Flere av endringene i det nye direktivet anses som fornuftige presiseringer av NIS1, blant annet knyttet til presiseringer av varslingskrav. Dersom NIS2 blir tatt inn i EØS-avtalen vil det medføre behov for endringer i lov om digital sikkerhet. Slike endringer vil bli sendt på høring på vanlig måte.

2.3.2 Nasjonale rammeverk for sikkerhet i nettverks- og informasjonssystemer

Etter NIS-direktivets artikler 7, 8 og 9 plikter hver stat å etablere en nasjonal strategi for digital sikkerhet, en nasjonal kompetent sikkerhetsmyndighet, et nasjonalt kontaktpunkt og en nasjonal enhet som skal håndtere digitale sikkerhetshendelser. De nasjonale enhetene som skal håndtere sikkerhetshendelser benevnes i direktivet som såkalte CSIRT som står for «computer security incident response team». Proposisjonen vil i det videre gjennomgående benytte betegnelsen «responsmiljøer» eller «nasjonale responsmiljøer» om CSIRT.

Dersom oppgavene til sikkerhetsmyndigheten og kontaktpunktet er fordelt på flere virksomheter, skal disse samarbeide om gjennomføringen av direktivet, jf. artikkel 10.

2.3.3 Samarbeid mellom statene og de nasjonale responsmiljøene

NIS-direktivet etablerer to internasjonale samarbeidsfora gjennom artiklene 11 og 12. Etter artikkel 11 skal det opprettes en samarbeidsgruppe for strategisk styring (NIS samarbeidsgruppe) med representanter fra statene, EU-kommisjonen og det europeiske byrået for nettverks- og informasjonssikkerhet (ENISA). Samarbeidsgruppen skal blant annet utarbeide en handlingsplan for implementering av direktivet, utarbeide strategiske råd til nettverket av nasjonale responsmiljøer og utveksle bestepraksis om informasjonsdeling relatert til hendelseshåndtering og kapasitetsbygging.

Etter artikkel 12 skal det opprettes et nettverk for nasjonale responsmiljøer bestående av representanter fra de nasjonale responsmiljøene og responsmiljøet i EU (CERT-EU). Nettverket skal fremme raskt og effektivt operativt samarbeid, samt utvikling av tillit mellom statene. EU-kommisjonen deltar som observatør og ENISA står for sekretariatet. Nettverkets arbeidsoppgaver vil blant annet bestå av informasjonsdeling om responsmiljøenes tjenester, operasjoner og samarbeidskapasiteter, informasjonsdeling om hendelser og samarbeid om felles respons mot hendelser.

2.3.4 Sikkerhetstiltak og varsling for tilbydere av samfunnsviktige tjenester

I artikkel 14 stilles det generelle og overordnede krav til sikkerheten hos tilbydere av samfunnsviktige tjenester. Blant annet gjennom innføring av krav om risikostyring skal statene sørge for at tilbydere av samfunnsviktige tjenester iverksetter sikkerhetstiltak som står i et rimelig forhold til risikoen den enkelte tilbyder står overfor. Det skal også iverksettes tiltak for å forebygge og minimere virkningen av hendelser i nettverks- og informasjonssystemer, med henblikk på opprettholdelse av tjenesteleveransen. Se nærmere artikkel 14 nr. 1 og 2.

For å legge til rette for harmonisert gjennomføring av artikkel 14 nr. 1 og 2, skal statene fremme bruk av europeiske og internasjonale standarder. ENISA skal bistå med rådgivning og retningslinjer.

Etter artikkel 14 nr. 3 skal statene sørge for at tilbydere av samfunnsviktige tjenester uten ugrunnet opphold varsler om hendelser som virker betydelig inn på kontinuiteten i de samfunnsviktige tjenestene de yter. Vurderingskriteriene for om innvirkningen er betydelig er listet opp i artikkel 14 nr. 4 bokstav a til c:

- antallet brukere som påvirkes
- hendelsens varighet
- størrelsen på det geografiske området som berøres av hendelsen

Dette betyr altså at det kun skal varsles om hendelser som faktisk innvirker negativt på tjenesteleveransen. Det skal ikke varsles om fare for slik virkning, ei heller kompromittering av konfidensialitet, tilgjengelighet eller integritet der dette ikke har betydning for tjenesteleveransen. Det er den forhåndsbestemte kompetente myndigheten eller det nasjonale responsmiljøet som skal varsles. Dersom hendelsen også fører til brudd på personvernet skal den kompetente myndigheten samarbeide med personvernmyndighetene.

Etter artikkel 15 skal statene sørge for at den utpekte kompetente myndigheten har tilstrekkelig myndighet til å undersøke hvorvidt tilbydere av samfunnsviktige tjenester overholder kravene om sikkerhet etter artikkel 14. Dette innebærer blant annet at myndigheten skal kunne få tilgang til all informasjon som er nødvendig for å kunne undersøke sikkerheten hos tilbyderne og at tilbyderne skal kunne fremskaffe dokumentasjon og resultater fra tidligere tilsyn. I etterkant av en slik undersøkelse av dokumentasjon fra en tilbyder, skal den kompetente myndigheten kunne gi bindende pålegg om retting dersom det er behov.

2.3.5 Sikkerhetstiltak og varsling for tilbydere av digitale tjenester

Etter artikkel 16 skal statene sørge for at tilbydere av digitale tjenester iverksetter sikkerhetstiltak som står i et rimelig forhold til risikoen tilbyderen står overfor. Også overfor denne gruppen tilbydere skal det stilles krav om risikostyring. Det skal også iverksettes tiltak for å forebygge og minimere virkningen av hendelser i nettverks- og informasjonssystemer, med henblikk på opprettholdelse av tjenesteleveransen. Til forskjell fra tilbydere av samfunnsviktige tjenester kan statene, med visse unntak, ikke innføre strengere sikkerhetstiltak for tilbydere av digitale tjenester enn det direktivet legger opp til. Noe av begrunnelsen er at det for tilbydere av digitale tjenester er behov for harmoniserte sikkerhetskrav i EØS. Sikkerhetskravene som stilles til tilbydere av digitale tjenester er spesifisert i gjennomføringsforordningen.

Tilbydere av samfunnsviktige tjenester skal varsle en på forhånd bestemt kompetent myndighet om hendelser som virker betydelig inn på leveringen av en tjeneste som nevnt i vedlegg III og som de tilbyr i EØS, jf. artikkel 16 nr. 3. Etter artikkel 16 nr. 4 bokstav a til e skal det ved vurderingen av om innvirkningen er betydelig legges vekt på:

- antallet brukere som påvirkes
- hendelsens varighet
- størrelsen på det geografiske området som berøres av hendelsen
- omfanget av funksjonalitetssvikten i tjenesten
- omfanget av innvirkningen på økonomisk og samfunnsmessig aktivitet

Etter artikkel 17 skal statene sørge for at den kompetente myndigheten kan agere dersom det er bevist at en tilbyder av digitale tjenester ikke har overholdt kravene i artikkel 16. Dette innebærer blant annet at myndigheten skal kunne få tilgang til all den informasjonen som er nødvendig for å vurdere sikkerhetsnivået hos tilbyderen og kunne kreve retting av ethvert brudd med artikkel 16.

2.4 Gjennomføringsforordningen

Forordning (EU) 2018/151 (gjennomføringsforordningen) ble vedtatt 30. januar 2018 og trådte i kraft 10. mai 2018. Forordningen er vedtatt av EU-kommisjonen med hjemmel i NIS-direktivets artikkel 16 nr. 8. Forordningen gjelder kun for tilbydere av digitale tjenester etter NIS-direktivet og utdyper og presiserer innholdet i kravene som følger av NIS-direktivet.

Forordningens overordnede formål er tilsvarende NIS-direktivet, å oppnå et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i EØS for å forbedre virkemåten til det indre marked. Forordningens mer konkrete formål er å sette tilbydere av digitale tjenester bedre i stand til å treffe de tekniske og organisatoriske tiltak som er tilstrekkelige for å styre sikkerhetsrisiko i nettverks- og informasjonssystemene. Formålet er også å presisere hva som skal vektlegges for å identifisere om virkningen av en hendelse er «betydelig».

Gjennomføringsforordningen er en viktig presisering av overordnede krav for tilbydere av digitale tjenester. Presiseringene knyttet til elementer som skal vektlegges av tilbyderne når de skal etablere et sikkerhetsnivå som står i forhold til risikoen er funksjonelt utformet.

Selv om forordningen kun gjelder tilbydere av digitale tjenester, vil artikkel 3 og 4 om kriterier for å avgjøre hvorvidt en hendelse er betydelig og falle inn under varslingsplikten, også ha veiledende betydning for tilbydere av samfunnsviktige tjenester når det gjelder antall brukere som påvirkes, hendelsens varighet og størrelsen på det geografiske området som berøres. Disse parameterne er felles for tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester.

Gjennomføringsforordningen artikkel 2 spesifiserer hvilke momenter tilbydere av digitale tjenester skal ta i betraktning når de fastsetter og iverksetter tiltak for å garantere et nivå av sikkerhet i nettverks- og informasjonssystemer som benyttes i leveransen av tjenester som nevnt i vedlegg III til NIS-direktivet.

Der NIS-direktivet omtaler sikkerheten i systemer og utstyr i artikkel 16 nr. 1 bokstav a,

presiserer forordningen at dette innebærer systematisk forvalting av nettverks- og informasjonssystemer, fysisk og miljømessig sikkerhet, forsyningssikkerhet og adgangskontroll, jf. artikkel 2 nr. 1.

Der NIS-direktivet omtaler hendelseshåndtering i artikkel 16 nr. 1 bokstav b, presiserer forordningen at det omfatter tiltak som innebærer opprettholdelse og overvåkning av deteksjonsprosesser, prosesser og retningslinjer for rapportering om hendelser, plan for reaksjon på hendelser og vurdering av hendelsenes alvorlighetsgrad, jf. artikkel 2 nr. 2.

I NIS-direktivet artikkel 16 nr. 1 bokstav c omtales håndtering av kontinuitet for tilbydere av digitale tjenester. Ifølge gjennomføringsforordningen artikkel 2 nr. 3 innebærer dette utarbeidelse av beredskapsplanverk og å opprettholde en katastrofeberedskapskapasitet som vurderes og testes jevnlig.

I NIS-direktivet artikkel 16 nr. 1 bokstav d omtales overvåkning, revisjon og testing. Det presiseres i gjennomføringsforordningen artikkel 2 nr. 4 at dette innebærer å gjennomføre planlagte sekvenser for observasjon og målinger, inspeksjoner for å sjekke om retningslinjer etterleves og en prosess for å avdekke mangler i systemers sikkerhetsmekanismer.

I NIS-direktivet artikkel 16 nr. 1 bokstav e vises det til at det skal tas hensyn til overholdelse av anerkjente internasjonale standarder. Ifølge gjennomføringsforordningen artikkel 2 nr. 5 innebærer dette standarder vedtatt av et internasjonalt standardiseringsorgan etter Europaparlamentets og Rådets forordning (EU) 1025/2012. Etter NIS-direktivets artikkel 19 kan det også benyttes andre standarder som er relevante for sikkerheten, herunder også nasjonale.

Gjennomføringsforordningen artikkel 2 nr. 6 stiller krav om at tilbyderne skal kunne fremlegge dokumentasjon om overnevnte som den kompetente myndighet etter NIS-direktivet trenger for å utøve sin kontroll.

Gjennomføringsforordningen artikkel 3 spesifiserer hvilke parametere som skal tas i betraktning for å avgjøre om virkningen av en hendelse er betydelig.

Etter NIS-direktivet artikkel 16 nr. 4 bokstav a skal det tas hensyn til antall berørte brukere som påvirkes av hendelsen, særlig brukere som er avhengige av tjenesten for å kunne yte egne tjenester. Etter gjennomføringsforordningen artikkel 3 nr. 1 bokstav a og b skal tilbydere av digitale tjenester kunne fastslå enten antallet av berørte fysiske og juridiske personer som det er inngått avtale om levering av tjeneste med, eller antallet berørte brukere som har benyttet tjenesten basert på tidligere trafikkdata.

Gjennomføringsforordningen presiserer i artikkel 3 nr. 2 hva som mener med en hendelses «varighet» i NIS-direktivet artikkel 16 nr. 4 bokstav b. Med varighet forstås tidsrommet fra avbrytelse av tjenesteleveranse hva gjelder tilgjengelighet, autentisitet eller fortrolighet, til det tidspunkt hvor tjenesten er gjenopprettet.

Artikkel 3 nr. 3 presiserer at ved avgjørelse av hendelsens geografiske omfang, jf. NIS-direktivet artikkel 16 nr. 4 bokstav c, må tilbyderne være i stand til å fastslå om hendelsen påvirker leveransen av tjenester i bestemte EU-land.

Når det gjelder omfanget av driftsforstyrrelser etter NIS-direktivet artikkel 16 nr. 4 bokstav d, presiserer gjennomføringsforordningen artikkel 3 nr. 4 at dette skal måles basert på om en eller flere av følgende egenskaper svekkes som følge av en hendelse: dataenes eller dermed tilknyttede tjenesters tilgjengelighet, autentisitet, integritet eller konfidensialitet.

Når det gjelder omfanget av virkningen på økonomisk og samfunnsmessig virksomhet, jf. NIS-direktivet artikkel 16 nr. 4 bokstav e, presiserer gjennomføringsforordningen i artikkel 3 nr. 5 at tilbydere skal kunne avgjøre om hendelsen har medført betydelige materielle eller ikke-materielle tap for brukerne, for eksempel med hensyn til helse, sikkerhet eller skade på eiendom.

Artikkel 3 nr. 6 slår fast at tilbydere av digitale tjenester ikke er forpliktet til å innsamle informasjon om overstående som de ikke har adgang til.

Artikkel 4 angir nærmere konkrete parametere for å fastslå om virkningen av en hendelse er betydelig, jf. NIS-direktivet artikkel 16 nr. 4.

2.5 Cybersikkerhetsforordningen

2.5.1 Innledning

Forordning (EU) 2019/881 (cybersikkerhetsforordningen) ble vedtatt i EU 17. april 2019 og har som formål å sikre et velfungerende indre marked med et høyt nivå av cybersikkerhet, motstandsdyktighet og tillit innad i EØS, jf. forordningen artikkel 1. Dette skal oppnås ved å

1. fastsette mål, oppgaver og organisatoriske forhold for ENISA, og
2. etablere et rammeverk for opprettelse 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 opp-

splittingen av det indre markedet med hensyn til cybersikkerhetssertifiseringsordninger i Unionen.

Cybersikkerhetsforordningen opphever forordning (EU) 526/2013 av 21 mai 2013 om det europeiske byrå for nett- og informasjonssikkerhet (ENISA) og om oppheving av forordning (EF) nr. 460/2004.

Forordningen regulerer to hovedområder: ENISA og cybersikkerhetssertifisering.

2.5.2 ENISA

Forordningen innebærer at ENISA får et styrket budsjett, flere ansatte og et styrket og permanent mandat (jf. artikkel. 3) og byrået vil dermed spille en større rolle innen digital sikkerhet i EØS. ENISA vil med et permanent mandat ivareta rollen som Den Europeiske Unions Byrå for Cybersikkerhet. ENISA skal etter anmodning kunne bistå statene med grenseoverskridende hendelseshåndtering, herunder blant annet rådgivning, analyse og tekniske undersøkelser. ENISA skal også særlig bistå og legge til rette for statenes kapasitetsutbygging, operasjonelt samarbeid og forskning og utvikling.

ENISA skal utføre oppgavene de pålegges gjennom denne forordningen, og andre oppgaver som følger av andre rettsakter som vedrører cybersikkerhet, blant annet NIS-direktivet.

2.5.3 Cybersikkerhetssertifisering

Forordningen etablerer et nytt regelverk for sikkerhetssertifisering av IKT-produkter, IKT-tjenester og IKT-prosesser jf. artikkel 46 til 65. Noe av bakgrunnen for dette er at trusselbildet og økningen av IKT-kriminalitet har fremtvunget ulike nasjonale sertifiseringsregelverk. Konsekvensen er blant annet fragmenterte og lite hensiktsmessige ordninger som ikke samspiller effektivt inn mot det indre marked i EØS.

ENISA får viktige oppgaver i forbindelse med å utvikle og administrere dette rammeverket. Forordningen stiller i denne sammenheng også et krav om at statene skal etablere tilsynsmyndigheter og andre roller for sikkerhetssertifisering.

Forordningen innfører ikke direkte operasjonelle sertifiseringsordninger, men etablerer et rammeverk for etablering av spesifikke europeiske sertifiseringsordninger for IKT-produkter, IKT-tjenester og IKT-prosesser. Disse vil bli utarbeidet etter forslag fra ENISA og vedtatt som gjennomføringsrettsakter fra EU-kommisjonen.

En cybersikkerhetssertifiseringsordning vil i henhold til forordningen attestere at IKT-produktene, IKT-tjenestene og IKT-prosessene som er sertifisert i overensstemmelse med ordningen og oppfyller fastsatte sikkerhetskrav. De europeiske sertifiseringsordningene vil ikke selv utvikle tekniske standarder, men benytte eksisterende standarder om tekniske krav og evalueringsprosedyrer som produktene skal overholde. Etter artikkel 51 skal sertifiseringsordningene utformes slik at de, basert på relevans for den aktuelle prosess, produkt- eller tjenestegruppen, tar hensyn til flere sikkerhetsmål, herunder:

- Beskytte data mot utilsiktet eller uautorisert lagring, behandling eller offentliggjøring, og beskytte data mot utilsiktet eller uautorisert ødeleggelse, tap eller endring, i hele IKT-produktet, tjenesten eller prosessens levetid.
- Sikre at kun autoriserte personer, programmer eller maskiner har adgang til dataene, herunder blant annet gjennom tilstrekkelig logging av type data og hvilke handlinger som er utført.
- Verifisere at IKT-produkter, tjenester eller prosesser ikke inneholder kjente sårbarheter, og at disse er sikre som følge av standardinnstillinger og innebygget sikkerhet.
- Sikre tilgjengelighet og tilgang til data ved tilfeller av fysiske eller tekniske hendelser.
- Sikre at IKT-produkter og -tjenester innehar ajourført software og hardware fri for kjente sårbarheter, samt er gitt mekanismer for sikker oppdatering.

Videre innebærer forordningens bestemmelser at ordningene skal fastsette flere spesifikke elementer knyttet til omfang og innhold i cybersikkerhetssertifiseringen, jf. artikkel 54. Det omfatter blant annet valg av aktuelle IKT-produkter, -tjenester og prosesser, spesifisering av cybersikkerhetskrav (for eksempel med henvisning til relevante standarder eller tekniske spesifikasjoner), evalueringskriterier og -metoder og det tillitsnivået de er ment å garantere, herunder grunnleggende, betydelig eller høyt, jf. artikkel 52. For tillitsnivået «grunnleggende» vil det i en sertifiseringsordning også kunne åpnes for en forenklet prosedyre med selvvurdering, jf. artikkel 53.

Tilbydere av sertifiserte IKT-produkter, tjenester eller prosesser skal også offentliggjøre enkelte supplerende opplysninger, blant annet veiledninger og anbefalinger for å bistå sluttbrukerne med sikker konfigurasjon, installasjon, bruk, drift og vedlikehold. Det skal angis hvor lenge det tilbys sikkerhetsstøtte og det skal gjøres mulig for

sluttbruker å orientere seg om sårbarheter samt å kunne melde om sårbarheter de selv oppdager.

Det skal være frivillig å benytte seg av sertifiseringsregelverket. EU-kommisjonen vil imidlertid regelmessig vurdere effekten og anvendelsen av de vedtatte sertifiseringsordningene, og hvorvidt en ordning skal gjøres obligatorisk.

Forordningen legger opp til at de europeiske sertifiseringsordningene skal utarbeides av ENISA primært etter anmodning fra EU-kommisjonen basert på EU-kommisjonens arbeidsprogram, jf. artikkel 48. Utarbeidelse skal skje med bistand fra og i tett samarbeid med den Europeiske Cybersikkerhetssertifiseringsgruppen (ECCG) jf. artikkel 49. ECCG er opprettet etter forordningens artikkel 62, og skal fungere som et ekspertorgan sammensatt av representanter for nasjonale sertifiseringsmyndigheter.

Når en europeisk cybersikkerhetssertifiseringsordning har blitt vedtatt kan produsenter og tilbydere av IKT-tjenester søke sertifisering for deres produkter, tjenester eller prosesser. Sertifiseringen er i henhold til forordningen frivillig, med mindre annet blir fastsatt jf. omtale av artikkel 56 over.

Sertifisering og utstedelse av cybersikkerhetsattest skal utføres av samsvarsvurderingsorganer som er akkreditert til å utføre sertifiseringer primært for tillitsnivåene «grunnleggende» og «betydelig» jf. artikkel 56 nr. 4. For tillitsnivået «høyt» er det primært en nasjonal cybersikkerhetssertifiseringsmyndighet som utsteder sertifikatet. Hvordan dette gjøres beror på hvordan sertifiseringsordningen er utformet. Akkrediteringen av samsvarsorganer utføres av nasjonale akkrediteringsorganer som er utpekt i henhold til forordning (EF) nr. 765/2008 om krav til akkreditering og markedsovervåkning i forbindelse med markedsføring av produkter. I medhold av lov 12. april 2013 nr. 13 om det frie varebytte i EØS (EØS-vareloven) § 3 første ledd er Norsk Akkreditering pekt ut som nasjonalt akkrediteringsorgan i Norge. Forordningen åpner for at man kan fastsette i en sertifiseringsordning at sertifiseringen i godt begrunnede tilfeller skal foretas av et offentlig organ jf. artikkel 56 nr. 4, 5 og 6, jf. artikkel 60.

Etter artikkel 57 vil nasjonale sertifiseringsordninger som allerede er omfattet av en europeisk sertifiseringsordning opphøre fra det tidspunkt det fastsettes i en gjennomføringsrettsakt som etablerer en ny ordning etter artikkel 49. Selv om en ordning opphører, vil utstedte attester gjelde til utløpsdato. Nasjonale sertifiseringsordninger som ikke er omfattet av en europeisk cybersikkerhetssertifiseringsordning vil fortsatt bestå.

Forordningen innebærer at det må utpekes minst én myndighet i hvert land som kan føre tilsyn med sertifiseringen, herunder blant annet at samsvarsorganene overholder regelverket, at de attester som organene har utstedt er i overenstemmelse med kravene som følger av forordningen og at de er i henhold til den europeiske cybersikkerhetssertifiseringsordningen.

Etter artikkel 58 skal den nasjonale myndigheten være uavhengig av de enheter den fører tilsyn med, og statene skal sikre at nasjonale sertifiseringsmyndigheters aktiviteter vedrørende utstedelse av sertifiseringsattester etter artikkel 56 nr. 5 bokstav a og nr. 6 er strengt adskilt fra sine tilsynsaktiviteter.

Den nasjonale myndigheten skal kunne behandle klager i forbindelse med attester utstedt av etterlevelsesorganene.

Etter artikkel 62 etablerer forordningen en europeisk cybersikkerhetssertifiseringsgruppe (ECCG) bestående av alle statenes nasjonale sertifiseringstilsynsmyndigheter. Gruppen skal både gi råd til EU-kommisjonen i cybersikkerhetssertifiseringspolitikk, samt samarbeide med ENISA om å utarbeide forslag til europeiske cybersikkerhetssertifiseringsordninger, følge utviklingen, fremme samarbeid og støtte gjennomføringen av ordningen med fagfellevurdering. Gruppen kan også foreslå for EU-kommisjonen konkrete ordninger som ENISA bør få i oppdrag å utarbeide.

Etter artikkel 65 skal statene fastsette regler for sanksjoner for brudd på forordningens bestemmelser og de europeiske sertifiseringsordninger. Sanksjonene skal være effektive, stå i rimelig forhold til bruddet og ha avskrekkende effekt.

2.6 Metode for gjennomføring av rettsaktene

NIS-direktivet pålegger private virksomheter plikter. Direktivbestemmelser som berører privates rettigheter og plikter, må gjennomføres i eller i medhold av lov. Departementet foreslår at NIS-direktivet gjennomføres delvis i lov og delvis i forskrift. Departementet legger opp til at det blir utarbeidet en forskrift som utfyller loven, og at lov om digital sikkerhet og tilhørende forskrift trer i kraft samtidig. Cybersikkerhetsforordningen og gjennomføringsforordningen vil i sin helhet inkorporeres som forskrift, hjemlet i lov om digital sikkerhet.

Departementet foreslår at det i lovteksten angis at tilbydere av samfunnsviktige tjenester

innenfor visse sektorer er omfattet av loven, og at det i forskrift blir nærmere regulert hvilke typer virksomheter som anses å være tilbydere av samfunnsviktige tjenester. Dette vil sikre fleksibilitet med hensyn til behov for endringer i tråd med samfunnsutviklingen og regelverksutvikling i EØS. I forskriften vil også sikkerhets- og varslingskravene som stilles til både tilbydere av samfunnsviktige tjenester og digitale tjenester spesifiseres nærmere. Forskriften vil også gi nærmere regler om responsfunksjoner, tilsyn, tvangsmulkt og overtredelsesgebyr.

Departementet har merket seg en tiltakende regelverksutvikling i EØS om digital sikkerhet. En del av rettsaktene har et teknisk og faglig preg som passer inn i forskrift. Ambisjonen er at lov om digital sikkerhet skal kunne fungere som en rammelov som legger til rette for gjennomføring av flere rettsakter innenfor digital sikkerhet. Departementet foreslår derfor en egen bestemmelse som gir hjemmel til å gjennomføre forpliktelser som følger av EØS-avalen og andre internasjonale avtaler som understøtter lovens regler og formål, jf. forslag til § 18 bokstav f. Gjennomføring av cybersikkerhetsforordningen som forskrift foreslås hjemlet i forslag til § 19. Bestemmelsen er utformet på en slik måte at den viser til forordningens tittel, formål og virkeområde knyttet til cybersikkerhetssertifisering.

2.7 Høringen

Justis- og beredskapsdepartementet sendte 21. desember 2018 på høring et utkast til lov som forbereder gjennomføring av NIS-direktivet i norsk rett. Høringsnotatet ble sendt sammen med IKT-sikkerhetsutvalgets utredning NOU 2018: 14 *IKT-sikkerhet i alle ledd*.

Høringsnotatet ble sendt til følgende høringsinstanser:

Departementene
Statsministerens kontor

Agder lagmannsrett
Arbeids- og velferdsdirektoratet
Brønnøysundregistrene
Cyberforsvaret
Datatilsynet
De nasjonale forskningsetiske komiteene
Departementenes sikkerhets- og serviceorganisasjon
Direktoratet for barnehage, utdanning og IKT
Direktoratet for e-helse
Direktoratet for forvaltning og IKT (nå Digitaliseringsdirektoratet)
Direktoratet for internasjonalisering og kvalitetssikring i høyere utdanning
Direktoratet for nødkommunikasjon
Direktoratet for samfunnssikkerhet og beredskap
Domstoladministrasjonen
Ekom-CERT
Etterretningstjenesten
Finanstilsynet
Fiskeridirektoratet
Folkehelseinstituttet
Forbrukerrådet
Forsvarets forskningsinstitutt
Fylkesmennene (nå statsforvalterne)
Helsedirektoratet
Hovedredningssentralen Nord
Hovedredningssentralen Sør
Integrerings- og mangfoldsdirektoratet
Jernbanedirektoratet
Jernbanetilsynet
Justervesenet
Kompetanse Norge
Konkurransetilsynet
Kriminalpolitisentralen (Kripos)
Kystverket
Landbruksdirektoratet
Luftfartstilsynet
Mattilsynet
Meteorologisk institutt
Miljødirektoratet
Nasjonal kommunikasjonsmyndighet
Nasjonal sikkerhetsmyndighet
Norges Bank
Norges forskningsråd
Norges vassdrags- og energidirektorat
Norsk romsenter
Norsk utenrikspolitisk institutt
NSM NorCERT
Oljedirektoratet
Petroleumstilsynet
Politidirektoratet
Politiets sikkerhetstjeneste
Regelrådet
Regjeringsadvokaten
Riksadvokaten
Sjøfartsdirektoratet
Skattedirektoratet
Statens helsetilsyn
Statens jernbanetilsyn
Statens kartverk
Statens legemiddelverk
Statens strålevern
Statens vegvesen
Statistisk sentralbyrå

Teknologirådet
Toll- og avgiftsdirektoratet
Unit – Direktoratet for IKT og fellestjenester i høyere utdanning og forskning
Utdanningsdirektoratet
Utlendingsdirektoratet
Valgdirektoratet
Vegtilsynet
Økokrim

Det Kongelige Hoff
Riksrevisjonen
Sametinget
Stortingets kontrollutvalg for etterretnings-, overvåkings- og trygghetstjenester (EOS-utvalget)
Stortingets ombudsmann for forvaltningen (nå Stortingets ombud for forvaltningen)

Bodø kommune
Fauske kommune
Færder kommune
Gausdal kommune
Harstad kommune
Hemsedal kommune
Kristiansand kommune
Kvænangen kommune
Longyearbyen lokalstyre
Lørenskog kommune
Molde kommune
Oslo kommune
Trondheim kommune

Finnmark fylkeskommune
Hordaland fylkeskommune
Oppland fylkeskommune
Telemark fylkeskommune
Troms fylkeskommune
Vestfold fylkeskommune

Arkitektur- og designhøgskolen i Oslo
Christian Michelsens Institutt
Det norske Nobelinstitutt
Fafo
Institutt for fredsforskning
Institutt for journalistikk
Norges Handelshøgskole
Norges miljø- og biovitenskapelige universitet
Norges teknisk- og naturvitenskapelige universitet
Politihøgskolen
Sintef
Teknologisk institutt
UiOCERT
Universitetet i Agder
Universitetet i Bergen
Universitetet i Oslo
Universitetet i Stavanger
Universitetet i SørØst Norge
Universitetet i Tromsø

Aerospace Industrial Maintenance Norway
Andøya Space Center
Avinor
Bane NOR SF
Flytoget
Gassco AS
Helse Midt RHF
Helse Nord RHF
Helse Sør-Øst RHF
Helse Vest RHF
Helse-CERT
Innovasjon Norge
Norsk Helsenett SF
Norsk rikskringkasting AS
Posten Norge AS
Simula UIB
Statkraft AS
Statnett SF
Uninett
UNINETT/NORID

Akademikerne
Amnesty International Norge
Arbeidsgiverforeningen Spekter
Bedriftsforbundet
Den Norske Advokatforening
Den Norske Atlanterhavskomité
Den Norske Dataforening
Den norske Helsingforskomité
Distriktenes energiforening
Energi Norge AS
Fagforbundet
Fagpressen
Fellesforbundet
Finans Norge
Finansieringsselskapenes forening
Forum for informasjonssikkerhet i kraftforsyningen
Hovedorganisasjonen Virke
IKT-Norge
Industri Energi
Kommunal informasjonssikkerhet
KS – Kommunesektorens organisasjon
Kontaktutvalget for telesaker i kraftforsyningen
Landsorganisasjonen i Norge
Norges ingeniør- og teknologiorganisasjon
Norges Juristforbund
Norges Rederiforbund
Norsk Havneforening
Norsk Journalistlag

Norsk Olje og Gass
Norsk Presseforbund
Norsk Tjenestemannslag
Norsk Vann
Næringslivets hovedorganisasjon
Næringslivets sikkerhetsorganisasjon
Næringslivets sikkerhetsråd
Samfunnsviterne
Standard Norge
Unio
Virke
Yrkesorganisasjonenes Sentralforbund

Abelia
Accenture
Altibox
Apple
ATEA
Bankenes standardiseringskontor
Basefarm
BDO
Boston Consulting Group
Bouvet
Broadnet
Cap Gemini
Cargo Net AS
Cisco
Computas
Dataequipment
Datametrix
Devoteam
DNB
Equinor
Evry
Experis
Falck Nutec
Gartner Group
GET
Gjensidige
Grenland Rail AS
Hafslund AS
Hydro
IBM
ICE
Jotne
Kongsberg Gruppen ASA
Kongsberg Satellite Services AS
KPMG
Kraft-CERT
LKAB Malmtrafikk AB
Lyse AS
McKinsey
Microsoft
Mnemonic AS
NAMMO AS
NETS
NorConsult
NorSIS
NTT Com Security
Oslo Børs
PWC
Safetec
Skagerak energi
Software innovation
Sopra Steria
Space Norway AS
Telenor
TelenorCERT
Telia
Thales Norge AS
Viken fiber
VPS (verdipapirsentralen)
Watchcom

66 høringsinstanser hadde merknader:
Abelia
Advokatforeningen
Arbeidsgiverforeningen Spekter
Avinor
Bane NOR SF
Datatilsynet
Den norske legeforeningen
Departementenes sikkerhets- og service-organisasjon
Direktoratet for e-helse
Direktoratet for forvaltning og IKT
Direktoratet for samfunnssikkerhet og beredskap
Domstoladministrasjonen
Fagforbundet
Finans Norge
Finanstilsynet
Forbrukerrådet
Forsvarsdepartementet
Fylkesmannen i Vestfold og Telemark
Helsedirektoratet
Helsetilsynet
Hovedredningssentralene
Jernbanedirektoratet
KS – Kommunesektorens organisasjon
Kartverket
Kompetanse Norge
Kunnskapsdepartementet
LO
Luftfartstilsynet
Microsoft Norge
NHO
Norges ingeniør- og teknologorganisasjon
Nasjonal kommunikasjonsmyndighet
Nasjonal sikkerhetsmyndighet
Norges Bank

Norges Rederiforbund
Norges vassdrags- og energidirektorat
Norsk Helsenett SF
Norsk Romsenter
Norsk Vann BA
Norsk olje og gass
Norsk senter for informasjonssikring
Næringslivets Sikkerhetsråd
Olje- og energidepartementet
Oljedirektoratet
Oslo kommune
Petroleumstilsynet
Politidirektoratet (med uttalelse fra Kripos)
Politiets sikkerhetstjeneste
Posten Norge AS
Regelrådet
Samferdselsdepartementet
Samferdselsdepartementet
Simula UIB
Sjøfartsdirektoratet
Skatteetaten
Statens jernbanetilsyn
Statens vegvesen
Statistisk sentralbyrå
Statkraft Energi AS
Teknisk-naturvitenskapelig forening
Telia Norge AS
Unio
Direktoratet for IKT og fellestjenester i høyere utdanning og forskning
Universitetet i Oslo / UiO-CERT
Utlendingsdirektoratet
Vegtilsynet

Høringsinstansenes syn vil bli behandlet under redegjørelsen for de ulike lovforslagene.

3 Lovens formål, virkeområde og forholdet til andre lover

3.1 Gjeldende rett

Det finnes i norsk rett i dag ingen tverrsektorielle eller sektorspesifikke lover som fullt ut tilsvarer NIS-direktivet. Blant de lovene som finnes, har sikkerhetsloven flest fellestrekk med NIS-direktivet. Formålet med sikkerhetsloven er å ivareta nasjonale sikkerhetsinteresser gjennom å sikre grunnleggende nasjonale funksjoner.

I Prop. 153 L (2016–2017) i punkt 6.4.2 uttaler Forsvarsdepartementet følgende om sikkerhetslovens formål:

> «Departementet mener at lovens primære formål er å trygge de overordnede nasjonale sikkerhetsinteressene, ved å forebygge, motvirke og avdekke sikkerhetstruende virksomhet, det vil si tilsiktede handlinger der målet er å ramme interessene og tilsiktede handlinger som indirekte kan true interessene. I dette ligger det implisitt at beskyttelse av nasjonale sikkerhetsinteresser også omfatter beskyttelse av de grunnleggende nasjonale funksjonene som understøtter dem».

Sikkerhetsloven gjelder for virksomheter som har avgjørende betydning for grunnleggende nasjonale funksjoner. Dette er «tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser», jf. sikkerhetsloven § 1-5 nr. 2.

Departementene skal innenfor sine ansvarsområder fatte vedtak om at loven helt eller delvis skal gjelde for virksomheter som enten behandler sikkerhetsgradert informasjon, råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner, eller driver aktivitet som har avgjørende betydning for grunnleggende nasjonale funksjoner, jf. sikkerhetsloven § 1-3 første ledd bokstav a til c.

I tillegg gjelder sikkerhetsloven for statlige, fylkeskommunale og kommunale organer og leverandører av varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser, jf. sikkerhetsloven § 1-2 første og andre ledd.

Det er imidlertid vesentlige forskjeller mellom sikkerhetsloven og NIS-direktivet. For det første angir sikkerhetsloven og direktivet ulike formål med sikringen. Sikkerhetslovens formål er å bidra til å ivareta nasjonale sikkerhetsinteresser ved å sikre grunnleggende nasjonale funksjoner som understøtter disse. NIS-direktivets formål er å forbedre det indre markedets funksjon, gjennom å stille sikkerhetskrav til nettverks- og informasjonssystemer som er nødvendige for å opprettholde leveransen av samfunnsviktige tjenester.

For det andre handler sikkerhetsloven i første rekke om å beskytte seg mot tilsiktede handlinger. NIS-direktivet har ikke en slik begrensning. I tillegg er det ulikheter når det gjelder hvilket sikkerhetsnivå som kreves, varsling av hendelser og tilsynsregime.

Lov 25. juni 2010 nr. 45 om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (sivilbeskyttelsesloven) har som formål «å beskytte liv, helse, miljø, materielle verdier og kritisk infrastruktur ved bruk av ikke-militær makt når riket er i krig, når krig truer, når rikets selvstendighet eller sikkerhet er i fare, og ved uønskede hendelser i fredstid», jf. § 1. Loven gir blant annet bestemmelser om Sivilforsvaret, allmennhetens bistandsplikt i akuttsituasjoner, kommunal beredskapsplikt og beskyttelse av kritisk infrastruktur.

Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven) har som formål å beskytte personopplysninger. Behandlingsansvarlige og databehandlere er derfor pålagt plikter om blant annet sikring av personopplysningene. For å ivareta informasjonens konfidensialitet, integritet og tilgjengelighet må informasjonssystemene som behandler personopplysningene sikres. Personopplysningsregelverket, forvaltningsloven og eforvaltningsforskriften gjennomgås nærmere i punkt 5.

En gjennomgang av gjeldende rett innen sektorregelverk viser at kravene som stilles i sektorene varierer. En rekke virksomheter er underlagt sikkerhetskrav av ulik art, men det er i mange til-

feller uklart om det kan tolkes slik at det stilles krav om digital sikkerhet. Tilsvarende er tilfelle for krav om varsling.

Eksisterende regelverk benytter dessuten til dels ulike begreper for å beskrive digital sikkerhet.

3.2 Direktivet

3.2.1 Innledning

NIS-direktivet retter seg mot virksomheter som leverer tjenester som er viktige for et velfungerende samfunn og næringsliv. Virksomhetene er delt i to hovedkategorier: tilbydere av samfunnsviktige tjenester, jf. artikkel 4 nr. 4 og tilbydere av digitale tjenester, jf. artikkel 4 nr. 6. Alle tjenestene er listet opp i direktivets vedlegg II og III.

NIS-direktivet gjelder ikke for virksomheter som er omfattet av europaparlaments- og rådsdirektiv 2002/21/EF av 7. mars 2002 om felles rammeregler for elektroniske kommunikasjonsnett og -tjenester (rammedirektivet), artikkel 13 bokstav a b. Direktivet er innlemmet i EØS-avtalen og gjennomført i norsk rett gjennom ekomregelverket. Ekomloven gjelder for tilbydere av elektronisk kommunikasjonsnett- og tjenester. Dette gjelder blant annet mobiltilbyder, bredbåndstilbyder og tilbydere av internettjenester.

NIS-direktivet gjelder ikke for virksomheter som er omfattet av 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. Forordningen er gjennomført i norsk rett gjennom lov 15. juni 2018 nr. 44 om elektroniske tillitstjenester. Virksomheter som er omfattet av lov om elektroniske tillitstjenester er tilbydere av elektronisk identifikasjon (eID), elektronisk signatur, elektronisk segl, tidsstemplingstjenester, elektronisk tjeneste for registrert sending og sertifikattjenester for nettstedsautentisering. Loven gjelder kun elektroniske tillitstjenester som tilbys til offentligheten og som har virkning overfor tredjemann.

NIS-direktivet skal ikke legge begrensninger på statenes muligheter til å iverksette tiltak for å ivareta essensielle statsfunksjoner, særlig nasjonal sikkerhet og opprettholdelse av lov og orden, herunder adgangen til å etterforske, oppdage og iretteføre kriminelle handlinger, jf. artikkel 1 nr. 6.

Det følger videre av artikkel 1 nr. 7 et unntak for virksomheter som er underlagt sektorspesifikt EØS-regelverk. Dersom slikt regelverk stiller krav om sikkerhet og varsling som har effekt som minst tilsvarer direktivets krav, skal sektorregelverket anvendes. Etter fortalepunkt 9 er det kun det aktuelle regelverket og hvordan det er implementert nasjonalt som skal tas i betraktning ved vurderingen av om bestemmelsen kommer til anvendelse.

Dersom regelen kommer til anvendelse er den aktuelle sektoren eller de virksomhetene som er underlagt regelverket unntatt fra direktivet. Anvendelsen av bestemmelsen skal rapporteres til EU-kommisjonen (for Norges del vil rapportering skje til EFTAs overvåkingsorgan).

3.2.2 Tilbydere av samfunnsviktige tjenester

Det følger av artikkel 5 nr. 2 at en virksomhet skal anses som tilbyder av en samfunnsviktig tjeneste dersom tre kumulative kriterier er oppfylt. De tre kriteriene følger av artikkel 5 nr. 2 bokstav a til c.

Det første kriteriet, jf. artikkel 5 nr. 2 bokstav a, er at virksomheten må tilby en tjeneste som er viktig for opprettholdelsen av kritiske samfunnsmessige eller økonomiske aktiviteter. I henhold til fortalepunkt 20 er det tilstrekkelig å fastslå at virksomheten leverer en slik tjeneste som er opplistet i direktivet vedlegg II. Det er kun den delen av virksomheten som leverer den aktuelle tjenesten som omfattes. For eksempel vil trafikkstyringen på en stor flyplass omfattes, mens butikkområdet ikke omfattes. Vedlegg II lister opp følgende samfunnssektorer:

- Energi (elektrisitet, olje og gass)
- Transport (luft, jernbane, sjø og vei)
- Helse (helsetjenester)
- Bank
- Finansmarkedsinfrastruktur
- Drikkevannsforsyning og -distribusjon
- Digital infrastruktur
  - IXP – internet exchange point
  - DNS – domain name server service provider
  - TLD – top level domain name registries

Det fremgår av direktivets vedlegg II en nærmere spesifisering av hvilke tjenester som omfattes.

Det andre kriteriet, jf. artikkel 5 nr. 2 bokstav b, er at tjenesteleveransen må være avhengig av nettverks- og informasjonssystemer. Begrepet nettverks- og informasjonssystemer defineres i artikkel 4 nr. 1. Det tredje kriteriet, jf. artikkel 5 nr. 2 bokstav c, er at en hendelse i virksomhetens nettverks- og informasjonssystemer ville hatt betydelig forstyrrende virkning på leveransen av den samfunnsviktige tjenesten. Som det fremgår av punktene under er vurderingstemaet her

tjenesteleveranse i en samfunnssammenheng, og ikke virksomhetens tjenesteleveranse isolert sett. Det er altså spørsmål om i hvilken grad det går utover samfunnets tilgang på en viss tjeneste, at den aktuelle virksomheten ikke leverer sitt bidrag til totalen som normalt.

Ved vurderingen av vesentligheten av en sikkerhetshendelses forstyrrende virkning skal både tverrsektorielle og sektorspesifikke momenter tas i betraktning. Artikkel 6 oppstiller en ikke uttømmende liste med tverrsektorielle momenter som skal vurderes:

- antall brukere som baserer seg på tjenesten
- andre vedlegg II-sektorers avhengighet av tjenesten
- omfanget og varigheten av hendelsers mulige virkning på økonomiske og samfunnsmessige aktiviteter og samfunnssikkerhet
- virksomhetens markedsandel
- geografisk område som kan rammes av hendelsen
- viktigheten av virksomhetens bidrag til leveranse av tjenesten, med tanke på alternative tjenestetilbydere

Det endelige virkeområdet for direktivet skal fastlegges gjennom en identifiseringsprosess i regi av hver enkelt stat. Det er opp til statene hvordan denne prosessen gjennomføres, så lenge direktivets krav om å opprette en liste over alle tilbydere av samfunnsviktige tjenester oppfylles. Det er for eksempel ikke krav om at det fattes enkeltvedtak om identifisering eller utpeking av hver enkelt virksomhet. Listen skal oppdateres jevnlig og minst hvert andre år.

Det er opp til statene å definere flere samfunnssektorer og tjenester som samfunnsviktige enn det som følger av direktivet. Se blant annet fortalepunkt 23.

3.2.3 Tilbydere av digitale tjenester

Digitale tjenester omfatter tilbydere av nettbaserte markedsplasser, nettbaserte søkemotorer og skytjenester.

Det følger av NIS-direktivet artikkel 4 nr. 5 at med digital tjeneste menes tjenester som nevnes i vedlegg III. Videre henvises det til definisjonen av tjenester i Europaparlaments- og rådsdirektiv (EU) 2015/1535 av 9. september 2015 om en informasjonsprosedyre for tekniske regler og standarder og informasjonssamfunnstjenester (kodifisering) artikkel 1 nr. 1 bokstav b. Direktivet er gjennomført i lov 23. mai 2003 nr. 35 om visse sider av elektronisk handel og andre informasjonssamfunnstjenester (ehandelsloven). I § 1 bokstav a og b er informasjonssamfunnstjeneste definert som

a. enhver tjeneste som vanligvis ytes mot vederlag og som formidles elektronisk, over avstand og etter individuell anmodning fra en tjenestemottaker, samt
b. enhver tjeneste som består i å gi tilgang til, eller overføre informasjon over, et elektronisk kommunikasjonsnett, eller i å være nettvert for data som leveres av tjenestemottakeren

De tre digitale tjenestene som omfattes av NIS-direktivet defineres i artikkel 4 nr. 17, 18 og 19.

En nettbasert markedsplass er en digital tjeneste som gjør det mulig for forbrukere og næringsdrivende å inngå nettbaserte salgs- eller tjenesteavtaler med næringsdrivende, enten på nettstedet til den nettbaserte markedsplassen eller på nettstedet til en næringsdrivende som bruker datatjenester som leveres av den nettbaserte markedsplassen. Applikasjonsbutikker trekkes i fortalepunkt 15 frem som en type butikk som faller inn under denne kategorien.

En nettbasert søkemotor er en digital tjeneste som gjør det mulig for brukere å foreta søk på i prinsippet alle nettsteder på et bestemt språk, på grunnlag av en forespørsel om et hvilket som helst emne i form av et nøkkelord, en setning eller andre inndata, og som viser lenker hvor det er mulig å finne informasjon om det forespurte innholdet.

En skytjeneste er en digital tjeneste som gir tilgang til en skalerbar og fleksibel samling av delbare databehandlingsressurser.

I følge artikkel 16 nr. 11 omfattes ikke mikrovirksomheter og små virksomheter, jf. Kommisjonsrekommandasjon 2003/361/EF av 6. mai 2003 om definisjonen av mikroforetak og små og mellomstore bedrifter. Det vil si at virksomheter som har færre enn 50 ansatte og som har en årlig omsetning eller årlig samlet balanse som ikke overstiger 10 millioner euro ikke omfattes av direktivet.

Det skal ikke foretas en ytterligere identifisering av tilbydere av digitale tjenester. For denne kategorien skal det være like regler i hele EØS, jf. fortalepunkt 49. Det er derfor ikke noe nasjonalt handlingsrom hva gjelder definisjon av de digitale tjenestene eller sikkerhets- og varslingskrav, med unntak av de føringer som er gitt i artikkel 1 nr. 6, jf. artikkel 16 nr. 10. Dette har blant annet sammenheng med at aktiviteten er grenseoverskridende av natur, se nærmere fortalepunkt 57.

Av samme grunn har EU-kommisjonen i medhold av artikkel 16 nr. 8 utarbeidet gjennomføringsforordningen som konkretiserer direk-

tivets krav om sikkerhet og varsling. Bestemmelsene hindrer imidlertid ikke den enkelte tilbyder fra å iverksette strengere sikkerhetstiltak enn det som følger av direktivet. Det følger dessuten av fortalepunkt 54 at offentlige virksomheter står fritt til gjennom kontrakt å kreve at tilbydere av digitale tjenester har et høyere sikkerhetsnivå enn det som følger av direktivet.

Det følger videre av fortalepunkt 58 at direktivet ikke utelukker statene fra å stille krav om sikkerhet og varsling til virksomheter som ikke faller inn under direktivets definisjon av tilbydere av digitale tjenester.

3.3 Forslaget i høringsnotatet

Departementet foreslo i høringsnotatet at lovens formål skal tilsvare NIS-direktivets formål, å bidra til å opprettholde kritisk samfunnsmessig og økonomisk aktivitet ved å forebygge, avdekke, motvirke og varsle tilsiktede og utilsiktede uønskede hendelser i nettverk og informasjonssystemer som brukes for å levere samfunnsviktige tjenester.

Siden virkeområdet i NIS-direktivet fremgår av vedlegg, foreslo departementet at Kongen kan gi forskrift med nærmere bestemmelser om lovens virkeområde. Det ble vurdert som mest hensiktsmessig at virkeområdet ikke fremgikk uttømmende av forskrift, da direktivet også forutsetter en nærmere kartlegging av hvilke virksomheter som faller inn under virkeområdet.

Departementet mente det var behov for en oversikt over begreper som loven benytter, og foreslo en bestemmelse hvor definisjonen av de fleste av lovens begreper fremgikk. Disse definisjonene tilsvarer i det vesentlige direktivets definisjoner.

Departementet foreslo også i høringsnotatet at dersom annen lov stiller krav om sikkerhet og varsling som minst tilsvarer departementets forslag til lov, skal annen lov benyttes.

3.4 Høringsinstansenes syn

Et flertall av høringsinstansene uttrykte støtte til høringsnotatet, blant annet *Olje- og energidepartementet*, *Avinor*, *Statkraft*, *Direktoratet for e-helse*, *Oljedirektoratet*, *Nasjonal kommunikasjonsmyndighet*, *Statens jernbanetilsyn*, *Jernbanedirektoratet*, *Bane NOR SF*, *Helsedirektoratet*, *Telia Norge AS*, *Universitetet i Oslo UiO-CERT*, *Hovedredningssentralene*, *Hovedorganisasjonen for universitets- og høyskoleutdannede*, *Microsoft Norge*, *Direktoratet for samfunnssikkerhet og beredskap*, *Norsk Romsenter*, *Abelia*, *Datatilsynet*, *LO*, *Finanstilsynet og Næringslivets hovedorganisasjon*. *Telia Norge* mener en slik tverrsektoriell lov vil heve sikkerhetsnivået i Norge samtidig som den standardiserer kravene til IKT-sikkerhet på tvers av bransjer. *Telia Norge*, *Næringslivets hovedorganisasjon*, *Microsoft* og *Direktoratet for e-helse* trekker også frem at forslaget vil bidra til å harmonisere reguleringen på tvers av landegrensene, noe som blant annet vil legge grunnlaget for felles sikkerhetsnivå og like konkurransevilkår.

Enkelte høringsinstanser trekker frem at gjennomføring av NIS-direktivet ikke vil ha noen innvirkning for deres virksomheter da kravene allerede finnes i eksisterende regelverk, blant andre *Finanstilsynet*, *Petroleumstilsynet*, *Norges vassdrags- og energidirektorat* og *Norsk Vann*. *Norsk Vann* skriver at de i sin gjennomgang av NIS-direktivet har tolket direktivet slik at dette i all hovedsak er implementert gjennom drikkevannsforskriftens krav.

Enkelte høringsinstanser er positive til gjennomføring av NIS-direktivet, men trekker frem at det bør vurderes om direktivet skal gjennomføres i sektorregulering. Dette gjelder blant andre *Norges vassdrags- og energidirektorat* og *Posten Norge AS*. *Norges vassdrags- og energidirektorat* mener at gjennomføring av NIS-direktivet i sektorregulering vil skape en større nærhet til regelverket. Videre at bestemmelsene i større grad kan konkretiseres og lettere harmoniseres med allerede eksisterende sikkerhetsregelverk. En mellomløsning kan ifølge Norges vassdrags- og energidirektorat være at de deler av NIS-direktivet som gjelder samfunnsviktige tjenester og som er knyttet til spesifikke sektorer gjennomføres i relevant sektorregelverk, mens bestemmelsene knyttet til digitale tjenester gjennomføres i sektorovergripende lov.

Enkelte høringsinstanser, blant andre *Direktoratet for forvaltning og IKT* (nå Digitaliseringsdirektoratet), har påpekt at formålet med loven fremstår som uklart. De uttaler at det bør fremgå at lovens hovedfokus er kontinuitet i drift.

Flere høringsinstanser støtter gjennomføring av NIS-direktivet, men trekker frem at lovforslaget har et uklart virkeområde, blant andre *Luftfartstilsynet*, *Fagforbundet*, *Spekter*, *Norges vassdrags- og energidirektorat*, *Skatteetaten*, *Politiets sikkerhetstjeneste*, *Advokatforeningen*, *Statens Helsetilsyn* og *Legeforeningen*. *Skatteetaten* skriver at lovforslaget etter deres vurdering kan være tydeligere på hvilke aktører som faller inn under

det saklige virkeområdet som er angitt i lovforslaget § 2, på tross av forutsetningen om at det skal gis en nærmere presisering gjennom forskrift. Videre foreslår *Skatteetaten* at det inntas en nærmere avgrensning mot sikkerhetsloven slik man har gjort i Sverige. *Legeforeningen* trekker frem at rekkevidden til lovforslaget fremstår som uklar, og at de er usikre på hvilken innvirkning lovforslaget vil ha på helsesektoren. *Statens Helsetilsyn* trekker frem at det er viktig at det blir klart hvilke virksomheter og tjenester som omfattes av loven. Behovet for klarhet gjelder særlig siden loven innfører varslingsplikt og har hjemler for tilsynsmyndigheten til å kunne gi pålegg, ilegge tvangsmulkt og overtredelsesgebyr.

Flere av høringsinstansene trekker frem at det bør vurderes om loven skal ha et utvidet virkeområde utover NIS-direktivet, blant andre *Forsvarsdepartementet*, *Helsedirektoratet*, *Utlendingsdirektoratet*, *Fagforbundet, Kunnskapsdepartementet, Spekter* og *Direktoratet for samfunnssikkerhet og beredskap*. *Utlendingsdirektoratet* skriver at økende digitalisering utgjør en strukturell sårbarhet i samfunnet, og hvor offentlig og privat virksomhet har en gjensidig avhengighet. *Utlendingsdirektoratet* og *Kartverket* mener det er hensiktsmessig å vurdere om en slik lov også bør omfatte offentlig forvaltning.

I forbindelse med å utvide virkeområdet ser enkelte høringsinstanser hen til særlig IKT-sikkerhetsutvalgets anbefaling om en egen lov om IKT-sikkerhet for alle samfunnskritiske virksomheter og offentlig forvaltning, blant andre *Samferdselsdepartementet*, *Nasjonal sikkerhetsmyndighet*, *Næringslivets sikkerhetsråd, Statens vegvesen, Teknisk-naturvitenskapelig forening, Kripos, Norsk Helsenett SF, KS – kommunesektorens organisasjon, Norges Bank, Norges ingeniør- og teknologorganisasjon, Departementenes sikkerhets- og serviceorganisasjon, Oslo kommune og Domstoladministrasjonen*.

Simula UIB er positive til å gjennomføre NIS-direktivet først, før en eventuelt utvider virkeområdet. Simula UIB anbefaler at det samtidig som det samles erfaringer ved at loven får virke, igangsettes et arbeid som bygger et kunnskapsgrunnlag innen digitale verdikjeder. Simula UIB trekker frem at en god og målrettet utvidelse av loven til å dekke alle norske virksomheter vil kunne komme som en naturlig forlengelse av et slikt arbeid.

Enkelte høringsinstanser trekker frem behovet for også å vurdere andre virkemidler enn regulering innenfor digital sikkerhet, blant andre *Abelia*, *Norsk senter for informasjonssikring* og *Datatilsynet*. *Politiets sikkerhetstjeneste, Direktoratet for e-helse*, *Direktoratet for IKT og fellestjenester i høyere utdanning og forskning* og *Helsedirektoratet* trekker frem behov for veiledninger for hvordan eksisterende regelverk og lov som gjennomfører NIS-direktivet skal forstås og brukes.

Flere høringsinstanser har innspill til høringsnotatets foreslåtte bestemmelser om forholdet til andre lover. Enkelte høringsinstanser trekker frem at det er positivt at strengere særregelverk går foran en lov som gjennomfører NIS-direktivet, blant andre *Sjøfartsdirektoratet, Telia* og *Forsvarsdepartementet*. *Forsvarsdepartementet* skriver at de støtter denne tilnærmingen, da sikkerhetstiltak i ulike sektorer vil kunne kreve forskjellig tilnærming og utforming av krav til sikring. *Advokatforeningen, Spekter, Samferdselsdepartementet*, *Kartverket, Statens vegvesen, Norges Rederiforbund, Politiets sikkerhetstjeneste* og *Statens helsetilsyn* trekker frem at loven må klargjøre forholdet til annet tverrsektorielt og sektorspesifikt regelverk i Norge. *Norges rederiforbund* skriver at det må tilstrebes å unngå dublerende og motstridende reguleringer og lovverk.

Enkelte høringsinstanser har gitt innspill på departementets foreslåtte bestemmelser om definisjoner. *Departementenes sikkerhets- og serviceorganisasjon* og *Næringslivets hovedorganisasjon* peker på at det er ulik terminologi i ulikt regelverk. *Næringslivets hovedorganisasjon* mener at myndighetene må søke å harmonisere og standardisere bruk av begreper brukt innenfor det digitale feltet.

3.5 Departementets vurderinger

3.5.1 Formål og virkeområde

Med fravær av tverrsektorielle eller sektorspesifikke lover som fullt ut tilsvarer NIS-direktivet, mener departementet at det er behov for en lov som omfatter direktivets formål, jf. forslag til lovens § 1. Selv om det finnes tverrsektorielle og sektorspesifikke lover og forskrifter som på ulikt vis setter krav til digital sikkerhet og varsling av uønskede hendelser, er det en rekke aktuelle virksomheter som per i dag ikke er omfattet av krav til digital sikkerhet og varsling. Gjennomføring av NIS-direktivet er etter departementets syn et viktig bidrag for å redusere digitale sårbarheter både i samfunnet og i den enkelte virksomhet.

Departementet merker seg at flere høringsinstanser ser at en norsk lov kan bidra til å heve sikkerhetsnivået i Norge, men også harmonisere krav som stilles på tvers av landene i EØS. Departementet mener dette er et viktig formål

med loven, men ser ikke grunn til å presisere dette nærmere i formålsbestemmelsen.

Formålet med NIS-direktivet er å forbedre det indre markedets funksjon, gjennom å stille sikkerhetskrav til nettverks- og informasjonssystemer som er nødvendige for å opprettholde leveransen av samfunnsviktige tjenester. Det vil da dreie seg om tjenester som er viktige for samfunnets funksjonalitet i sin helhet og der et avbrudd i tjenesten hindrer gjennomføring av økonomisk virksomhet, genererer omfattende økonomiske tap, undergraver brukernes tillit og medfører alvorlige konsekvenser for økonomien i landet og i EØS.

Formålet med cybersikkerhetsforordningen er å sikre at det indre markedet fungerer på tilfredsstillende måte og samtidig oppnår et høyt nivå av cybersikkerhet, cyberresiliens (motstandsdyktighet) og tillit i EØS, gjennom permanente regler om ENISA og en ramme for cybersertifisering av IKT-produkter, IKT-tjenester og IKT-prosesser.

Forslag til ordlyd i formålsbestemmelsen søker å ivareta formålet til både NIS-direktivet og cybersikkerhetsforordningen. Departementet påpeker at lovens formål også må sees i sammenheng med sikkerhetskravene som stilles til tilbyderne og som fremgår av loven §§ 7 og 10. Sikkerhetstiltak skal gjennomføres for å redusere risiko i systemer som benyttes til en tjenesteleveranse for nettopp å opprettholde leveransen av samfunnsviktige tjenester. Høringsnotatet la opp til en formålsbestemmelse som ligger nært opp til NIS-direktivets formål. Med økningen i oppmerksomhet om viktigheten av digital sikkerhet, er det naturlig å anta at det vil komme nye EØS-rettslige krav og nasjonale reguleringer som har sin naturlige plass i en lov om digital sikkerhet. Departementet bemerker derfor at det i fremtiden kan være grunn til å justere formålsbestemmelsen til å i større grad reflektere helheten av reguleringer innenfor digital sikkerhet. Dette synes også i tråd med en av anbefalingene i NOU 2018: 14 *IKT-sikkerhet i alle ledd*, hvor det anbefales en lov med krav til IKT-sikkerhet i alle samfunnskritiske virksomheter og offentlig forvaltning.

Mange høringsinstanser påpeker at lovens virkeområde er uklart.

Lovens saklige virkeområde fremgår av lovforslaget § 2. Hva som menes med henholdsvis tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester følger av definisjonene angitt i henholdsvis § 6 første ledd og § 9 første ledd. Definisjonene bygger på NIS-direktivet vedlegg II og III som inneholder en nærmere angivelse av hvilke tjenester som omfattes. Utover disse definerte subjektene følger ingen annen angivelse av virkeområde enn sektortilhørighet. Departementet merker seg høringsinstansenes synspunkter om angivelse av lovens virkeområde. Departementet mener at det ikke er hensiktsmessig å forsøke å angi virkeområdet mer konkret i lovs form. Det må fremkomme ytterligere kriterier og terskelverdier som tilpasses den enkelte sektor og delsektor i størst mulig grad for en nærmere avgrensning av virkeområdet. Departementet mener dette må fremkomme i forskrift. Etter direktivet forutsettes det også at det skal føres en liste over tilbydere av samfunnsviktige tjenester i hvert land direktivet gjelder, og at denne gjennomgås jevnlig og ajourføres ved behov. Dette tilsier også at regelverket og virkeområdet har en viss dynamikk, som er vanskelig å ivareta i lovs form.

Som noen høringsinstanser har påpekt er et alternativ å endre sektorlovgivning slik at det blir klart at det stilles krav i tråd med NIS-direktivet. For de virksomhetene som ikke er omfattet av relevant sektorregelverk måtte det blitt utformet nye lovregler. Departementet har funnet en slik tilnærming mindre hensiktsmessig. Mange virksomheter er allerede underlagt sikkerhetskrav, men det er ikke alltid klart om disse omfatter krav om digital sikkerhet. Departementet mener at et felles regelverk om digital sikkerhet vil kunne fjerne slik tvil. Om det er ikke er digitale sikkerhetskrav i sektorregelverket, vil den nye loven etablere dette. Departementet mener også at et felles regelverk er lettere å forvalte med tanke på harmonisering både nasjonalt og internasjonalt. Videre er en tverrsektoriell lov et godt utgangspunkt for videre regelverksutvikling blant annet i tråd med den felles satsingen innen cybersikkerhet i EØS eller andre nasjonale behov. Departementet mener det er fornuftig å følge prosessene i EU, særlig i tilknytning til NIS-direktivet, og i første omgang gjennomføre et regelverk som legger til rette for innføring av direktivet slik det foreligger. EU-kommisjonens revisjonsrapporter og erfaringer i andre EØS-stater, vil spille en viktig rolle for hvordan departementet deretter ønsker å videreutvikle loven, både med hensyn til virkeområde, men også med tanke på sikkerhetskrav og kontroll.

I tråd med direktivet artikkel 1 nr. 3 foreslår departementet i loven § 2 andre ledd et uttrykkelig unntak for virksomheter som omfattes av lov om elektroniske tillitstjenester. Av artikkel 1 nr. 3 følger det også at virksomheter som er omfattet av direktiv 2002/21 artikkel 13a og 13b ikke er omfattet av direktivets sikkerhets- og varslingskrav. Direktivet er gjennomført i norsk rett i

ekomloven. Departementet ser ikke behov for en bestemmelse om dette i loven, da ekomsektoren ikke er nevnt i lovforslaget § 2 første ledd.

Departementet viser også til at EU-kommisjonen i sin kommunikasjon (COM/2017/0476 final) «Making the most of NIS» nyanserer unntaket for «ekom-virksomheter» noe. Det følger av kommunikasjonen punkt 5.2 at dersom virksomheten i tillegg tilbyr digitale tjenester, jf. direktivet vedlegg III eller samfunnsviktige tjenester, jf. direktivet vedlegg II, punkt 7, så må virksomheten når det gjelder disse tjenestene forholde seg til bestemmelsene i direktivet.

Departementet legger til grunn EU-kommisjonens forståelse av direktivet. Departementet foreslår derfor at virksomheter underlagt ekomregelverket ikke uttrykkelig unntas virkeområdet, da det kan fremstå misvisende dersom virksomheten likevel vil være omfattet dersom de i tillegg tilbyder digitale tjenester eller samfunnsviktige tjenester.

Departementet bemerker at NIS2-direktivet opphever unntaket for virksomheter omfattet av ekomregelverket og lov om tillitstjenester. Det fremgår i fortalepunkt 92 at det er ønskelig at disse virksomhetene drar nytte av det rammeverket som er etablert, ikke minst etableringen av responsmiljøer for varsling og arbeidet i NIS samarbeidsgruppe.

NIS-direktivets artikkel 1 nr. 7 oppstiller et unntak fra direktivet der det foreligger EØS-regelverk som stiller minst like strenge krav til sikkerhet og varsling som kravene etter direktivet.

EU-kommisjonen fremhever finanssektoren, og særlig sektorene bank- og finansmarkedsinfrastruktur som nevnt i nr. 3 og 4 i vedlegg II, som en sektor med relevant sektorregelverk om sikkerhet og varsling. Disse sektorene trekkes også frem i NIS-direktivets fortalepunkt 12 og 13.

I lovforslaget § 5 er det inntatt en bestemmelse som regulerer forholdet til andre lover. I bestemmelsen fremgår det at «[k]rav om sikkerhet og varsling i §§ 7, 8, 10 og 11 gjelder ikke så langt tilsvarende krav er fastsatt i eller i medhold av annen lov.»

Bestemmelsen regulerer forholdet mellom den foreslåtte loven og annen lovgivning som stiller krav om sikkerhet og varsling. Dersom tilbyderen er underlagt sikkerhets- og varslingskrav som minst tilsvarer kravene i den foreslåtte loven, skal kravene i annen lov benyttes. Tilsvarende gjelder for krav i forskrift gitt i medhold av lov.

Et eksempel på lovgivning med sikkerhets- og varslingskrav som ikke tilsvarer kravene i ny lov om digital sikkerhet er personvernforordningen, gjennomført som lov ved personopplysningsloven. Etter forordningen artikkel 32 skal behandlingsansvarlige og databehandlere sørge for egnet sikkerhetsnivå og etter artikkel 33 melde fra til tilsynsmyndigheten ved brudd på personopplysningssikkerheten. Disse kravene er knyttet til sikkerheten til opplysningene om personene og ikke sikkerheten i nettverks- og informasjonssystemene som sådanne.

Bank og finansmarkedsmarkedsinfrastruktur er eksempler på sektorer som har sikkerhets- og varslingskrav som tilsvarer kravene i den nye loven. Begge sektorene er omfattet av forskrift 21. mai 2003 nr. 630 om bruk av informasjons- og kommunikasjonsteknologi som stiller krav til sikkerhet (§ 5) og avviks- og endringshåndtering (§ 9).

Forslaget til § 5 vil ha en todelt funksjon. Dels gjennomfører den direktivets bestemmelse i artikkel 1 nr. 7 om at EØS-basert regelverk går foran direktivet dersom sikkerhets- og varslingskravene tilsvarer kravene i direktivet. Bestemmelsen vil imidlertid også gjelde for nasjonale sektorspesifikke regler om sikkerhet og varsling som i utgangspunktet ikke er EØS-baserte, men som likevel oppfyller NIS-direktivets krav. I slike tilfeller vil NIS-direktivets krav til sikkerhet og varsling bli ivaretatt av de sektorspesifikke reglene i stedet for de generelle kravene i lov om digital sikkerhet.

Til forskjell fra unntaksbestemmelsen i lovforslaget § 2 andre ledd, vil § 5 ikke unnta tilbyderen fra virkeområdet til loven. Dette innebærer for tilbydere av samfunnsviktige tjenester at identifiseringsprosessen for virksomheter i hver sektor fremdeles skal gjennomføres, og myndighetene i sektoren vil pålegges oppgaver etter loven. Anvendelse av regelen foreslått i § 5 innebærer at underleggelse av loven ikke vil medføre endringer for de aktuelle virksomhetene ved sikkerhet og varsling, ettersom de allerede følger minst tilsvarende krav. Konsekvensene for virksomhetene vil derfor være begrenset, ettersom kravene i annen lov skal benyttes.

Myndigheter eller andre funksjoner i sektoren vil få nye oppgaver gjennom loven. Bakgrunnen for at departementet ønsker at virksomheter som allerede følger regelverk med minst tilsvarende krav om sikkerhet og varsling underlegges loven, er at det vil knytte sektorene sammen i et felles regelverk. Etter departementets syn vil dette gi en bedre tverrsektoriell oversikt, og gi grunnlag for samarbeid knyttet til forebyggende digital sikkerhet, og også operasjonelt samarbeid, både nasjonalt og internasjonalt.

Departementet har vurdert om det er grunn til å gjøre flere uttrykkelige unntak fra lovens virkeområde for sektorer hvor eksisterende sektorlovgivning mer enn oppfyller sikkerhets- og varslingskravene. Departementet har særlig vurdert om det bør gjøres unntak for virksomheter underlagt sikkerhetsloven. Dette kunne vært aktuelt fordi tiltak som skal sikre nasjonal sikkerhet i utgangspunktet er et nasjonalt anliggende og fordi artikkel 1 nr. 6 uttrykkelig uttaler at direktivet ikke berører tiltak som statene treffer for å ivareta blant annet nasjonal sikkerhet. Departementet har likevel kommet til å ikke foreslå et slikt unntak. Det anses hensiktsmessig at også virksomheter underlagt sikkerhetsloven er en del av rammeverket for digital sikkerhet, og at det for disse virksomhetene heller vil være aktuelt å benytte unntaksbestemmelsen i § 5, eventuelt at det i forskrift kan angis særskilte regler. Etter departementets vurdering har det selvstendig verdi at tilbydere av samfunnsviktige tjenester i Norge utpekes og identifiseres.

3.5.2 Tilbydere av samfunnsviktige tjenester

Tilbydere av samfunnsviktige tjenester er definert i lovforslaget § 6 første ledd, og omfatter virksomheter innenfor sektorer nevnt i NIS-direktivets vedlegg II, og som oppfyller kriteriene som følger av direktivet artikkel 5 nr. 2.

Et vilkår i definisjonen av en samfunnsviktig tjeneste er at en hendelse vil kunne få betydelig forstyrrende virkning på tjenesteleveransen, se lovforslaget § 6 andre ledd og direktivet artikkel 5 nr. 2 bokstav c. Vilkåret «betydelig forstyrrende virkning» tilsvarer direktivet artikkel 6. I § 6 andre ledd bokstav a til g angis hva det skal legges vekt på ved vurderingen av om en hendelse kan få betydelig forstyrrende virkning. Vurderingstemaet er hvilken samfunnsvirkning en hendelse i virksomheten kan få. Det er dermed ikke bare spørsmål om en hendelse helt eller delvis kan slå ut den enkelte virksomhetens tjenesteleveranse. Dette er et viktig moment for direktivets og dermed også lovens virkeområde. Det er meningen å omfatte de virksomheter som er så viktig for samfunnet at en hendelse hos virksomheten får negativ virkning for samfunnet.

Nasjonal sikkerhetsmyndighet har på vegne av departementet og i samarbeid med berørte sektormyndigheter gjort en nærmere og foreløpig vurdering av hvilke kriterier og terskelverdier som kan benyttes for å identifisere hvilke virksomheter som skal anses som tilbydere av samfunnsviktige tjenester etter lovforslaget. Nærmere kriterier for identifisering av tilbydere av samfunnsviktige tjenester vil reguleres i forskrift. Dette vil oppføres i en liste som omtalt over under punkt 3.2.2.

Ettersom formålet med en opplistet oversikt også er å sikre en overgripende harmonisering mellom statenes bedømming av hva som anses som samfunnsviktige tjenester, må det tas hensyn til hvordan andre stater gjør sine avveininger av hva som utgjør samfunnsviktige tjenester, samtidig som det må tilpasses norske forhold.

Direktoratet for samfunnssikkerhet og beredskap har i sitt høringssvar foreslått at lovens virkeområde utvides utover de sektorer som omfattes av NIS-direktivet slik at det harmoniserer med DSBs rammeverk «Samfunnets kritiske funksjoner». En slik tilnærming innebærer at virkeområdet utvides til blant annet å omfatte politiets og påtalemyndighetens ansvarsområder, redningstjenesten, mat- og drivstofforsyning og meteorologiske og satellittbaserte tjenester. Etter departementets vurdering er det på nåværende tidspunkt mest hensiktsmessig å sørge for en lov som gjennomfører NIS-direktivets bestemmelser. Dersom NIS2-direktivet blir tatt inn i EØS-avtalen vil dette utløse behov for å se på virkeområdet på nytt. Departementet viser videre til at EU har vedtatt et direktiv (EU) 2022/2557 om motstandsdyktigheten til kritiske enheter, hvor det stilles krav om å koordinere gjennomføringen av direktivet med gjennomføringen av NIS2-direktivet. En vurdering av forholdet mellom samfunnets kritiske funksjoner og lov om digital sikkerhet hører naturlig inn i dette arbeidet.

Ved identifisering av virksomheter underlagt loven vil det som utgangspunkt være to mulige tilnærminger, enten utpeking ved enkeltvedtak (ovenfra og ned) eller selv-identifisering basert på nærmere fastsatte kriterier og terskelverdier (nedenfra og opp).

Ovenfra og ned-tilnærmingen er for eksempel valgt for utpeking av grunnleggende nasjonale funksjoner og virksomheter med avgjørende betydning for disse etter sikkerhetsloven. Fordelen med en slik tilnærming er at den gir sektormyndighetene god oversikt over verdikjedene og avhengighetene i sektoren. Ulempen er at en slik løsning blir svært ressurskrevende da loven vil ha et vesentlig bredere nedslagsfelt enn sikkerhetsloven. En ovenfra og ned-tilnærming vil medføre at det tar lengre tid før loven får anvendelse, da utpeking og den foregående analysen vil ta tid. På den andre siden vil en nedenfra og opp-tilnærming gi sektormyndighetene mindre kontroll, men likevel ikke mer enn det som kan aksepteres.

Over tid vil sektormyndighetene kunne danne seg et bedre bilde over kravene til digital sikkerhet i sektoren og ha oversikt over virksomhetene og regelverket.

I høringssvaret fra *Teknisk-naturvitenskapelig forening* påpekes det at det er en risiko for at virksomheter enten skriver seg unødvendig inn i loven og dermed pådrar seg unødvendige kostnader, eller definerer seg ut av lovens virkeområde og dermed ikke har tilstrekkelig sikkerhet eller varsler ved alvorlige hendelser. Ved valg av en nedenfra og opp-tilnærming vil det være en forutsetning at det utarbeides tilstrekkelig konkrete terskelverdier slik at eventuelle usikkerheter rundt hvorvidt en virksomhet er omfattet blir redusert i størst mulig grad.

Etter departementets syn fremstår en nedenfra og opp-tilnærming, der virksomhetene selv vil identifisere seg, som den mest hensiktsmessige. For å sikre at virksomheter som ikke tilfredsstiller terskelverdiene, men som kan være i en særstilling, og slik likevel har en rolle at de bør omfattes av loven, mener departementet det vil være hensiktsmessig at sektormyndighet gis anledning til å utpeke enkeltvirksomheter loven skal gjelde for. Dette vil gi sektormyndighetene nødvendig fleksibilitet, og ligner på vedtakskompetansen som sikkerhetsmyndigheten har etter sikkerhetsloven § 1-3. Også her må nærmere vilkår for en slik utpeking fremgå av underliggende regelverk og departementet vurderer at forskriftshjemmelen i § 2 tredje ledd er dekkende for dette formålet.

Ved utarbeidelsen av terskelverdier er det lagt til grunn arbeid gjort i andre europeiske land, særlig Storbritannia og Sverige. Den foreløpige kartleggingen av terskelverdiene er utarbeidet av Nasjonal sikkerhetsmyndighet i dialog med Direktoratet for samfunnssikkerhet og beredskap og sektormyndighetene i de sektorene som omfattes av loven. Terskelverdiene er søkt harmonisert på tvers av sektorer slik at innslagspunktet for loven vil være likest mulig uavhengig av sektor.

Videre er det lagt vekt på å benytte allerede eksisterende sektorregelverk, herunder terskelverdier der det foreligger, og harmonisere disse med terskelverdiene etter loven. Terskelverdiene identifiserer hvilke tjenester som er viktige for å opprettholde kritiske samfunnsmessige eller økonomiske aktiviteter, jf. lovforslaget § 6 første ledd bokstav a og direktivet artikkel 5 nr. 2, jf. artikkel 4 nr. 4. Virksomheter som yter disse tjenestene vil være underlagt loven. Tilnærmingen med terskelverdier vil fungere ved at det innenfor hver sektor eksempelvis angis kategorier av tjenester eller størrelser på produksjon, drift eller brukere. Dersom virksomheten leverer en tjeneste som oppfyller kriteriene, vil den være omfattet av lovens virkeområde. Terskelverdiene som identifiserer tjenestene skal utformes så konkret at det skal være mulig for virksomheter selv å avgjøre hvorvidt de leverer den omtalte tjenesten.

3.5.3 Tilbydere av digitale tjenester

«Tilbyder av digitale tjenester» og «digitale tjenester» er definert i direktivet artikkel 4 henholdsvis nr. 6 og 5, og omfatter tilbydere av skytjenester, digitale markedsplasser og digitale søkemotorer. Digitale tjenester er omtalt i direktivets fortalepunkt 15 til 17.

På dette området er hensikten i enda større grad å få ensartede regler i hele EØS, både hva gjelder virkeområde og sikkerhets- og varslingsplikter. De aktuelle virksomhetene må dermed vurdere om de er omfattet ut ifra lovforslagets bestemmelser. Tilbydere av digitale tjenester er definert i lovforslaget § 9 første ledd. Også definisjonen av digitale tjenester tilsvarer NIS-direktivets definisjoner. Departementet ser det som uhensiktsmessig å definere dette på en annen måte enn det som følger av direktivet.

Nærmere krav og presiseringer for å sikre like forutsetninger i Norge som i resten av EØS forutsetter at det i forskrift tas inn bestemmelser som spesifiserer hvilke momenter tilbydere av digitale tjenester skal ta i betraktning når de fastsetter og iverksetter tiltak for å garantere et nivå av sikkerhet i nettverks- og informasjonssystemer som benyttes i leveransen av tjenester som nevnt i vedlegg III til NIS-direktivet. Herunder også hvilke kriterier som skal tas i betraktning ved fastsettelsen av hvorvidt en hendelse har betydelig innvirkning på leveringen av disse tjenestene.

I direktivet artikkel 16 nr. 11 fremgår det at direktivet ikke skal gjelde for tilbydere av digitale tjenester som er mikrovirksomheter og små virksomheter, slik dette er definert i Kommisjonsrekommandasjon 2003/361/EF av 6. mai 2003. Det vil si at virksomheter som har færre enn 50 ansatte og som har en årlig omsetning eller årlig samlet balanse som ikke overstiger 10 millioner euro ikke omfattes av direktivet. Departementet ser det som mest hensiktsmessig å regulere dette og en nærmere definisjon av mikrovirksomheter og små virksomheter i forskrift.

4 Lovens geografiske virkeområde

4.1 Gjeldende rett

Som beskrevet over er det i norsk lovgivning i dag ikke ett samlet regelverk som innholdsmessig tilsvarer NIS-direktivet. Eksisterende tverrsektorielt og sektorspesifikt regelverk om digital sikkerhet er for øvrig heller ikke samlet sett dekkende for å oppfylle NIS-direktivet.

Sikkerhetsloven gjelder for virksomheter på Svalbard, Jan Mayen og i bilandene i den utstrekning Kongen bestemmer, jf. sikkerhetsloven § 1-2 tredje ledd. I sikkerhetsloven § 1-2 fjerde ledd fremgår det at Kongen i statsråd kan gi forskrift om lovens virkeområde. For øvrig er det ikke egne bestemmelser om lovens geografiske virkeområde.

Det geografiske virkeområdet til personopplysningsloven følger av § 4, hvor det i første ledd heter at «[l]oven og personvernforordningen gjelder for behandling av personopplysninger som utføres i forbindelse med aktivitetene ved virksomheten til en behandlingsansvarlig eller en databehandler i Norge, uavhengig av om behandlingen finner sted i EØS eller ikke». Etter § 4 fjerde ledd kan Kongen i forskrift gi nærmere bestemmelser om lovens anvendelse på Svalbard og Jan Mayen.

4.2 Direktivet

4.2.1 Tilbydere av samfunnsviktige tjenester

Direktivet gjelder i EØS-stater og for virksomheter som er etablert på statenes territorium. For øvrig er det ikke særlige bestemmelser om geografisk virkeområde for tilbydere av samfunnsviktige tjenester.

4.2.2 Tilbydere av digitale tjenester

For tilbydere av digitale tjenester gir direktivet bestemmelser om det geografiske virkeområdet. Det følger av direktivet artikkel 18 nr. 1 og 2 at en tilbyder av digitale tjenester anses å være underlagt jurisdiksjonen i den EØS-staten hvor den har sitt hovedforetak. Videre anses virksomheten å ha sitt hovedforetak der den har sitt hovedkontor. Tilbydere som ikke er etablert i EØS, men som tilbyr digitale tjenester i EØS, skal utpeke en representant. Representanten skal være etablert i en av EØS-statene hvor tjenestene tilbys. Tilbyderen av digitale tjenester skal anses som underlagt jurisdiksjonen til staten hvor representanten er etablert.

4.3 Forslaget i høringsnotatet

Departementet foreslo i høringen at Kongen i forskrift kan bestemme at loven helt eller delvis skal gjelde for Svalbard og Jan Mayen.

4.4 Høringsinstansenes syn

Ingen høringsinstanser hadde innspill til lovens geografiske virkeområde.

4.5 Departementets vurderinger

Som utgangspunkt vil direktivets geografiske virkeområde tilsvare EØS-avtalens virkeområde. Det vil si at direktivet vil gjelde på norsk territorium, jf. EØS-avtalen artikkel 126. Ut i fra en tradisjonell folkerettslig tilnærming betyr dette at EØS-avtalen gjelder det geografiske området hvor det utøves suverenitet, det vil si på landjorden, territorialfarvannet og luftrommet. Kontinentalsokkelen, den økonomiske sonen og den tilstøtende sonen omfattes ikke.

Svalbard, Jan Mayen og bilandene er underlagt norsk suverenitet, men står likevel i en særstilling da de er unntatt fra virkeområdet til EØS-avtalen. Departementet mener at også Svalbard, Jan Mayen og bilandene bør omfattes av en nasjonal lov om digital sikkerhet. Departementet mener at det bør fastsettes i forskrift om og eventuelt i hvilken utstrekning og med hvilke stedlige tilpasninger loven også skal gjelde for Svalbard, Jan Mayen og bilandene.

For tilbydere av digitale tjenester som ikke er etablert i EØS, men som tilbyr tjenester i EØS,

følger det av direktivet artikkel 18 nr. 2 at tilbyderen må oppnevne en representant. Representanten må være etablert i et av landene der tjenesten tilbys.

Departementet foreslår en egen bestemmelse i § 12 med krav om at tilbydere av digitale tjenester som ikke har sitt hovedkontor i Norge eller en annen EØS-stat, og som tilbyr digitale tjenester i Norge, skal utpeke en representant i Norge, med mindre tilbyderen har utpekt en representant i en annen EØS-stat hvor tjenestene tilbys. Det kan synes lite hensiktsmessig å oppstille en plikt til å utpeke en representant andre steder, ettersom loven her i så fall ikke skal gjelde. Plikten til å utpeke kommer først på spissen dersom man ikke har gjort det i en EØS-stat. Derfor foreslår departementet en plikt til å utpeke i Norge, med mindre man utpeker en representant i en annen EØS-stat.

På denne bakgrunn foreslår departementet en egen bestemmelse i § 3 om geografisk virkeområde og en bestemmelse i § 12 om plikt til å utpeke representant i Norge.

Det foreslås at § 3 første ledd bokstav a angir at loven gjelder for tilbydere av samfunnsviktige tjenester som er etablert i Norge og i bokstav b at den gjelder for tilbydere av digitale tjenester med hovedkontor i Norge eller som har eller skal ha en representant i Norge etter § 12. I andre ledd gis det hjemmel for at Kongen kan gi forskrift om lovens anvendelse for Svalbard, Jan Mayen og bilandene.

Direktivets artikkel 18 nr. 1 og 2 om jurisdiksjon foreslås med dette gjennomført i lovforslaget §§ 3 og 12.

5 Behandling av personopplysninger

5.1 Gjeldende rett

5.1.1 Innledning

Behandling av personopplysninger kan være nødvendig for flere oppgaver etter loven, blant annet for varslings- og tilsynsplikt, og for sikkerhetstiltak som den enkelte tilbyderen skal iverksette. Disse oppgavene kan nødvendiggjøre behandling av personopplysninger, blant annet ved innhenting og formidling av informasjon i forbindelse med en hendelse og ved tilsyn fra tilsynsmyndigheten. Det er ikke alltid disse oppgavene i utgangspunktet dreier seg om behandling av personopplysninger, men personopplysninger kan inngå i informasjonsgrunnlaget det er nødvendig å behandle ved utførelsen av oppgavene. Eksempelvis kan det ved varsling av en hendelse inngå personopplysninger i informasjonen den rammede tilbyderen oversender til det organ som er utpekt til å motta varsel. Mottak og behandling av varsler kan for eksempel inneholde personopplysninger i form av IP-adresser knyttet til digitale sikkerhetshendelser, personell som er berørt av hendelsen eller innhold som eventuelt er blitt kompromittert av hendelsen.

Etter lovforslaget skal tilbyderne iverksette «hensiktsmessige og proporsjonale tekniske og organisatoriske sikkerhetstiltak», jf. §§ 7 andre ledd og 10 andre ledd. Ettersom det er opp til den enkelte tilbyderen å vurdere hvilke tiltak som bør iverksettes, er det ikke mulig å angi nærmere når det i den forbindelse vil være nødvendig å behandle personopplysninger, og heller ikke hvilke personopplysninger som vil behandles. Enkelte eksempler på sikkerhetstiltak som kan innebære behandling av personopplysninger om ansatte i virksomheten eller personer som kommuniserer eller benytter tilbyderens tjenester kan imidlertid nevnes, så som tilgangskontroll, kontrollert dataflyt, beskyttelse av data i ro og transitt, beskyttelse av e-post og sikkerhetsovervåking.

5.1.2 Personvernforordningen og personopplysningsloven

Det stilles krav til behandling av personopplysninger i personvernforordning (EU) 2016/679 og personopplysningsloven av 20. juli 2018, som gjennomfører personvernforordningen i norsk rett.

Personvernforordningen artikkel 5 nr. 1 angir grunnleggende prinsipper for behandling av personopplysninger. Prinsippene er lovlighet, rettferdighet og åpenhet, jf. bokstav a til f om formålsbegrensning, dataminimering, riktighet, lagringsbegrensning, integritet og konfidensialitet.

Etter personvernforordningen artikkel 6 nr. 1 må det foreligge et behandlingsgrunnlag for at behandling av personopplysninger skal være lovlig, og i bokstav a til f angis mulige grunnlag. For behandling på grunnlag av artikkel 6 nr. 1 bokstav c og e kreves det etter artikkel 6 nr. 3 at grunnlaget for behandlingen fastsettes «i unionsretten eller medlemsstatens nasjonale rett som den behandlingsansvarlige er underlagt». Det må etter disse behandlingsgrunnlagene foreligge et såkalt supplerende rettsgrunnlag for behandlingen.

I artikkel 9 nr. 1 oppstilles det et utgangspunkt om at behandling av særlige kategorier av personopplysninger er forbudt. I artikkel 9 nr. 1 listes følgende opplysninger: «personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering». Unntak fra dette utgangspunktet følger av artikkel 9 nr. 2 bokstav a til j. For behandling av særlige kategorier personopplysninger må det foreligge et behandlingsgrunnlag etter artikkel 6 nr. 1, jf. fortalepunkt 51. I tillegg må grunnlaget for behandlingen følge av unionsretten eller medlemsstatenes nasjonale rett. Det må med andre ord foreligge et supplerende rettsgrunnlag for behandlingen.

Behandling av personopplysninger om straffedommer og lovovertredelser reguleres i personvernforordningen artikkel 10. Det fremgår av artikkel 10 at behandling av slike opplysninger «på grunnlag av artikkel 6 nr. 1» bare skal utføres «under en offentlig myndighets kontroll» eller dersom behandlingen er «tillatt i henhold til unionsretten eller medlemsstatenes nasjonale rett som sikrer nødvendige garantier for de registrertes rettigheter og friheter». Dersom behandlingen ikke utføres under en offentlig myndighets kontroll må det altså foreligge et supplerende rettsgrunnlag for behandling av personopplysninger etter artikkel 10.

Personvernforordningen artikkel 5 nr. 1 bokstav b bestemmer at personopplysningene skal samles inn for spesifikke, uttrykkelig angitte og berettigede formål. Videre slår bestemmelsen fast at opplysningene ikke må viderebehandles på en måte som er uforenlig med disse formålene. Behandling av opplysninger til et formål som ikke er forenlig med det opprinnelige formålet, er dermed i utgangspunktet forbudt. Dette omtales som prinsippet om «formålsbegrensning». For innhenting av opplysninger som allerede er samlet inn for uforenlige formål, eller utlevering av opplysninger som er samlet inn i medhold av bestemmelsen, til uforenlige formål, kreves et særskilt viderebehandlingsgrunnlag som oppfyller kravene i artikkel 6 nr. 4.

5.1.3 Grunnloven og internasjonale forpliktelser

Vernet av privatlivet etter Grunnloven § 102, den europeiske menneskerettighetskonvensjonen (EMK) artikkel 8, FNs konvensjon om sivile og politiske rettigheter (SP) artikkel 17 og Europarådets personvernkonvensjon setter skranker for behandling av personopplysninger. I tillegg stiller legalitetsprinsippet krav ved myndighetenes inngrep overfor den enkelte, jf. Grunnloven § 113.

Grunnloven § 102 lyder:

> «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. Statens myndigheter skal sikre et vern om den personlige integritet».

I Prop. 56 LS (2017–2018) i punkt 6.4, har Justis- og beredskapsdepartementet redegjort nærmere for krav om rettsgrunnlag etter Grunnloven:

> «Bestemmelsen kom inn i Grunnloven som ledd i grunnlovsreformen i 2014. Komiteen ga i Innst.186 S (2013–2014) punkt 2.1.9 side 27 uttrykk for at bestemmelsen «skal leses som at systematisk innhenting, oppbevaring og bruk av opplysninger om andres personlige forhold bare kan finne sted i henhold til lov, benyttes i henhold til lov eller informert samtykke og slettes når formålet ikke lenger er til stede».
>
> Grunnloven § 102 gir ikke anvisning på noen adgang til eller vilkår for å gjøre inngrep i rettigheten. Høyesterett har imidlertid lagt til grunn at det kan gjøres inngrep i retten etter Grunnloven § 102 dersom tiltaket har en tilstrekkelig hjemmel, forfølger et legitimt formål og er forholdsmessig, se Rt-2014-1105 avsnitt 28 og Rt-2015-93 avsnitt 60.»

EMK artikkel 8 lyder:

> «1. Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.
> 2. Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter».

I Prop. 56 LS (2017–2018) har Justis- og beredskapsdepartementet uttalt følgende om krav om rettsgrunnlag for behandling av personopplysninger etter EMK artikkel 8:

> «Grunnloven § 102 har klare likhetstrekk med EMK artikkel 8, og må tolkes i lys av denne, jf. Rt-2015-93 avsnitt 57. Det er etter departementets vurdering ikke holdepunkter for at Grunnloven § 102 stiller strengere krav enn EMK artikkel 8 om rettsgrunnlag for behandling av personopplysninger. Ved siden av Grunnloven § 102 må også legalitetsprinsippet, jf. Grunnloven § 113, tas i betraktning. Det følger av Grunnloven § 113 at «[m]yndighetenes inngrep overfor den enkelte må ha grunnlag i lov».
>
> […]
>
> Hva som er tilstrekkelig rettsgrunnlag for inngrep, beror på en konkret vurdering, blant annet av hvor inngripende behandlingen er. Etter departementets syn er det imidlertid ikke holdepunkter i EMDs praksis for at det gjelder et unntaksfritt krav om uttrykkelig hjemmel i

særlovgivning for behandling av personopplysninger. Departementet legger til grunn at forordningen artikkel 6 nr. 1 bokstav a, b, d og f i seg selv etter omstendighetene kan være tilstrekkelige lovhjemler. Også forordningen artikkel 6 nr. 1 bokstav c og e i kombinasjon med et supplerende rettslig grunnlag som oppfyller kravene etter ordlyden i nr. 3, kan være tilstrekkelig. Videre vil forordningens generelle regler, eksempelvis om personvernombud, forhåndsdrøftinger, den registrertes rettigheter mv., utgjøre garantier i EMKs forstand.

Samtidig er det ikke tvilsomt at forordningens generelle regler, eventuelt i kombinasjon med et supplerende rettsgrunnlag som bare oppfyller minimumskravene etter ordlyden i artikkel 6 nr. 3, ikke alltid vil gi tilstrekkelig spesifikt rettsgrunnlag eller nødvendige garantier i tråd med Grunnloven og EMK. Det blir da nødvendig å utforme mer spesifikke rettsgrunnlag og ytterligere garantier i nasjonal rett, og det vil i mange tilfeller være nødvendig med uttrykkelig hjemmel i særlovgivning. Forordningen må med andre ord tolkes og anvendes i lys av Grunnloven og EMK.

Som beskrevet nærmere i neste punkt følger det av forordningen artikkel 6 nr. 2 og 3 at det i tilknytning til et supplerende rettsgrunnlag for behandling på grunnlag av artikkel 6 nr. 1 bokstav c og e «kan» fastsettes utfyllende og spesifiserende regler om behandlingen. Kravene i Grunnloven og EMK om rettsgrunnlag for inngrep i privatlivet kan etter omstendighetene innebære at det supplerende rettsgrunnlaget må inneholde slike mer spesifikke bestemmelser som artikkel 6 nr. 2 og 3 åpner for. Hva som kreves av det supplerende rettsgrunnlaget, kan ikke besvares generelt, men må avgjøres etter en konkret vurdering.»

5.2 Direktivet

NIS-direktivet artikkel 2 nr. 1 bestemmer at personopplysninger som behandles i henhold til direktivet, skal behandles i samsvar med direktiv 95/46/EF. Direktiv 95/46/EF ble opphevet og erstattet av personvernforordningen ved sistnevntes vedtakelse, jf. personvernforordningen artikkel 94 og fortalepunkt 171. Behandling av personopplysninger i henhold til NIS-direktivet skal i dag dermed skje i overenstemmelse med reglene i personvernforordningen.

5.3 Forslaget i høringsnotatet

I høringsnotatet foreslo departementet at personopplysninger som behandles i henhold til loven skal behandles i samsvar med de til enhver tid gjeldende personopplysningsregler, nå den generelle personvernforordningen. Det ble foreslått en egen lovbestemmelse om at adgangen til å behandle personopplysninger kommer til uttrykk i et forslag til § 6, som også ville omfatte behandling av særlige kategorier av personopplysninger, jf. personvernforordningen artikkel 9 nr. 2 bokstav g.

5.4 Høringsinstansenes syn

Kun et fåtall av høringsinstansene har kommet med merknader til høringsnotatets forslag til § 6 om behandling av personopplysninger. *Datatilsynet* skriver at de ikke kan se at bestemmelsen er begrunnet og forklart i høringsnotatet, og etterlyser dermed en nærmere redegjørelse for hvordan den tilfredsstiller kravene i personvernforordningen. Videre mener Datatilsynet at bestemmelsens formulering er for lite presis til å fungere som rettslig grunnlag etter personvernforordningen, og skriver at det bør være klare referanser til de bestemmelsene i personvernforordningen som er ment å være grunnlaget for behandlingens lovlighet. Datatilsynet viser til artikkel 6 nr. 1 bokstav f og artikkel 9 nr. 2 bokstav g som aktuelle referanser, og skriver at «[b]egge disse bestemmelsene forutsetter konkrete interesseavveiinger og at det er iverksatt egnede tiltak for å verne de registrertes grunnleggende rettigheter og friheter. Det bør fremgå klart hvilke vurderinger som er gjort av nødvendighet og forholdsmessighet, hvilke momenter som er vektlagt i interesseavveiingen og hvilke tiltak som er iverksatt som vern av grunnleggende rettigheter for de registrerte».

Advokatforeningen mener at lovens § 6 også bør inneholde en spesifikk henvisning til at det også kan behandles personopplysninger som er omfattet av personvernforordningens artikkel 10 om lovovertredelser når det er nødvendig for å utføre pliktene som følger av loven. De peker på relevansen for en slik hjemmel «ettersom behandling av informasjon relatert til IKT og informasjonssikkerhet, herunder særlig sett i lys av varslingsplikt om hendelser, vil kunne innebære behandling av opplysninger om for eksempel hacking som er straffbart etter straffeloven § 201».

5.5 Departementets vurderinger

Etter høringen har departementet konkludert med at det ikke er grunn til å innta en egen bestemmelse om behandling av personopplysninger i loven, men foreslår at nærmere regler om behandling av personopplysninger kan reguleres i forskrift.

Et relevant behandlingsgrunnlag angitt i personvernforordningen er artikkel 6 nr. 1 bokstav c som gir behandlingsgrunnlag dersom og i den grad behandlingen er «nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige». Videre gir artikkel 6 nr. 1 bokstav e behandlingsgrunnlag for behandling av personopplysninger dersom og i den grad behandlingen er «nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt». Etter omstendighetene vil også behandlingsgrunnlaget som følger av artikkel 6 nr. 1 bokstav f kunne være relevant. Bokstav f gir behandlingsgrunnlag der behandlingen er «nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn». Etter personvernforordningens fortalepunkt 49 vil behandling av personopplysninger i det omfang som er strengt nødvendig og forholdsmessig for å sikre nettverks- og informasjonssikkerheten utgjøre en berettiget interesse for den berørte behandlingsansvarlige. Offentlige myndigheter kan derimot ikke benytte bokstav f som behandlingsgrunnlag i forbindelse med myndighetsutøvelse, jf. artikkel 6 nr. 1 siste ledd.

Departementet legger til grunn at lovens bestemmelser med tilhørende forskrifter langt på vei vil gi virksomhetene og myndighetene rettsgrunnlag for behandling av personopplysninger der dette er nødvendig etter personvernforordningen artikkel 6 nr. 1, jf. nr. 3 og nr. 4 og artikkel 9 og 10, for eksempel behandling av personopplysninger som er nødvendig i forbindelse med varsling. Etter departementets vurdering er det ikke hensiktsmessig å innta én generell lovbestemmelse om behandling av personopplysninger som skal gjelde både for virksomhetene som pålegges plikter, og for myndighetene etter loven. Det må vurderes konkret om det er nødvendig og forholdsmessig å behandle personopplysninger i det enkelte tilfelle, men det legges til grunn at pliktene etter loven utgjør forholdsmessige tiltak og at den registrertes rettigheter ivaretas blant annet ved at pliktene er avgrenset og ikke primært rettet mot rapportering om enkeltpersoner, jf. vilkårene i artikkel 9 nr. 2 bokstav g. Dersom det blir behov for nærmere regulering av behandling av personopplysninger, for eksempel knyttet til personopplysninger som nevnt i personvernforordningen artikkel 9 og 10, bør dette etter departementets syn inntas i forskrift, ettersom det gjør det mulig å fastsette mer konkrete og spesifikke bestemmelser. Departementet foreslår derfor en hjemmel for forskrifter om behandling av personopplysninger, jf. § 18 bokstav g. Forslaget åpner for at Kongen kan gi forskrift med nærmere bestemmelser om formålet med behandlingen, behandlingsansvar, hvilke personopplysninger som kan behandles, adgangen til viderebehandling, utlevering, deling og sletting. Som ledd i et eventuelt forskriftsarbeid kan også behovet for regulering av myndighetens videre bruk av opplysninger som innrapporteres, og forholdet til annet relevant regelverk som regulerer dette, vurderes nærmere.

6 Krav om sikkerhet

6.1 Gjeldende rett

Per i dag finnes det kun for noen sektorer regler som tilsvarer NIS-direktivets krav om sikkerhet. En rekke virksomheter er underlagt sikkerhetskrav av ulik art, men det er i mange tilfeller uklart om det kan tolkes slik at det stilles krav om digital sikkerhet. Under følger en gjennomgang av et utvalg relevante tverrsektorielle regelverk med bestemmelser om sikkerhet.

Sikkerhetsloven stiller krav om sikring av informasjonssystemer som behandler skjermingsverdig informasjon eller som i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner, kalt skjermingsverdige informasjonssystemer, jf. § 6-1. I Prop. 153 L (2016–2017) punkt 10.5.3.4 legges det til grunn at skjermingsverdige informasjonssystemer kan utpekes som skjermingsverdige objekter eller infrastruktur.

Et informasjonssystem anses å ha avgjørende betydning for grunnleggende nasjonale funksjoner dersom bortfall eller svekkelse av systemets funksjonalitet vil svekke den grunnleggende nasjonale funksjonen det inngår i eller understøtter. Med grunnleggende nasjonale funksjoner menes tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser.

Loven, med tilhørende forskrifter, stiller relativt tydelige og omfattende krav til styringen av sikkerheten i virksomheten, herunder informasjonssystemsikkerheten. Departementet legger til grunn at sikkerhetskravene mer enn oppfyller direktivets krav, og henviser derfor til Prop. 153 L (2016–2017) for en nærmere beskrivelse av kravene.

Etter personopplysningsloven § 1 gjelder personvernforordningen som norsk lov. Personopplysningsloven inneholder ikke nasjonale bestemmelser om sikkerhet ved behandlingen av personopplysninger. Personvernforordningen artikkel 5 nr. 1 bokstav f og artikkel 32 er de viktigste sikkerhetsbestemmelsene. De må imidlertid ses i sammenheng med andre bestemmelser, slik som for eksempel artikkel 24. Se for øvrig fortalepunkt 39 og 83.

Begrepet informasjonssystem brukes ikke i bestemmelsen. Likevel fremgår det klart av sammenhengen at når det brukes informasjonssystemer til å behandle personopplysninger, så må disse sikres.

Det gjøres i lovens forarbeider punkt 16.4.2 nærmere rede for forordningens regler om sikkerhet, se Prop. 56 LS (2017–2018):

> «Forordningens regler om informasjonssikkerhet følger av artikkel 32. Bestemmelsen fastslår at både den behandlingsansvarlige og databehandleren plikter å «gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen», jf. artikkel 32 nr. 1. Eksempler på slike tiltak fremgår av bokstav a til d. En angivelse av sentrale elementer i risikovurderingen følger av artikkel 32 nr. 2. Overholdelse av godkjente atferdsnormer etter artikkel 40 eller en godkjent sertifiseringsmekanisme etter artikkel 42 kan brukes som en faktor for å påvise at kravene til informasjonssikkerhet er oppfylt, jf. artikkel 32 nr. 3. Etter artikkel 32 nr. 4 skal den behandlingsansvarlige og databehandleren sikre at enhver som handler på vegne av den behandlingsansvarlige eller databehandleren bare behandler opplysninger etter instruks fra den behandlingsansvarlige, med mindre unionsretten eller medlemsstatenes rett pålegger en plikt til behandling.»

I forbindelse med høringen av den nye personopplysningsloven uttalte departementet i høringsnotatets punkt 13.5.3 om sikkerhetsbestemmelsene at:

> «Etter departementets vurdering vil imidlertid anvendelse av reglene i artikkel 32 trolig lang på vei gi samme resultat som gjeldende regler slik de er formulert i personopplysningsloven § 13 og personopplysningsforskriften kapittel 2».

Datatilsynet har i sin veileder om internkontroll og informasjonssikkerhet, blant annet tatt for seg risikovurderinger knyttet til informasjonssystemer.

For forvaltningsorganer gjelder forskrift 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften). Forskriften er fastsatt med hjemmel i forvaltningsloven § 15 a. Forskriften gjelder for elektronisk kommunikasjon med forvaltningen og for elektronisk saksbehandling og kommunikasjon i forvaltningen. Formålet med forskriften er å legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen.

Det følger av forskriften § 1 at:

> «Forskriften gjelder for elektronisk kommunikasjon med forvaltningen og for elektronisk saksbehandling og kommunikasjon i forvaltningen når ikke annet er bestemt i lov eller i medhold av lov».

Bestemmelsen får dermed anvendelse på informasjonssystemer som brukes til saksbehandling og kommunikasjon med og i forvaltningen. På samme måte som at det ikke er enkelt å trekke et skarpt skille mellom et forvaltningsorgans saksbehandling og tjenesteproduksjon, er det heller ikke uten videre enkelt å trekke en skarp grense for hvilke informasjonssystemer forskriften gjelder for.

Sikkerhetskravene følger av eForvaltningsforskriften kapittel 3, Styring og kontroll med informasjonssikkerheten. Paragraf 15 stiller krav om internkontroll. Etter første og andre ledd skal det etableres mål og strategi for informasjonssikkerheten og et tilfredsstillende system for internkontroll. Det stilles ikke eksplisitte krav om for eksempel tekniske og organisatoriske tiltak.

6.2 Direktivet

6.2.1 Tilbydere av samfunnsviktige tjenester

Sikkerhetskravene som stilles til tilbydere av samfunnsviktige tjenester følger av artikkel 14 nr. 1 og 2. Tilbyderne skal sikre de nettverks- og informasjonssystemer som de bruker for å levere den samfunnsviktige tjenesten. Tilbyderen skal treffe tekniske og organisatoriske tiltak som er hensiktsmessige og står i et rimelig forhold til risikoen som knytter seg til nettverkene og informasjonssystemene. Ved vurderingen av hvilke tiltak som er proporsjonale skal det tas hensyn til den tekniske utviklingen. For å sikre opprettholdelse av tjenesteleveransen, skal tilbyderen treffe tiltak som er egnet til å forebygge, avdekke og redusere virkningen av hendelser som truer sikkerheten i tilbyderens IKT-systemer.

Nærmere om hva som ligger i dette er bare til en viss grad omhandlet i fortalen. Det gis ikke særlig veiledning utover det som allerede følger av direktivbestemmelsene. Det fremgår av fortalepunkt 44 blant annet at landene gjennom innføring av passende lovgivningstiltak og frivillige bransjenormer skal fremme en risikostyringskultur som inkluderer risikovurdering og gjennomføring av proporsjonale sikkerhetstiltak. I fortalepunkt 46 står det at risikostyringstiltak omfatter tiltak for å identifisere risikoer for hendelser, med sikte på å forebygge, avdekke og håndtere hendelser og begrense skaden.

NIS-samarbeidsgruppen har utarbeidet retningslinjer for hva som ligger i sikkerhetskravet i *Reference document on security measures for Operators of Essential Services CG Publication 01/2018*.

Etter NIS-direktivet artikkel 3 står statene fritt til å stille strengere sikkerhetskrav enn det som følger av direktivet. Overfor tilbydere av digitale tjenester er det ikke tilsvarende nasjonalt handlingsrom, jf. artikkel 16 nr. 10.

6.2.2 Tilbydere av digitale tjenester

Sikkerhetskravene som stilles til tilbydere av digitale tjenester følger av artikkel 16. Tilbyderen skal sikre nettverks- og informasjonssystemene den bruker for å levere tjenesten. Videre skal tilbyderen ha en risikobasert tilnærming til sikkerhetsarbeidet. Den skal iverksette sikkerhetstiltak som står i et rimelig forhold til risikoen tilbyderen står overfor. Det skal også iverksettes tiltak for å forebygge og minimere virkningen av hendelser i nettverks- og informasjonssystemer, med særlig henblikk på opprettholdelse av tjenesteleveransen. Sikkerhetstiltakene skal også ta hensyn til følgende fem elementer:

- Sikkerheten i systemer og anlegg (informasjonssystemsikkerhet og fysisk sikkerhet)
- Hendelseshåndtering
- Styring av driftskontinuitet (opprettholdelse av tjenesteleveranser)
- Overvåkning, revisjon og testing
- Overholdelse av internasjonale standarder

Alle de fem punktene er nærmere spesifisert i gjennomføringsforordningen.

Det går tydelig frem av fortalen til direktivet at det skal stilles mindre strenge sikkerhetskrav til tilbydere av digitale tjenester da de anses noe

mindre viktige enn de samfunnsviktige tjenestene. Det følger dessuten av fortalepunkt 49 at blant annet på grunn av digitale tjenesters grensekryssende natur, bør de være underlagt et regelverk som er harmonisert i hele EØS. Dette er ivaretatt gjennom gjennomføringsforordningen, som etterlater lite rom for nasjonale tilpasninger.

I forordningen spesifiseres hvilke momenter tilbydere av digitale tjenester skal ta i betraktning når de fastsetter og iverksetter tiltak for å garantere et nivå av sikkerhet i nettverks- og informasjonssystemer som benyttes i leveransen av tjenester som nevnt i vedlegg III til NIS-direktivet. Videre spesifiseres hvilke kriterier som skal tas i betraktning ved fastsettelsen av hvorvidt en hendelse har betydelige konsekvenser for leveringen av disse tjenestene.

6.3 Forslaget i høringsnotatet

Departementet foreslo i høringsnotatet at krav om sikkerhet for tilbydere av samfunnsviktige tjenester og digitale tjenester tilsvarer NIS-direktivets krav om sikkerhet. Det betyr at tilbyderne skal gjennomføre en risikovurdering av nettverks- og informasjonssystemer som benyttes for å levere tjenesten. For å redusere risikoen skal tilbyderne iverksette hensiktsmessige og proporsjonale tekniske og organisatoriske sikkerhetstiltak. For å opprettholde tjenesteleveransen skal tilbyderne iverksette tiltak for å forebygge, avdekke og redusere konsekvensene av hendelser.

Departementet foreslo i høringsnotatet at Kongen kan gi forskrift med nærmere bestemmelser om sikkerhetskrav.

6.4 Høringsinstansenes syn

Enkelte høringsinstanser er positive til sikkerhetskravene som fremgår av høringsnotatet, blant andre *Domstoladministrasjonen* og *Direktoratet for IKT og fellestjenester i høyere utdanning og forskning*.

For å sikre sammenheng med øvrig virksomhetsstyring anbefaler *Direktoratet for forvaltning og IKT* (nå Digitaliseringsdirektoratet) at loven inkluderer en bestemmelse om at risikostyringen skal inngå i helhetlig styring og kontroll. Direktoratet anbefaler at man gjenbruker formuleringer fra eforvaltningsforskriften § 15, for eksempel ved å ta inn bestemmelser om at risikostyringen på IKT-sikkerhetsområdet bør være en integrert del av en helhetlig internkontroll, og at omfang og innretning på internkontrollen skal være tilpasset risiko.

I følge *Direktoratet for forvaltning og IKT* (nå Digitaliseringsdirektoratet) vil et slikt tillegg klargjøre at risikostyring innen lovens område bør knyttes til øvrig risikostyring i virksomheten. Videre at det vil sikre samsvar med annet regelverk og anbefaling i internasjonale standarder. Dersom ordensforskrifter ikke ønskes i bestemmelsen, mener direktoratet man kan oppnå noe av det samme ved å føye til i bestemmelsen at arbeidet skal være risikobasert og systematisk.

Enkelte høringsinstanser mener at kravene om sikkerhet burde være tydeligere, blant andre *Skatteetaten, Teknisk-naturvitenskapelig forening, Statens Helsetilsyn* og *Advokatforeningen*. *Advokatforeningen* er av den oppfatning at departementet før ikrafttredelse av loven må klargjøre hvilke krav som konkret stilles med tanke på risikovurdering og passende tiltak.

Næringslivets hovedorganisasjon trekker frem at implementeringen av NIS-direktivet vil bety innføring av lovgivning og nye IKT-sikkerhetskrav til tilbydere av digitale tjenester som foreløpig ikke har vært underlagt slike krav. Næringslivets hovedorganisasjon mener det er påliggende at regelverket som nå innføres er enkelt og gjennomførbart for bedriftene det omfatter, og at myndighetenes opplysnings- og informasjonsvirksomhet rundt dette er god.

6.5 Departementets vurderinger

Departementet mener det er behov for bestemmelser som stiller krav til digital sikkerhet i virksomhetene som er omfattet av lovforslaget. Selv om enkelte regelverk til dels kan ha relativt like sikkerhetskrav, mener departementet det likevel er mest hensiktsmessig at det blir stilt likelydende krav om digital sikkerhet innenfor kategoriene tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester. Kravene kommer til uttrykk i lovforslaget §§ 7 og 10. Departementet vil likevel understreke at kravene som stilles etter loven og direktivet utgjør minimumskrav til digital sikkerhet, og at de ikke er til hinder for at tilbyderne iverksetter strengere sikkerhetstiltak enn de som følger av direktivet og loven. Dette følger også av direktivets fortalepunkt 6.

Det er et uttalt mål med lovforslaget at de samfunnsviktige og digitale tjenestene faktisk blir levert. Det er direkte sammenheng mellom formålsbestemmelsen og sikkerhetskravene, for å gjøre det tydeligere hva som er poenget med

sikringen og hvilke nettverks- og informasjonssystemer som skal sikres.

Departementet har ved utforming av bestemmelsen om sikkerhetskrav ment å fange opp det samme som direktivets krav. Direktivet konkretiserer i liten grad sikkerhetskravet utover det som følger av bestemmelsene.

Flere av høringsinstansene, blant andre *Advokatforeningen*, har pekt på at kravene om sikkerhet bør være tydeligere, og at det bør klargjøres hvilke krav som konkret stilles med tanke på risikovurdering og passende tiltak.

Departementet er enig i at innholdet i krav om sikkerhet, herunder kravet om å iverksette hensiktsmessige og proporsjonale tekniske og organisatoriske sikkerhetstiltak, bør presiseres. En tydeliggjøring av hvilke krav som stilles vil etter departementets syn bidra til at formålet med sikkerhetskravene, og i forlengelsen lovens og direktivets formål, oppnås. Videre vil det gjøre kravene mer forutberegnelige og sikre en likere praktisering. Dette vil være både i tilbydernes og tilsynsmyndighetenes interesse. En tydeliggjøring av krav om sikkerhetstiltak har også en side til sanksjonering ved overtredelser av kravene.

Utover den generelle føringen i direktivet om at det skal stilles noe mindre strenge krav til tilbydere av digitale tjenester, gis det ikke særlige føringer på hvor store forskjeller det er snakk om eller hva dette betyr i praksis. For tilbydere av digitale tjenester er, i tråd med direktivet, momenter som skal hensyntas konkretisert i lovforslaget § 10 andre ledd bokstav a til e. Kravene som stilles til tilbydere av digitale tjenester er ytterligere konkretisert i gjennomføringsforordningen. Departementets vurdering er at forordningens bestemmelser bør vedtas som forskrift til den loven som denne proposisjonen omhandler. En slik forskrift vil i så fall bli hørt på vanlig måte på et senere tidspunkt.

For tilbydere av samfunnsviktige tjenester vil NIS-samarbeidsgruppens retningslinjer gi støtte til tilbydernes vurderinger ved implementering av tiltak. Det er departementets vurdering at hvis tilbydere følger «NSMs grunnprinsipper for IKT-sikkerhet», vil de ivareta kravene som fremgår av loven og retningslinjene. I den forbindelse ønsker departementet også å vektlegge viktigheten av å se digital sikkerhet i sammenheng med tilbydernes mer generelle sikkerhetsstyringssystem og tilbydernes overordnede styringssystem.

Krav om sikkerhet etter lovforslaget §§ 7 og 10 reguleres nærmere i forskrift, jf. lovforslagets § 18 bokstav a. Samtidig må nærhetsprinsippet og sektoransvaret tas i betraktning. Hvilke tiltak som bør iverksettes kan variere avhengig av hvilken sektor det er tale om og den enkelte tilbyderens egenart. En for detaljert regulering i forskrift kan i lys av dette være lite hensiktsmessig. Den digitale utviklingen taler også for at reguleringen bør være dynamisk og fleksibel. Ved utforming av forskrift om krav om sikkerhet for tilbydere av samfunnsviktige tjenester må derfor behovet for tydeligere krav balanseres mot behovet for dynamiske og fleksible krav. Anbefalingen fra *Direktoratet for forvaltning og IKT* (nå Digitaliseringsdirektoratet) om å knytte risikostyring innen digital sikkerhet til øvrig risikostyring i virksomheten vil være et av flere momenter som må vurderes nærmere fastsatt i forskrift.

I lovforslaget §§ 7 og 10 i andre ledd andre punktum vises det til at det ved vurderingen av hva som er et forsvarlig sikkerhetsnivå blant annet skal ses hen til den teknologiske utviklingen. Dette følger også av direktivet, men det er ikke presisert noe nærmere. Etter departementets vurdering bør den teknologiske utviklingen hensyntas både med tanke på nye trusler og sårbarheter og oppdatering av tiltak eller iverksetting av nye tiltak.

Det følger av lovforslaget § 5, at i den grad tilstrekkelig sikkerhet oppnås gjennom gjeldende regelverk, vil loven ikke medføre endringer. I motsatt fall vil tilbyderen måtte følge lovens sikkerhetskrav.

7 Krav om varsling

7.1 Gjeldende rett

I sektorene er det ulike krav til varsling av hendelser. En rekke sektorregelverk har generelle krav om varsling ved hendelser. Enkelte regelverk har konkrete krav til varsling ved digitale hendelser. Enkelte regelverk er det ikke krav til varsling av hendelser. Under følger en gjennomgang av et utvalg relevante tverrsektorielle regelverk med bestemmelser om varsling.

Ifølge sikkerhetsloven § 4-5 skal virksomheten varsle sikkerhetsmyndigheten og sektormyndigheten dersom den har blitt rammet av eller det er begrunnet mistanke om at sikkerhetstruende virksomhet har rammet eller vil kunne ramme virksomheten. Sikkerhetstruende virksomhet er i loven § 1-5 nr. 4 definert som tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser. Etter § 4-5 andre ledd er det også varslingsplikt selv om ikke egen virksomhet er truet, men «dersom den får kunnskap om en planlagt eller pågående aktivitet som kan medføre en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet.»

Paragraf 4-5 første ledd bokstav c bestemmer at det også skal varsles om alvorlige brudd på krav til sikkerhet som følger av loven for øvrig. Hva som er årsaken til sikkerhetsbruddet har ikke betydning, hvilket innebærer at også ikke tilsiktede sikkerhetsbrudd skal varsles.

Det følger av særmerknaden til bestemmelsen at «[e]n forutsetning for at myndighetene skal kunne ha oversikt over sikkerhetstilstanden i de ulike samfunnssektorene, er at myndighetene får rettidig og tilstrekkelig informasjon om hendelser av betydning». Verken loven eller forskriftene konkretiserer ytterligere hva slags informasjon varselet skal inneholde.

I personopplysningsloven følger det av personvernforordningen artikkel 33 nr. 1 at brudd på personopplysningssikkerheten skal varsles til tilsynsmyndigheten. Brudd på personopplysningssikkerheten er i artikkel 4 nr. 12 definert som «et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet».

Artikkel 33 nr. 3 angir hva varselet skal inneholde av opplysninger. Behandlingsansvarlig skal varsle senest 72 timer etter å ha fått kjennskap til bruddet.

eForvaltningsforskriften stiller ikke krav om at virksomheten skal varsle om brudd på sikkerhetskravene i forskriften § 15.

7.2 Direktivet

7.2.1 Tilbydere av samfunnsviktige tjenester

Det følger av artikkel 14 nr. 3 at tilbydere av samfunnsviktige tjenester uten unødig opphold skal varsle tilsynsmyndigheten eller det nasjonale responsmiljøet om hendelser som virker betydelig inn på kontinuiteten i de samfunnsviktige tjenestene de yter.

I artikkel 4 nr. 7 defineres en «hendelse» som «ethvert tilfelle av reell negativ virkning på sikkerheten i nettverks- og informasjonssystemer». Med begrepet «sikkerhet i nettverks- og informasjonssystemer» menes «den evnen nettverk eller informasjonssystemer har til å tåle, på et gitt tillitsnivå, enhver handling som går ut over tilgjengeligheten, autentisiteten, integriteten eller tilliten til lagrede eller overførte eller behandlede data eller tilknyttede tjenester som tilbys eller er tilgjengelige via slike nettverks- og informasjonssystemer», jf. artikkel 4 nr. 2.

Det ligger i begrepet «ethvert tilfelle» at årsaken til hendelsen er irrelevant. Det som betyr noe er om tjenesteleveransen er redusert. Sett hen til nevnte definisjoner kan det imidlertid ikke bare vurderes om tjenestens tilgjengelighet er berørt. Hendelser som har negativ innvirkning på autentisitet, integritet eller konfidensialitet til data eller relaterte tjenester, kan potensielt utløse en varslingsplikt.

Ved vurderingen av om innvirkningen har vært betydelig skal det legges vekt på antall brukere av tjenesten som påvirkes, hendelsens varighet og størrelsen på det geografiske området som berøres av hendelsen. Varselet skal dessuten inneholde nok

opplysninger til at det kan fastslås om hendelsen har virkninger utover Norges grenser.

Varsling av hendelser skal ikke medføre utvidet ansvar for tjenestetilbyderen. I fortalepunkt 57 trekkes det frem at ved eventuell offentliggjøring av hendelser må hensyn til publikums behov for informasjon veies opp mot mulige omdømme- og kommersielle konsekvenser for den som er rammet av hendelsen. I denne sammenhengen må myndighetene ta særlig hensyn til behovet for å holde informasjon om produktsårbarheter hemmelig frem til det foreligger en tilstrekkelig god løsning på problemet.

Det følger av fortalepunkt 47 at kompetente myndigheter skal kunne utstede nasjonale retningslinjer om når og på hvilken måte tilbydere av samfunnsviktige tjenester skal varsle om hendelser.

Dersom det foreligger en hendelse som har betydelig innvirkning på opprettholdelsen av tjenesteleveransen, skal tilbyderen av den samfunnsviktige tjenesten varsle tilsynsmyndigheten eller det nasjonale responsmiljøet «uten unødig opphold». I veilederen for varsling utgitt av NIS-samarbeidsgruppen *Reference document on Incident Notification for Operators of Essential Services Circumstances of notification CG Publication 02/2018* er det gitt retningslinjer for tidspunktet for varsling.

7.2.2 Tilbydere av digitale tjenester

Det følger av artikkel 16 nr. 3 at tilbydere av digitale tjenester uten unødig opphold skal varsle tilsynsmyndigheten eller det nasjonale responsmiljøet om hendelser som virker betydelig inn på leveringen av en tjeneste som nevnt i vedlegg III og som de tilbyr i EØS.

Omtalen over av definisjonene av begrepene «hendelse» og «sikkerheten i nettverks- og informasjonssystemer» er relevant også her.

For tilbydere av digitale tjenester skal det tas hensyn til følgende parametere når det skal fastslås om virkningen av en hendelse er betydelig:

- antallet brukere som påvirkes av hendelsen, særlig brukere som er avhengig av tjenesten for å kunne yte egne tjenester
- hendelsens varighet
- størrelsen på det geografiske området som berøres av hendelsen
- omfanget av forstyrrelsen for tjenestens funksjon
- omfanget av virkningen for økonomiske og samfunnsmessige aktiviteter

De fem punktene er nærmere spesifisert i gjennomføringsforordningen.

Slik som artikkel 14 nr. 3 avsluttes også artikkel 16 nr. 3 med at varsling av hendelser ikke skal medføre utvidet ansvar for tjenestetilbyderen.

Tilsvarende som for tilbydere av samfunnsviktige tjenester, skal tilbydere av digitale tjenester varsle om hendelser som har betydelig innvirkning på opprettholdelsen av tjenesteleveransen «uten unødig opphold».

7.3 Forslaget i høringsnotatet

Departementet foreslo i høringsnotatet at krav om varsling for tilbydere av samfunnsviktige tjenester og digitale tjenester tilsvarer NIS-direktivets krav om varsling.

Videre ble det foreslått at tilbydere av samfunnsviktige tjenester skal varsle det organ Kongen utpeker om hendelser som har betydelig innvirkning på opprettholdelsen av tjenesteleveransen. Varselet skal inneholde nok opplysninger til at det kan fastslås om hendelsen har virkninger utover Norges grenser. Varslingsplikten ble foreslått til å bare gjelde dersom tilbyderen har tilgang til informasjon som er nødvendig for å kunne vurdere om hendelsen har betydelig innvirkning på tjenesteleveransen.

Departementet foreslo at Kongen kan gi forskrift med nærmere bestemmelser om varslingskrav.

7.4 Høringsinstansenes syn

Enkelte høringsinstanser mener at kravene om varsling burde være tydeligere, blant andre *Skatteetaten, Statens Helsetilsyn* og *Advokatforeningen*. *Advokatforeningen* mener det er viktig for pliktsubjektenes etterlevelse av regelverket at krav til når varsel skal inngis og innhold i varselet utpensles ytterligere i forskrifter og eventuelle veiledninger. *Kartverket, Utlendingsdirektoratet* og *Statens Helsetilsyn* mener det må klargjøres hvordan de som er underlagt flere regelverk skal varsle flere responsmiljøer og tilsynsmyndigheter, og hvordan ansvars- og myndighetsfordelingen er mellom de ulike responsmiljøene og tilsynsmyndighetene. *Kartverket* og *Utlendingsdirektoratet* mener videre at det vil det være mer hensiktsmessig med et felles varslingssystem for virksomhetene.

Direktoratet for samfunnssikkerhet og beredskap støtter krav om varsling av alvorlige digitale

sikkerhetshendelser og mener det vil gi tilgang til informasjon om både trusler og sårbarhet – en kunnskap som vil bidra til enda bedre arbeid med digital sikkerhet i fremtiden. Direktoratet for samfunnssikkerhet og beredskap mener videre at varsling av uønskede hendelser som rammer nettverks- og informasjonssystemer må inngå som del av det ordinære forvaltnings- og krisehåndteringssystemet. *NorSIS* foreslår at de angjeldende paragrafer endres slik at det kun er for de virksomheter som ikke er knyttet til et etablert responsmiljø at myndighetene kan gå inn og bestemme hvilket organ det skal varsles til.

7.5 Departementets vurderinger

7.5.1 Varslingskrav

Selv om enkelte lover og forskrifter har relativt like varslingskrav som NIS-direktivet, mener departementet det likevel er mest hensiktsmessig at det i den foreslåtte loven blir stilt likelydende krav om varsling av hendelser til myndighetene. Se forslag til lovens §§ 8 og 11. Det vil følge av loven § 5, at i den grad denne typen hendelser etter gjeldende regelverk allerede varsles til relevante myndigheter, vil direktivet ikke medføre endringer. I motsatt fall vil tilbyderen måtte følge direktivets varslingskrav. Departementet registrerer at direktivet benytter en noe ulik ordlyd i varslingskravene for de to kategoriene av tilbydere. Tilbydere av samfunnsviktige tjenester skal varsle om hendelser som «virker betydelig inn på kontinuiteten i de samfunnsviktige tjenestene de yter», mens tilbydere av digitale tjenester skal varsle om hendelser som «virker betydelig inn på leveringen av en tjeneste [...] som de tilbyr». Departementet anser at denne nyanseforskjellen ikke er til hinder for at det i loven kan etableres likelydende varslingskrav for tilbyderne. Departementet foreslår at varsling skal skje ved hendelser som «virker betydelig inn på tjenesteleveransen». Dersom det er behov for å fange opp nyanseforskjellen som direktivet har lagt opp til, kan dette reguleres i forskrift.

Det er flere grunner til at hendelser skal varsles til myndighetene. For det første av hensyn til den aktuelle tilbyderen. Dersom denne har behov for bistand fra myndighetene til å håndtere hendelsen, er det en forutsetning at det varsles til rette myndighet og at varselet inneholder nok informasjon til at det er mulig for den som blir varslet å bistå. For det andre vil sektormyndigheten få muligheten til å varsle videre til andre i samme sektor, til nasjonale myndigheter, og i enkelte tilfeller til andre land. For det tredje skal varslinger danne et nyttig kunnskapsgrunnlag for sikkerhetsmyndighetene.

Ved utformingen av bestemmelsene om varsling mener departementet å fange opp det samme som direktivets krav.

Det legges opp til at eksisterende myndighetsstruktur i størst mulig grad skal benyttes, og departementet anser det som mest hensiktsmessig at tilbydere innenfor en sektor varsler til ett punkt, og fortrinnsvis et punkt de kjenner fra før.

Utover den generelle føringen i direktivet om at det skal stilles noe mindre strenge krav til tilbydere av digitale tjenester, gis det ikke særlige føringer på hvor store forskjeller det er snakk om eller hva dette betyr i praksis utover det som er presisert i gjennomføringsforordningen.

Ved fastsettelse av krav om varsling, er tidspunktet det skal varsles sentralt. Etter direktivet skal tilbyderne varsle «uten unødig opphold», jf. artikkel 14 nr. 3 og 16 nr. 3. Departementet har inntatt tilsvarende ordlyd i lovforslaget §§ 8 og 11.

Innenfor rammen «uten unødig opphold», vil departementet presisere tidspunktet for varsling nærmere i forskrift. Etter departementets syn vil fristen for å varsle kunne bero på blant annet hvilken sektor tilbyderen tilhører.

Taushetsplikten skal ikke være til hinder for at tilbydere underlagt loven eller myndighet etter loven utleverer opplysninger til andre aktører eller offentlige organer når det er innenfor lovens formål. Departementet har derfor sett et behov for å presisere at varsling skal skje uten hinder av taushetsplikt, og har inntatt dette tillegget i lovforslaget §§ 8 og 11. Dette er for å ivareta operative hensyn ved hendelseshåndtering, og for å fjerne enhver tvil om hvorvidt en hendelse skal varsles. Det skal ikke deles mer enn det som er nødvendig for å oppnå formålet. Som antydet i punkt 5.6 vil det i forbindelse med hendelseshåndtering og varsling kunne inngå behandling av særlige kategorier av personopplysninger, herunder helseopplysninger, i forbindelse med håndtering i helsesektoren. Slike opplysninger kan være omfattet av regler om taushetsplikt for særlige yrkesutøvere, jf. tvisteloven § 22-5 og straffeprosessloven § 119. Opplysningene bør kunne innhentes uten hinder av taushetsplikt og departementet vil vurdere å klargjøre dette i forskrift, jf. forslag til § 18 bokstav a.

Direktivets angivelse av hva varselet minst skal inneholde, samt begrensningene i varslingsplikten for tilbydere av digitale tjenester, foreslås regulert i forskrift, jf. forslag til forskriftshjemmel i § 18 bokstav a.

7.5.2 Responsmiljø

Etter artikkel 9 i NIS-direktivet skal hver stat utpeke en eller flere nasjonale responsmiljøer som skal oppfylle kravene som følger av direktivet vedlegg I. Responsmiljøet skal blant annet overvåke hendelser på nasjonalt nivå, respondere på hendelser, bidra med analyser og situasjonsforståelse og delta i nettverket av responsmiljøer som er etablert av direktivet.

Direktivet stiller ikke krav om mer enn ett responsmiljø eller at alle hendelser skal rapporteres direkte til responsmiljøet.

I høringsnotatet foreslo departementet at Kongen kan utpeke ett eller flere responsmiljøer som skal kunne motta varsler etter loven. Videre at Kongen i forskrift kan gi nærmere bestemmelser om responsmiljøer og hendelseshåndtering.

Enkelte høringsinstanser støtter departementets vurderinger når det gjelder nasjonale responsmiljøer ved at det bør legges til rette for at de virksomheter som omfattes av loven varsler om hendelser i de samme kanalene som allerede er opprettet, blant andre *Norsk Helsenett* og *Helsedirektoratet*.

Enkelte høringsinstanser mener at kravene om responsmiljøer må klargjøres, blant andre *Statens Helsetilsyn* og *Advokatforeningen*. *Statens Helsetilsyn* skriver at det må klargjøres hvordan de som er underlagt flere regelverk skal varsle flere responsmiljøer og tilsynsmyndigheter, og hvordan ansvars- og myndighetsfordelingen er mellom de ulike respons- og tilsynsmyndigheter. *Advokatforeningen* mener at departementet må klargjøre hvilke responsmiljøer og tilsynsmyndigheter pliktsubjektene etter loven skal forholde seg til før ikrafttredelse av loven, eventuelt før ikrafttredelse av bestemmelser om varsling og tilsyn trer i kraft. Advokatforeningen mener også at departementet må klargjøre hvordan pliktsubjektene etter lovforslaget skal forholde seg til ulike responsmiljøer og tilsynsmyndigheter når pliktsubjektene også er underlagt annet tverrsektorielt og/eller sektorspesifikt regelverk.

Departementet foreslo i høringsnotatet på dette punktet regler utover minimumskravene i direktivet. Direktivet stiller ikke krav som nødvendiggjør lovregulering av hendelseshåndteringsmiljøer.

Departementet går ikke inn for å videreføre forslaget om en egen bestemmelse om responsmiljøer som varslingsmottakere. I bestemmelsen om varslingsplikt for tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester foreslås det at varselet sendes til «det organ Kongen utpeker». Med dette gis det forskriftshjemmel til å utpeke det organ som anses som mest hensiktsmessig til å motta varselet. Sammen med forskriftshjemmelen i forslag til § 18 bokstav a, legges det til rette for en fornuftig varslingsordning i forskrift. Dette inkluderer muligheten til å utpeke nasjonale responsmiljøer ved forskrift.

Departementet mener, i likhet med flere av høringsinstansene at varslingsplikten, herunder særlig hvem det skal varsles til, må være tydelig og enkelt. I utgangspunktet er det hensiktsmessig med likhet for alle tilbyderne. Departementet mener derfor at en nærmere utpeking av hvem det skal varsles til, organiseringen av varsling, varselmottak og videre-varsling, skal skje i forskrift gitt med hjemmel i lovens varslingsbestemmelser.

8 Tilsyn

8.1 Gjeldende rett

I mange sektorer er det etablert myndigheter som fører tilsyn med det gjeldende regelverket. Men som det fremgår av punkt 3.1, 6.1 og 7.1 er det samtidig for mange sektorer uklart om gjeldende regelverk stiller krav om digital sikkerhet. Dermed er det også uklart om tilsynsmyndighetene kan føre tilsyn med den digitale sikkerheten.

For noen sektorer er det klart at gjeldende rett ikke dekker direktivets krav om tilsyn. Enten fordi det er klart at det ikke er etablert relevant sektormyndighet som fører tilsyn, eller at gjeldende regler ikke stiller tilstrekkelige sikkerhetskrav.

Under følger en gjennomgang av et utvalg relevante tverrsektorielle regelverk med bestemmelser om tilsyn.

Sikkerhetsloven kapittel 3 regulerer tilsyn. Lovens hovedregel følger av § 3-1 hvor det står at sikkerhetsmyndigheten (i praksis Nasjonal sikkerhetsmyndighet) fører tilsyn med virksomheter som omfattes av loven. Et sektordepartement kan imidlertid i henhold til andre ledd bestemme at «myndigheter med sektoransvar som fører tilsyn med beskyttelse av informasjon, informasjonssystemer, objekter eller infrastruktur», i stedet skal føre slikt tilsyn. I praksis betyr dette at gjeldende sektormyndigheter kan føre tilsyn etter sikkerhetsloven, så fremt de har kompetanse til det.

Sikkerhetsmyndigheten skal i tillegg føre tilsyn med andre tilsynsmyndigheter, jf. § 3-1 tredje ledd. Et slikt tilsyn skal undersøke om sektormyndighetenes tilsyn etter sikkerhetsloven føres i tråd med sikkerhetslovens krav og de grunnleggende kriteriene for tilsyn som er fastsatt av sikkerhetsmyndigheten.

Samarbeid mellom sikkerhetsmyndigheten og andre myndigheter med tilsynsansvar reguleres av § 3-2. Første ledd bestemmer at det skal inngås en samarbeidsavtale og at gjennomføring av tilsyn så langt det er mulig skal samordnes med andre tilsynsmyndigheter. Etter andre ledd skal sikkerhetsmyndigheten utarbeide og utvikle grunnleggende kriterier for tilsyn og legge til rette for felles opplæring av tilsynspersonell. Når det er nødvendig kan sikkerhetsmyndigheten medvirke til forberedelse og gjennomføring av tilsyn som i utgangspunktet skal utføres av en sektormyndighet.

Etter § 3-4 kan tilsynsmyndigheten kreve tilgang til virksomhetens informasjon, informasjonssystemer, objekter og infrastruktur. Tilsynsmyndigheten har etter § 3-6 mulighet til å gi pålegg om gjennomføring av tiltak som er nødvendige for å ivareta lovens formål.

Tilsyn med etterlevelse av personopplysningsregelverket er relativt utførlig regulert i personvernforordningen kapittel VI. Tilsynets oppgaver er listet opp i artikkel 57. I Norge vil det fortsatt være Datatilsynet som er den sentrale myndighet som skal føre tilsyn med etterlevelse av regelverket. Datatilsynet skal både føre tilsyn, håndheve anvendelsen av reglene og behandle klager. Tilsynsmyndigheten skal også ha rådgivnings- og informasjonsoppgaver. Den skal i tillegg vedta standardkontraktsvilkår, godkjenne atferdsnormer og bindende virksomhetsregler og utarbeide kriterier for akkrediterings- og sertifiseringsoppgaver.

Etter artikkel 58 skal tilsynsmyndigheten ha undersøkelsesmyndighet, myndighet til å beslutte korrigerende tiltak og til å godkjenne visse typer behandlinger samt standardregler.

eForvaltningsforskriften har ikke regler om tilsyn.

8.2 Direktivet

8.2.1 Innledning

NIS-direktivet artikkel 8 og 9 bestemmer at statene skal utpeke eller etablere et nasjonalt kontaktpunkt, en eller flere kompetente myndigheter og ett eller flere hendelseshåndteringsmiljøer.

Den (eller de) kompetente myndigheten(e) skal i henhold til artikkel 8 for det første dekke hele direktivets virkeområde, jf. direktivet vedlegg II og III. Rollen som kompetent myndighet kan tildeles en eller flere eksisterende nasjonale myndigheter. Kompetent myndighet skal overvåke anvendelsen av direktivet, herunder kunne

føre tilsyn med tilbydernes etterlevelse av direktivet. Staten skal sørge for at kompetent myndighet har tilstrekkelige ressurser og virkemidler for gjennomføring av oppgavene som tillegges dem etter direktivet.

8.2.2 Tilbydere av samfunnsviktige tjenester

Artikkel 15 regulerer tilsyn med tilbydere av samfunnsviktige tjenester. Tilsynsmyndighetene skal ha hjemler til å innhente følgende fra tilbyderne av samfunnsviktige tjenester:

- Nødvendig informasjon for å kunne vurdere sikkerheten i deres nettverks- og informasjonssystemer, herunder dokumentert sikkerhetspolicy
- Dokumentasjon som viser effektiv gjennomføring av sikkerhetspolicyen, slik som resultater av sikkerhetsrevisjoner utført av kompetent inspektør og, i sistnevnte tilfelle, stille resultatene og den underliggende dokumentasjonen til rådighet for kompetent myndighet

Når det anmodes om slike opplysninger eller slik dokumentasjon, skal formålet med anmodningen angis og hvilke opplysninger som kreves skal presiseres. Kompetent myndighet skal i henhold til artikkel 15 nr. 4 samarbeide tett med personvernmyndighetene når hendelser som innebærer brudd på personopplysningsregelverket håndteres.

8.2.3 Tilbydere av digitale tjenester

Artikkel 17 regulerer tilsyn med tilbydere av digitale tjenester. Det følger av artikkel 17 nr. 1 at når det foreligger dokumentasjon på at en tilbyder av digitale tjenester ikke oppfyller direktivets krav, skal kompetent myndighet i ettertid ved behov gjennomføre tilsyn.

Tilsynsmyndigheten kan da kreve at tilbyderen

- gir nødvendige opplysninger for å kunne vurdere sikkerheten i nettverks- og informasjonssystemene deres, herunder en dokumentert sikkerhetspolicy
- utbedrer eventuelle avvik

I følge fortalepunkt 60 kan relevant informasjon for eksempel komme fra tilbyderen selv, en annen tilsynsmyndighet (også i andre land), eller fra en bruker av tjenesten. Tilsynsmyndighetene bør derfor ikke ha en forpliktelse til å kontrollere tilbydere av digitale tjenester.

Det følger av artikkel 17 nr. 3 at myndigheter i ulike stater skal samarbeide og bistå hverandre ved behov i de tilfeller en tilbyder har sitt hovedforetak eller representant i én stat og sine nettverks- og informasjonssystemer i en annen.

8.3 Forslaget i høringsnotatet

Departementet foreslo at Kongen utpeker en eller flere tilsynsmyndigheter som skal føre tilsyn med tilbydere av samfunnsviktige og digitale tjenester.

Forslaget innebar også at det skal fremgå av loven at det bare skal føres tilsyn med tilbydere av digitale tjenester etter at tilsynsmyndigheten har mottatt opplysninger om overtredelser av bestemmelser gitt i eller i medhold av lovforslaget og når tilsynsmyndigheten finner det nødvendig.

Departementet foreslo at tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester etter pålegg fra tilsynsmyndigheten skal gi de opplysninger den krever for å utføre sine oppgaver. Det ble også foreslått at tilsynet til enhver tid skal ha uhindret adgang til ethvert sted som omfattes av loven.

Av forslaget fremgår også at tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester plikter å medvirke til gjennomføring av tilsynet.

8.4 Høringsinstansenes syn

Enkelte høringsinstanser støtter prinsippet om å bruke eksisterende tilsynsmyndigheter for tilsyn med etterlevelse av NIS-direktivet, blant andre *Helsedirektoratet* og *Direktoratet for e-helse*. *Helsedirektoratet* mener at det imidlertid fordrer god og bred kunnskap om feltet hos tilsynsmyndigheten og at det lovfestes et mer aktivt tilsyn enn det som ble foreslått.

Enkelte høringsinstanser trekker frem at det må klargjøres hvilke tilsynsmyndigheter som skal føre tilsyn etter en lov som gjennomfører NIS-direktivet, blant andre *Advokatforeningen* og *Kartverket*.

Flere høringsinstanser trekker frem at tilsyn etter en lov som gjennomfører NIS-direktivet må sees i sammenheng med tilsyn etter andre sektorregelverk og tverrsektorielle regelverk, blant andre *Samferdselsdepartementet, Advokatforeningen, Teknisk-naturvitenskapelig forening, Direktoratet for IKT og fellestjenester i høyere utdanning og forskning, Statens Helsetilsyn, Direktoratet for e-helse, Finans Norge* og *Kartverket*. *Teknisk-naturvitenskapelig forening* skriver at de er særlig opptatt av at de ulike tilsynsorganenes roller og full-

makter avklares og at de opererer mer enhetlig i sine tilsyn med digital sikkerhet. Særlig må man vurdere om man har tilstrekkelig hjemmel til å føre tilsyn med underleverandører og å føre teknisk IKT-tilsyn.

Enkelte høringsinstanser trekker frem at tilsynsrollen til Nasjonal sikkerhetsmyndighet etter sikkerhetsloven må sees i sammenheng med tilsynsfunksjonen i en lov som gjennomfører NIS-direktivet, blant andre *Forsvarsdepartementet, Nasjonal sikkerhetsmyndighet* og *Direktoratet for samfunnssikkerhet og beredskap*. *Nasjonal sikkerhetsmyndighet* og *Direktoratet for samfunnssikkerhet og beredskap* mener at de bør utpekes som tilsynsmyndighet i henhold til loven. *Forsvarsdepartementet* trekker frem at en beslutning om å utpeke Nasjonal sikkerhetsmyndighet som tilsynsmyndighet ikke må påvirke direktoratets oppgaveløsning innenfor sikkerhetslovens virkeområde negativt.

8.5 Departementets vurderinger

Særlig fordi mange virksomheter per i dag ikke er underlagt tilsyn om digital sikkerhet, foreslår departementet i lovforslaget §§ 13-17 bestemmelser om tilsyn og sanksjoner som er ment å dels tilsvare direktivets krav. Det vil gis nærmere bestemmelser om tilsyn i forskrift, jf. forslag til § 18 bokstav b.

Departementet ser for seg en tilsynsmodell der myndigheter med sektoransvar fører tilsyn etter loven i den enkelte sektor. En forutsetning for en slik modell er at sektormyndighetene har tilstrekkelig kompetanse innenfor digital sikkerhet og gjennomføring av tilsyn. Der sektormyndighetene ikke allerede besitter nødvendig kompetanse innen digital sikkerhet, vil denne loven fungere som en pådriver for opparbeidelse av kompetanse på dette feltet. Der det per i dag eksisterer sektormyndigheter og de utpekes etter § 13 til å føre tilsyn etter denne loven, forutsettes det at deres hjemler justeres slik at de er i samsvar med loven når det gjelder tilsyn og sanksjonering. Videre bestemmelser om tilsyn fastsettes i forskrift.

Rollen som tilsynsmyndighet vil blant annet innebære å ha oversikt over og kontrollere den digitale sikkerhetstilstanden i egen sektor, og gi nødvendige pålegg om forbedringer, jf. § 15. I tillegg vil myndigheten til å fatte vedtak om tvangsmulkt og ilegge overtredelsesgebyr ligge til tilsynsmyndighetene, jf. §§ 16 og 17. Det er en klar forutsetning i lovforslaget at tilsynsmyndigheten gis tilgang til de opplysningene som er nødvendige for å gjennomføre tilsynet, jf. § 14. Departementet ser derfor behov for å presisere at plikten til å gi opplysninger ikke skal begrenses av taushetsplikt, og har inntatt et tillegg om dette i lovforslaget § 14 tredje ledd. I likhet som ved varsling vil det ved tilsyn kunne inngå behandling av opplysninger omfattet av regler om taushetsplikt for særlige yrkesutøvere, jf. tvisteloven § 22-5 og straffeprosessloven § 119. Slike opplysninger bør også kunne innhentes ved tilsyn uten hinder av taushetsplikt og departementet vil vurdere å klargjøre dette i forskrift, jf. forslaget til § 18 bokstav b.

I tråd med direktivet legges det til rette for forskjellige tilsynsregimer for henholdsvis tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester. Departementet ser det som mest hensiktsmessig at denne ulikheten reguleres i forskrift med hjemmel i forslag til § 18 bokstav b. I forskrift kan det for eksempel reguleres at det bare føres tilsyn med tilbydere av digitale tjenester etter at tilsynsmyndigheten har mottatt opplysninger om overtredelser av bestemmelser gitt i eller i medhold av denne loven og når tilsynsmyndigheten finner det nødvendig, slik som forutsatt i direktivet.

Departementet har for øvrig sett det som hensiktsmessig at det også gis hjemmel i lov til å gi forskrift om nasjonalt kontaktpunkt for sikkerhet i nettverks- og informasjonssystemer. En naturlig kandidat til rollen som nasjonalt kontaktpunkt er Nasjonal sikkerhetsmyndighet. Som kontaktpunkt vil Nasjonal sikkerhetsmyndighet for eksempel kunne ha en koordinerende rolle, og bistå tilsynsmyndighetene gjennom veiledning. Etter departementets syn vil en slik koordinerende rolle også være viktig for å sikre en sektorovergripende tilsynssamordning, og et tverrsektorielt perspektiv.

9 Pålegg, tvangsmulkt og overtredelsesgebyr

9.1 Gjeldende rett

I mange sektorer er det etablert sektorregelverk som har sanksjonsbestemmelser. Som det fremgår over er det samtidig for mange sektorer uklart om gjeldende regelverk stiller krav om digital sikkerhet. Dermed er det også uklart om sanksjonsbestemmelsene omfatter digital sikkerhet. Enkelte sektorregelverk har ikke sanksjonsbestemmelser. Under følger en gjennomgang av et utvalg relevante tverrsektorielle regelverk med sanksjonsbestemmelser.

Sikkerhetsloven kapittel 11 regulerer sanksjoner og straff. Tilsynsmyndigheten gis hjemmel for å fastsette tvangsmulkt og ilegge overtredelsesgebyr. Loven fastsetter ikke spesifikke beløp, men gir vurderingskriterier for fastsettelse av beløpenes størrelse. Det skal særlig legges vekt på «overtredelsens grovhet, overtredelsens varighet, utvist skyld og virksomhetens omsetning.» Forsettlige og uaktsomme overtredelser av nærmere bestemte forpliktelser er dessuten straffbelagt, jf. § 11-4.

Personopplysningsloven kapittel 7 regulerer sanksjoner og tvangsmulkt. Hovedregelen om overtredelsesgebyr er personvernforordningen artikkel 83, og det fremgår der i hvilke tilfeller dette kan ilegges. Det fremgår også av bestemmelsen at det kan gis gebyrer på opp til både 10 millioner euro og 20 millioner euro avhengig av overtredelsens karakter. Det følger av artikkel 83 at det skal foretas en konkret vurdering av hver enkelt sak ved vurderingen av om overtredelsesgebyr skal ilegges og det eventuelle gebyrets størrelse.

I tillegg følger det av personopplysningsloven at Datatilsynet også kan ilegge overtredelsesgebyr ved overtredelse av forordningen artikkel 10 om behandling av personopplysninger om straffedommer og lovovertredelser eller tilknyttede sikkerhetstiltak og artikkel 24 om internkontroll. Personopplysningsloven § 29 gir i tillegg Datatilsynet hjemmel til å fastsette tvangsmulkt for oppfyllelse av pålegg etter loven.

Forvaltningsloven har generelle bestemmelser om forvaltningsorganers mulighet til å ilegge administrative sanksjoner, herunder både overtredelsesgebyr og tvangsmulkt.

Det er ingen bestemmelser om sanksjonering av overtredelse av eForvaltningsforskriften.

9.2 Direktivet

Artikkel 21 bestemmer at EØS-statene skal fastsette regler om sanksjoner ved brudd på de forpliktelsene som følger av nasjonal lovgivning, som er vedtatt i henhold til direktivet. Sanksjonene skal være virkningsfulle, stå i et rimelig forhold til overtredelsen og virke avskrekkende. Bestemmelsen skiller ikke mellom tilbydere av henholdsvis samfunnsviktige og digitale tjenester.

Bestemmelsen kommenteres ikke i fortalen til direktivet, men i en kommunikasjon fra EU-kommisjonen *Making the most of NIS*. Det uttales i kommunikasjonen vedlegg I punkt 3.7 at EØS-statene i prinsippet står fritt til å bestemme maksimalbeløp ved overtredelser, men at det bør være rom for en konkret vurdering av hver enkelt sak som grunnlag for å ilegge et passende gebyr. Det bør legges vekt på blant annet forholdets alvorlighetsgrad og om det er snakk om gjentakende overtredelser.

9.3 Forslaget i høringsnotatet

Departementet foreslo i høringsnotatet at ved overtredelse av bestemmelser gitt i eller i medhold av loven kan tilsynsmyndigheten gi tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester pålegg om at forholdet skal bringes i orden. Videre at tilsynsmyndigheten kan sette en frist for oppfyllelse av pålegget.

Det ble foreslått at tilsynsmyndigheten gis hjemmel til å ilegge tvangsmulkt, der formålet er å sikre oppfyllelse av pålegg fastsatt i lovforslaget. Videre at vedtak om tvangsmulkt kan fastsettes samtidig med pålegget.

Det ble foreslått at departementet er klageinstans på vedtak om tvangsmulkt og at Kongen kan gi forskrift om tvangsmulkt, herunder om

mulktens størrelse og varighet og om gjennomføring av tvangsmulkten.

Departementet foreslo at tilsynsmyndigheten kan pålegge en virksomhet overtredelsesgebyr dersom virksomheten eller noen som handler på dennes vegne har overtrådt bestemmelser gitt i eller i medhold av loven eller har gitt uriktige eller ufullstendige opplysninger til tilsynsmyndigheten, også der ansvaret for overtredelsen ikke kan rettes mot noen enkeltperson. I høringsnotatet fremgår det at det bare kan ilegges overtredelsesgebyr for forsettlige eller uaktsomme overtredelser.

Ved fastsettelse av overtredelsesgebyrets størrelse ble det foreslått at det skal særlig legges vekt på overtredelsens grovhet, overtredelsens varighet, utvist skyld og virksomhetens omsetning.

Departementet foreslo at dersom den ansvarlige for overtredelsesgebyret er en virksomhet som inngår i et konsern, hefter foretakets morselskap og morselskapet i det konsern selskapet er en del av, subsidiært for beløpet.

Departementet foreslo at adgangen til å pålegge overtredelsesgebyr foreldes etter fem år, men at fristen avbrytes når tilsynsmyndigheten meddeler virksomheten at denne er mistenkt for overtredelse av loven eller vedtak fastsatt med hjemmel i loven.

Departementet foreslo at vedtak om overtredelsesgebyr kan påklages til departementet. Videre at Kongen kan gi forskrift om overtredelsesgebyr, herunder om vilkår for å ilegge overtredelsesgebyr, om størrelsen på overtredelsesgebyret, om rente og tilleggsgebyr dersom overtredelsesgebyret ikke blir betalt ved forfall og om frafall av ilagt overtredelsesgebyr.

9.4 Høringsinstansenes syn

Skatteetaten mener det fremstår som hensiktsmessig at tilsynsmyndigheten gis anledning til å sanksjonere manglende etterlevelse på en effektiv måte. Skatteetaten anser det imidlertid som en fordel at det stilles tydelige krav knyttet til sikkerhet og varsling.

Enkelte høringsinstanser trekker frem at anvendelse av sanksjonsbestemmelsene må klargjøres nærmere for å skape forutsigbarhet for de som underlegges loven, blant andre *Advokatforeningen* og *Kartverket*.

Helsedirektoratet og *Direktoratet for e-helse* mener det må presiseres nærmere hvilke sanksjonsbestemmelser som skal gjelde når bestemmelsene i både personvernforordningen og en lov som gjennomfører NIS-direktivet skal anvendes.

9.5 Departementets vurderinger

I lovforslaget § 15 foreslår departementet å gi tilsynsmyndigheten kompetanse til å pålegge den som overtrer lovens bestemmelser å bringe de ulovlige forholdene til opphør. Det fremgår at pålegg kan gis i tilknytning til brudd på loven og forskrifter gitt i medhold av loven. Påleggskompetansen er ikke avgrenset til grove eller gjentatte brudd på loven. Pålegg kan gis uavhengig av lovovertrederens subjektive skyld.

Departementet foreslår i lovforslaget § 16 at tilsynsmyndigheten gis hjemmel til å ilegge tvangsmulkt. Det fremgår av forslaget at formålet med tvangsmulkten er å sikre oppfyllelse av pålegg fastsatt i medhold av lovforslaget § 15.

Departementet mener at tvangsmulkt kan fastsettes i tilknytning til alle pålegg om tiltak. Tvangsmulkt kan således ilegges uavhengig av subjektiv skyld og uavhengig av omfanget av overtredelsen.

Departementet mener at tvangsmulktens størrelse fastsettes under hensyn til hvor viktig det er at pålegget blir gjennomført og hvilke kostnader det antas å medføre. Tvangsmulkt skal fungere som et pressmiddel, og utgangspunktet er at mulkten skal være så stor at den er effektiv uten å være urimelig.

Gjennomgangen av gjeldende rett viser at det er svært ulike regler om overtredelsesgebyr. Noen regelverk er dekkende for direktivets krav, noen er kanskje dekkende, mens andre igjen helt klart ikke er dekkende. Med dette som utgangspunkt foreslår departementet i lovforslaget § 17 bestemmelser om overtredelsesgebyr som gjelder alle tilbyderne som omfattes av loven.

Overtredelsesgebyr er ment å ivareta både individuelle og allmennpreventive hensyn. Mens bestemmelsene om pålegg og tvangsmulkt bare har som formål å bringe det ulovlige forholdet til opphør, vil et overtredelsesgebyr også ha som formål å hindre framtidige overtredelser. Etter departementets syn er det behov for å kunne reagere med overtredelsesgebyr både ved brudd på plikten til å sikre nettverks- og informasjonssystemer, ved brudd på plikten til å varsle om hendelser og der det er gitt uriktige eller ufullstendige opplysninger til tilsynsmyndigheten.

Ved høringen ble det foreslått at bestemmelsen om overtredelsesgebyr ikke nærmere skulle angi hvilke bestemmelser etter loven som vil utløse et overtredelsesgebyr ved overtredelse. Av hensyn til forutberegnelighet foreslår departementet at det i § 17 angis hvilke bestemmelser som kan utløse overtredelsesgebyr ved overtred-

else. Departementet foreslår at overtredelsesgebyr etter lovforslaget § 17 kan ilegges ved overtredelse av bestemmelsene om krav til sikkerhet (§§ 7 og 10), krav til varsling (§§ 8 og 11) og der det er gitt uriktige eller ufullstendige opplysninger til tilsynsmyndigheten (§ 14). Overtredelsesgebyr retter seg først og fremst mot den enkelte tilbyderen som er pliktsubjekt etter loven. Etter forslaget kan imidlertid overtredelsesgebyr ilegges fysiske personer som opptrer på vegne av en tilbyder dersom det er nødvendig i det enkelte tilfellet.

Departementet har vurdert, blant annet i lys av den tilsynelatende store effekten av at det i medhold av personvernforordningen kan gis relativt store bøter, om det også i dette lovforslaget bør kunne reageres med høye overtredelsesgebyrer ved overtredelse. Det er ulike løsninger i forskjellige EØS-stater. Departementet foreslår at bestemmelsen om overtredelsesgebyr i lovforslaget ikke angir hvilken størrelse på gebyret som er aktuelt. Det kommer an på hva slags overtredelse det er snakk om, om det har skjedd over tid og om det er tale om gjentakende og gjenstridige handlinger. Det vil måtte bero på en konkret helhetsvurdering i hver enkelt sak hva som er et passende gebyr der også den aktuelle tilbyderens omsetning kan vektlegges. Det vil dessuten kunne variere over tid hva som er passende beløpsmessige rammer. Blant annet kan dette påvirkes av rettsutviklingen i EØS. Departementet foreslår derfor at de beløpsmessige rammene fastsettes i forskrift, men vil i forskrift angi en øvre ramme for overtredelsesgebyrets størrelse slik som forutsatt i forvaltningsloven § 44 andre ledd.

Helsedirektoratet og *Direktoratet for e-helse* mener at det må presiseres nærmere hvilke sanksjonsbestemmelser som skal gjelde når bestemmelsene i både personvernforordningen og en lov som gjennomfører NIS-direktivet kan anvendes. Departementet viser i den sammenheng til forvaltningsloven § 47 om samordning av sanksjonssaker. I bestemmelsens andre ledd fremgår det at:

> «Dersom et forvaltningsorgan har grunn til å anta at det også for et annet organ kan være aktuelt å ilegge administrativ sanksjon mot samme forhold, må forvaltningsorganet sørge for en samordning av behandlingen av spørsmålet om å ilegge sanksjoner.»

Forvaltningslovens regler gjelder «når ikke annet er bestemt i lov eller i medhold av lov» jf. forvaltningsloven § 1 første punktum. Departementet foreslår ikke at forvaltningslovens regler fravikes i ny lov om digital sikkerhet. Forvaltningslovens bestemmelser om administrative sanksjoner, vil derfor gjelde for forvaltningsorganers virksomhet etter denne loven, jf. forvaltningsloven § 1. Tilsvarende gjelder forvaltningsloven § 51 ved vedtak om tvangsmulkt. Disse reglene vil supplere reglene om overtredelsesgebyr og tvangsmulkt etter denne loven.

Enkelte høringsinstanser trekker frem at anvendelse av sanksjonsbestemmelsene må klargjøres nærmere for å skape forutsigbarhet for de som underlegges loven. *Advokatforeningen* viser blant annet til at det vil føre til svært stor uforutsigbarhet å vedta en lov med slike sanksjoner, som også kan anvendes på fysiske personer, uten nærmere detaljer om hvilke krav som vil stilles til risikovurderingene som pålegges pliktsubjektene og hvilke tiltak som anses som tilstrekkelig ut fra ulike risikoer.

Til dette viser departementet til at adgangen til å ilegge overtredelsesgebyr vil gjelde for overtredelser av §§ 7 og 10 om krav til sikkerhet, §§ 8 og 11 om krav om varsling og § 14 om opplysningsplikt. Overtredelse av bestemmelsene om krav til varsling og til å gjennomføre en risikovurdering vil etter departementets syn være tilstrekkelig enkelt å fastslå. Kravet om å iverksette hensiktsmessige og proporsjonale tekniske og organisatoriske sikkerhetstiltak og krav om tiltak for å forebygge, avdekke og redusere konsekvensene av hendelser kan det være vanskeligere å vurdere om det foreligger en overtredelse, og derfor være mindre forutberegnelig for tilbyderne. Departementet vil spesifisere kravene til sikkerhet som stilles til tilbydere av samfunnsviktige tjenester nærmere i forskrift, og for tilbydere av digitale tjenester presiseres kravene til sikkerhet i gjennomføringsforordningen som departementet vil gjennomføre i forskrift. Se nærmere om dette i punkt 6.5.

Etter departementets syn vil lovens krav, sammenholdt med bestemmelser i forskrift som presiserer kravene, gi en tilstrekkelig klar beskrivelse. Når det gjelder fastsettelse av klageinstans, ser departementet behov for å åpne for en viss fleksibilitet og vil derfor ikke i loven fastslå at departementet er fast klageinstans slik det var foreslått i høringen. Nærmere regler om klage vil da måtte fastsettes i forskrift.

10 Samtykke til godkjenning av EØS-komiteens beslutninger

10.1 Innledning

EØS-komiteen fattet to beslutninger 3. februar 2023 om innlemmelse i EØS-avtalen av NIS-direktivet, gjennomføringsforordningen til NIS-direktivet og cybersikkerhetsforordningen. Beslutningene ble fattet med forbehold om Stortingets samtykke, da gjennomføringen i norsk rett nødvendiggjør lovendring, jf. Grunnloven § 26 annet ledd. Stortinget inviteres gjennom denne proposisjonen til å samtykke til godkjenning av EØS-komiteens beslutning.

Fyldigere omtale av innholdet i rettsaktene står i punkt 2.3, 2.4 og 2.5.

10.2 EØS-komiteens beslutning nr. 21/2023 om innlemmelse i EØS-avtalen av NIS-direktivet og gjennomføringsforordningen

EØS-komiteens beslutning nr. 21/2023 inneholder en innledning og fem artikler. I fortalen vises det til EØS-avtalen og spesielt artikkel 98. Beslutningen gjør tilføyelser til EØS-avtalens vedlegg XI og protokoll 37.

Artikkel 1 lister opp tilleggene til vedlegg XI til EØS-avtalen. Det legges til et nytt punkt 5cpa som viser til Europaparlamentets- og Rådets direktiv (EU) 2016/1148 om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i hele Unionen. I punktet presiseres det, i tråd med EØS-avtalen artikkel 101 om tilknytning til komiteer, at EFTA-statene skal delta fullt ut i samarbeidsgruppen og skal ha de samme rettighetene og forpliktelsene som EU-medlemsstatene, bortsett fra retten til å stemme.

Videre legges det til et nytt punkt 5cpaa som viser til EU-kommisjonens gjennomføringsforordning (EU) 2018/151 om fastsettelse av regler for anvendelse av europaparlaments- og rådsdirektiv (EU) 2016/1148 med hensyn til ytterligere spesifisering av de elementene som tilbydere av digitale tjenester skal ta hensyn til for å håndtere risikoene knyttet til sikkerheten i nettverks- og informasjonssystemer, og av parameterne for å avgjøre om en hendelse har en betydelig innvirkning.

Artikkel 2 slår fast at et nytt punkt 47 skal tilføyes til EØS-avtalens protokoll 37 der komiteene er oppført. Punktet gjelder samarbeidsgruppen for NIS-direktivet.

Artikkel 3 slår fast at teksten i direktiv (EU) 2016/1148 og gjennomføringsforordning (EU) 2018/151 på islandsk og norsk, som skal publiseres i EØS-tillegget til Den europeiske unions tidende, skal være autentisk/offisiell.

Artikkel 4 slår fast at beslutningen trer i kraft 4. februar 2023, under forutsetning av at EØS-komiteen har mottatt alle meddelelser etter avtalens artikkel 103 nr. 1.

Artikkel 5 slår fast at beslutningen skal kunngjøres i EØS-avdelingen av og EØS-tillegget til Den europeiske unions tidende.

10.3 EØS-komiteens beslutning nr. 22/2023 om innlemmelse i EØS-avtalen av cybersikkerhetsforordningen

EØS-komiteens beslutning nr. 22/2023 inneholder en innledning og 5 artikler. I fortalen vises det til EØS-avtalen og spesielt artikkel 98. Beslutningen gjør tilføyelser til EØS-avtalens vedlegg XI og protokoll 37.

Artikkel 1 viser til EØS-avtalens vedlegg XI og at teksten i nr. 5cp skal lyde: Europaparlaments- og rådsforordning (EU) 2019/881 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).

Artikkel 1 lister videre opp de bestemmelsene i forordningen som gjelder med tilpasninger:

a) Med mindre annet er fastsatt under, og uten at det berører bestemmelsene i avtalens protokoll 1, skal betegnelsen 'medlemsstat(er)' og andre betegnelser i forordningen som viser til deres myndigheter, i tillegg til den betydning

de har i forordningen, også omfatte EFTA-statene og deres myndigheter.

b) Med hensyn til EFTA-statene skal Byrået, slik og når det er hensiktsmessig, bistå EFTAs overvåkingsorgan eller eventuelt Den faste komité i utførelsen av deres respektive oppgaver.
c) Med hensyn til EFTA-statene skal henvisninger til unionsretten forstås som henvisninger til EØS-avtalen
d) I artikkel 14 skal nytt nummer lyde: '5. EFTA-statene skal delta fullt ut i styret og skal der ha de samme rettighetene og pliktene som EUs medlemsstater, unntatt stemmerett.'
e) I artikkel 28 skal nytt nummer lyde: '4. Ved anvendelse av denne forordningen skal forordning (EF) nr. 1049/2001 få anvendelse på alle Byråets dokumenter som også angår EFTA-statene.'
f) I artikkel 30 skal nytt nummer lyde: '3. EFTA-statene skal delta i bidraget fra Unionen nevnt i nr. 1 bokstav a. For dette formålet skal framgangsmåtene fastsatt i EØS-avtalens artikkel 82 nr. 1 bokstav a og protokoll 32 få tilsvarende anvendelse.'
g) I artikkel 34 skal nytt ledd lyde: 'Som unntak fra artikkel 12 nr. 2 bokstav a og artikkel 82 nr. 3 bokstav a i Tilsettingsvilkår for andre tjenestemenn i Den europeiske union kan statsborgere i EFTA-stater som nyter fulle borgerrettigheter, tilsettes på kontrakt av Byråets daglige leder.'
h) I artikkel 35 skal nytt ledd lyde: 'EFTA-statene skal tilstå Byrået og dets ansatte privilegier og immunitet tilsvarende de som er omhandlet i protokollen om Den europeiske unions privilegier og immunitet.'
i) I artikkel 40 skal nytt nummer lyde: '3. Som unntak fra artikkel 12 nr. 2 bokstav e, artikkel 82 nr. 3 bokstav e og artikkel 85 nr. 3 i Tilsettingsvilkår for andre tjenestemenn i Den europeiske union skal språkene nevnt i EØS-avtalens artikkel 129 nr. 1 anses av Byrået, med hensyn til sine ansatte, som et av Unionens språk nevnt i artikkel 55 nr. 1 i traktaten om Den europeiske union.'
j) I artikkel 62 skal nytt nummer lyde: EFTA-statene skal delta fullt ut, uten stemmerett, i ECCG

Artikkel 2 slår fast at et nytt punkt 48 skal tilføyes til EØS-avtalens protokoll 37 der komiteene er oppført. Punktet gjelder «Den europeiske cybersikkerhetssertifiseringsgruppen» etter forordningen.

Artikkel 3 slår fast at teksten i forordningen på islandsk og norsk, som skal publiseres i EØS-tillegget til Den europeiske unions tidende, skal være autentisk/ offisiell.

Artikkel 4 slår fast at beslutningen trer i kraft 4. februar 2023, under forutsetning av at EØS-komiteen har mottatt alle meddelelser etter avtalens artikkel 103 nr. 1, eller på den dagen EØS-komiteens beslutning nr. 21/2023 av 3. februar 2023 trer i kraft, alt etter hva som inntreffer sist.

Artikkel 5 slår fast at beslutningen skal kunngjøres i EØS-avdelingen av og EØS-tillegget til Den europeiske unions tidende.

Til slutt følger det med en felleserklæring fra avtalepartene som erklærer følgende:

«Partene erkjenner at innlemmingen av denne rettsakten ikke berører den direkte anvendelsen av protokoll 7 om Den europeiske unions privilegier og immunitet på statsborgere i EFTA-stater på territoriet til den enkelte medlemsstat i Den europeiske union i henhold til artikkel 11 i nevnte protokoll.»

10.4 Konklusjon

Rettsaktene er en del av EUs cybersikkerhetsstrategi som har som formål å sikre et globalt og åpent internett med sterkt vern mot risiko for at grunnleggende rettigheter og friheter i Europa kan bli truet. Et styrket samarbeid i EUs regi vil være av stor betydning for å løse fremtidige utfordringer innen digital sikkerhet. Det er viktig at Norge sikres en plass i dette samarbeidet, da nåværende og fremtidige utfordringer ikke kan løses av en stat alene.

Nettverks- og informasjonssystemer er forbundet med hverandre og store forstyrrelser i ett land kan få konsekvenser for andre land. Nettverks- og informasjonssystemers robusthet og stabilitet, samt kontinuiteten i de sentrale tjenestene er avgjørende for et velfungerende indre marked, og særlig for det digitale indre markeds videreutvikling.

Både NIS-direktivet og cybersikkerhetsforordningen har som hovedformål å forbedre det indre markeds funksjon.

NIS-direktivet har direkte innvirkning på berørte tilbyderes rammevilkår og indirekte for alle andre virksomheter ved at sikkerheten i sentral infrastruktur blir bedret.

Gjeldene forordning om ENISA (som erstattes av cybersikkerhetsforordningen) er en del av EØS-avtalen og i dag gjennomført i ekomregelverket. Erfaringen fra arbeidet i ENISA er at

byrået bidrar med viktige innsikter og bidrag innen digital sikkerhet som det ut fra et norsk standpunkt er ønskelig å delta i og være med på å forme.

Sertifisering av IKT-produkter, IKT-tjenester og IKT-prosesser vil etter forordningen inntil videre være frivillig. Innen en viss tid skal EU-kommisjonen ha gjort en første vurdering av hvorvidt enkelte sertifiseringsordninger skal gjøres obligatoriske. Det vil i første omgang være snakk om sektorer som er omfattet av NIS-direktivet. Flere norske virksomheter vil dermed kunne bli bundet av krav til sertifisering av IKT-produkter, IKT-tjenester eller IKT-prosesser. Ettersom leverandører av slike tjenester ofte er globale og/eller europeiske, er felles-europeiske løsninger riktig.

Forslag til lov om digital sikkerhet med tilhørende forskrifter vil gjennomføre NIS-direktivet. Gjennomføringsforordningen og cybersikkerhetsforordningen vil tas inn i norsk rett i sin helhet ved inkorporering i forskrift med hjemmel i forslag til ny lov om digital sikkerhet.

11 Økonomiske og administrative konsekvenser

11.1 Lov om digital sikkerhet, NIS-direktivet og gjennomføringsforordningen

Virksomhetene som blir omfattet av loven anses å være så viktige for å opprettholde et velfungerende samfunn at dersom en slik virksomhet stanser eller vesentlig reduserer sine normale leveranser, har det konsekvenser for andre deler av samfunnet.

De økonomiske og administrative kostnadene knyttet til lovforslaget er vanskelig å tallfeste. Loven legger opp til at det i forskrift både vil bli utarbeidet nærmere kriterier for identifisering av tilbydere av samfunnsviktige tjenester og også spesifisering av sikkerhets- og varslingskrav. Forslag til forskrift vil selvsagt bli gjenstand for egen offentlig høring hvor det trolig vil komme noe mer konkret om eventuelle kostnader knyttet til blant annet sikkerhets- og varslingskrav.

Tiltakende digitalisering av samfunnet anses som viktig for videre økonomisk vekst, i både Norge og EØS. NIS-direktivet skal bidra til å fremme økonomisk vekst i EUs indre marked. Videre er hovedformålet med EØS-avtalen, som danner grunnlaget for gjennomføring av direktivet for Norges del, nettopp å stimulere til økonomisk vekst i hele EØS.

Digital sikkerhet er en avgjørende forutsetning for at digitaliseringen skal lykkes, og det er fastslått i en rekke dokumenter at det er behov for styrking av den digitale sikkerheten i Norge, blant annet i NOU 2015: 13 *Digital sårbarhet – sikkert samfunn*, Meld. St. 38 (2016–2017) *IKT-sikkerhet – et felles ansvar*, NOU 2018: 14 *IKT-sikkerhet i alle ledd*, Nasjonal strategi for digital sikkerhet og senest i Meld. St. 9 (2022–2023) *Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet – Så åpent som mulig, så sikkert som nødvendig*. Gjennomføring av NIS-direktivet er etter departementets syn et viktig bidrag for å redusere digitale sårbarheter både i samfunnet og i den enkelte virksomhet.

Enkelte høringsinstanser har problematisert lovens uklare virkeområde og som en følge av dette gitt uttrykk for at det er vanskelig å se de økonomiske konsekvensene av lovforslaget. *Oslo Kommune* og *KS – kommunesektorens organisasjon* trekker frem at loven potensielt kan medføre kostnader det ikke er mulig å finne dekning for innen gjeldende budsjettrammer. Det omfatter både engangskostnader ved å tilpasse seg et nytt regelverk, og de løpende kostnadene ved vedlikehold, oppgradering og drift.

Andre høringsinstanser påpeker at de fleste virksomheter i dag må forventes å ha et fokus på digital sikkerhet, slik at selv om de ikke er underlagt krav til digital sikkerhet i sektorregelverk, vil det for de fleste medføre marginale kostnader å bli omfattet av loven.

Statens Helsetilsyn har i sitt høringssvar påpekt at nye oppgaver til tilsynsmyndighetene utfordrer sektorens samlede ressurser og medfører press på omprioritering fra tilsyn med helsetjenestens kjerneoppgaver til tilsyn med digital sikkerhet. Dette vil kunne kreve digital sikkerhetskompetanse og ressurser som en i dag ikke har. Samtidig påpeker de at dersom loven gir handlingsrom for å finne egnede løsninger for å ivareta tilsynsansvaret, og at tilsynet lar seg kombinere med sektormyndighetenes øvrige tilsyn på det digitale området, vil de økonomiske konsekvensene av forslaget være mer begrenset.

Departementet bemerker at bedre digital sikkerhet har flere positive sider. For det første er det her snakk om å styrke sikkerheten knyttet til viktig infrastruktur i landet. For det andre har god grunnsikring kriminalitetsforebyggende effekt, både for den enkelte virksomhet og for samfunnet. Norge som nasjon kan dessuten bli et mindre attraktivt sted å drive kriminell aktivitet. For det tredje vil god digital sikkerhet kunne være et konkurransefortrinn. I en direkte konkurranse kan virksomheten for eksempel tilby sikker drift eller god sikring av informasjon en tar vare på vegne av andre. Også globalt vil god digital sikkerhet i EØS som region kunne være en driver for å tiltrekke seg investorer.

Som nevnt i punkt 7.5 er noe av formålet med varslingskravene at myndighetene skal få bedre kunnskapsgrunnlag for å kunne forbedre arbeidet med sikkerhet. Dette vil etter hvert komme virk-

somheter, myndigheter og hele samfunnet til gode.

Det er viktig for norsk næringsliv og verdiskaping at tilsvarende regler som følger av direktivet også gjelder for Norge. For eksempel omfatter direktivet skytjenester. Fra norsk ståsted er det viktig at alle skytjenester innenfor EØS-området tilfredsstiller krav fra EU om både informasjonssikkerhet og personvern. Dette gjelder både for de norske virksomhetene som benytter skytjenester innenfor EØS-området, men det er også viktig dersom vi ønsker etablering av store, internasjonale datasentre i Norge. Det at Norge er omfattet av NIS-direktivet (og personvernforordningen) vil være med på å redusere usikkerhet knyttet til Norge som vertsnasjon.

I tillegg til konkurransehensyn er det også av rent sikkerhetsmessige hensyn et viktig moment at Norge faktisk gjennomfører kravene i NIS-direktivet. Angripere vil naturlig gå etter de svakeste leddene først. Når begrunnelsen for kravene delvis ligger i at alt henger sammen med alt, er det særlig viktig at alle følger opp kravene. Heri ligger også grunnen til at EU-kommisjonen kommer til å følge opp statenes etterlevelse av direktivet (for Norges del EFTAs overvåkingsorgan), og til at det må innføres krav ved lov og at myndighetene skal føre tilsyn og får sanksjonshjemler.

NIS-direktivet utgjør en viktig brikke i det digitale indre markedet i EØS. Hvis befolkningen ikke har tillit til de digitale tjenestene, så blir de ikke brukt. Et for lavt sikkerhetsnivå på de digitale tjenestene vil sette en effektiv stopper for den videre digitaliseringen.

For berørte virksomheter vil etterlevelse av kravene om sikkerhet og varsling kunne innebære økte kostnader. For berørte myndigheter vil forslaget innebære økte kostnader til gjennomføring av tilsyn og håndtering av varsler. Departementet forutsetter, i likhet med flere høringsinstanser, at mange virksomheter prioriterer arbeidet med digital sikkerhet og allerede har implementert et adekvat sikkerhetsnivå gitt dagens digitale trusselbilde. Departementet forutsetter, og erfarer gjennom dialog med andre departement og sentrale myndigheter, at også regulering av krav om digital sikkerhet i sektorregelverkene har tiltatt siden høringen. Også i EØS har fokuset på regulering av digital sikkerhet, både tverrsektorielt, men også i enkeltsektorer, økt betydelig de siste årene. Departementet mener derfor de krav loven stiller utgjør et minimum av det som må forventes av virksomheter og myndigheter hva gjelder digital sikkerhet i 2023 og utviklingen i den sikkerhetspolitiske situasjonen.

Når det gjelder inndekning av eventuelle økte kostnader mener departementet at kravene som følger av forslaget ikke er mer tyngende enn det som naturlig følger med samfunnsutviklingen. Digitaliseringen må ha som mål å bidra til effektivisering og økonomisk vekst. For å kunne ta del i dette er det nødvendig å investere i digital sikkerhet. Dette gjelder for både private og offentlige virksomheter. Private virksomheter som har en samfunnsmessig viktig rolle, har et selvstendig ansvar for å kunne levere sine tjenester. Forslaget krever ikke et spesielt høyt sikkerhetsnivå, men en grunnsikring. Gjennomføring av tiltak for å styrke den digitale sikkerheten vil ikke bare gagne samfunnet, men også den enkelte virksomhet.

Som nevnt over vil de fleste virksomhetene som omfattes av direktivet også være omfattet av personopplysningsloven. Departementet mener det ikke vil medføre særlige ekstra kostnader å sikre informasjonssystemer i henhold til forslaget, dersom systemet allerede er sikret i henhold til personopplysningsloven.

Offentlige myndigheter må som utgangspunkt kunne finne inndekning for merarbeidet som følger av forslaget innenfor gjeldende budsjettrammer. Skulle det ikke være tilstrekkelig vil det være opp til den enkelte sektor å finne tilstrekkelige midler, enten gjennom omprioritering eller tilførsel av friske midler, som må behandles som en del av den ordinære budsjettprosessen.

Som tidligere omtalt vil både virkeområdet, sikkerhetskrav, krav til varsling mv. nærmere konkretiseres i forskrift. Nærmere bestemmelser om tilsyn og hvordan tilsyn skal gjennomføres vil også være gjenstand for konkretisering i underliggende regelverk. Det samme gjelder hvilke myndigheter som skal føre tilsyn.

Det er forholdet mellom dagens krav på den ene siden, og NIS-direktivets krav på den andre siden som vil utgjøre direktivets og gjennomføringsforordningens økonomiske og administrative konsekvenser. En total oversikt over konsekvensene fordrer en vurdering av sikkerhetsnivået i hver virksomhet som underlegges regelverket. Ut fra forordningens presisering av overordnede krav innebærer dette i stor grad å utarbeide retningslinjer og planverk knyttet til de krav NIS-direktivet oppstiller. Forordningens presiseringer medfører således ikke økonomiske eller administrative konsekvenser som ikke allerede er forutsatt at vil påløpe som følge av innføringen av NIS-direktivet i norsk rett.

11.2 Cybersikkerhetsforordningen

Norge er allerede assosiert medlem av ENISA (uten stemmerett). Medlemskapet ivaretas av både Justis- og beredskapsdepartementet og Kommunal- og distriktsdepartementet- Kostnadene fordeles likt mellom departementene og dekkes innenfor det enkelte departementets budsjett. Etter at forordningen trådte i kraft i EU i 2019, har kontingenten for medlemmer av ENISA økt. For 2021 og 2022 utgjorde den samlede kontingenten for norsk deltakelse i ENISA henholdsvis omlag 5,6 og 5,3 mill. kroner. De økte kostnadene er kostnader som allerede effektueres, uavhengig av om forordningen implementeres i EØS-avtalen eller ikke. Organisering og styring av ENISA er lite forandret etter at forordningen trådte i kraft i EU i 2019, og departementet kan ikke se at innlemmelse av forordningen i EØS-avtalen vil medføre store endringer for Norges rolle i ENISA.

Hva gjelder cybersikkerhetssertifiseringsordningen vil forordningen innebære å avklare blant annet hvordan og hvem som utpekes til sertifiseringsmyndighet. Både Nasjonal sikkerhetsmyndighet og Nasjonal kommunikasjonsmyndighet har relevant kompetanse, så dette spørsmålet må vurderes nærmere. Per i dag har Nasjonal kommunikasjonsmyndighet en rolle når det gjelder funksjonalitet i ekomnett og ikke minst for utstyr som bruker radio. Nasjonal sikkerhetsmyndighet har på sin side allerede gjennomført sertifisering av operative sikkerhetstjenester og tjenestemiljøer. Det forutsettes at den nasjonale cybersikkerhetssertifiseringsmyndigheten deltar i den europeiske cybersikkerhetssertifiseringsgruppen, som vil ha en viktig rolle ved utarbeidelse av nye sertifiseringsordninger under rammeverket. Nasjonal sikkerhetsmyndighet deltar i den europeiske cybersikkerhetssertifiseringsgruppen i dag, men har som nevnt ikke blitt formelt utpekt til dette. Det er likevel naturlig å se for seg at Nasjonal sikkerhetsmyndighet innehar en overordnet myndighet etter forordningen.

Norge har i dag en sertifiseringsordning for sikkerhet i IT-produkter etter ISO/IEC 15408 (Common Criteria), jf. Norges tilslutning til *Common Criteria Recognition Arrangement (CCRA)* og *SOG-IS Mutual Recognition Arrangement (SOG-IS MRA)*. Nasjonal sikkerhetsmyndighet har rollen som sertifiseringsmyndighet for IT-sikkerhet (SERTIT) etter disse avtalene.

Ved innføringen av forordningen er det planlagt to sertifiseringsordninger – EUCC for produktsertifisering etter ISO/IEC 15408 og EUCS for sertifisering av skytjenester. Ved innføringen av EUCC vil sertifisering etter SOG-IS MRA opphøre, og sertifisering etter CCRA på sikt tilpasses denne ordningen.

Kravet om etablering av nasjonale organ i henhold til rammeverket for cybersikkerhetssertifisering vil innebære økonomiske konsekvenser. Nasjonal sikkerhetsmyndighet har avsatt to stillinger til arbeid med sertifiseringsordningen for IT-sikkerhet. Disse stillingene har både ansvar for rollen som sertifiseringsmyndighet og sertifiseringsorgan. Ved inkorporeringen av forordningen vil ikke lenger den nasjonale sertifiseringsmyndigheten inneha rollen som sertifiseringsorgan. Samtidig vil den nasjonale sertifiseringsmyndigheten blant annet ha ansvar for mottak av klager, egenerklæringer, utpeking av sertifiseringsorgan samt føre tilsyn med disse. Grunnet stor fleksibilitet i hvordan de nasjonale sertifiseringsmyndighetene kan utføre sine oppgaver og manglende erfaringsgrunnlag, er det vanskelig å vurdere ressursbehovet med særlig nøyaktighet. Det anslås at det vil måtte avsettes ressurser til å følge opp den enkelte sertifiseringsordning, herunder utpeking av sertifiseringsorgan, mottak av eventuelle klager og egenerklæringer og tilsyn med sertifiseringsorganene. Videre vil det være behov for ressurser til oppfølging av den europeiske cybersikkerhetssertifiseringsgruppen, kontakt med Norsk Akkreditering og andre relevante myndighetsaktører. Basert på tilgjengelig kunnskap om den fremtidige ordningen, anslås det ressursmessige merbehovet derfor til minimum to årsverk (ett årsverk per ordning).

Forordningen utvider virkeområdet for sertifisering fra kun produkter til også å dekke tjenesteleveranser og prosesser. Riktig bruk av gode sertifiseringsordninger kan bidra til å øke den samlede evnen til å motstå ulike former for cyberoperasjoner og dermed gi samfunnsøkonomisk gevinst. Videre vil også anskaffelsesprosesser kunne forenkles gjennom å stille krav til bruk av sertifiserte produkter, tjenester eller prosesser. Norske virksomheter som har ønsket å få produkter sertifisert etter ISO/EIC 15408, har til nå nytt godt av at selve sertifiseringen har blitt utført vederlagsfritt av sertifiseringsmyndighet for IT-sikkerhet. Etter forordningen vil sertifisering i utgangspunktet gjøres av kommersielle sertifiseringsorganer, og dette medfører en betydelig merkostnad for disse virksomhetene. Samtidig er det viktig å understreke at bruken av sertifiserte produkter, tjenester og prosesser i utgangspunktet er frivillig, derfor vil et marked for sertifiserte produkter, tjenester eller prosesser være styrt av tilbud og etter-

spørsel. Dette må også sees i sammenheng med NIS2-direktivet, hvor det i noen grad legges opp til krav om sertifisering.

Flere av de ledende sertifiseringsorganene i verden har i dag tilhold i Norge, sertifisering etter forordningen kan derfor åpne for et nytt virksomhetsområde for disse, noe også norske teknologibedrifter kan nyte godt av. Effekten av denne synergien vil være størst dersom det legges opp til en internasjonal anerkjennelse av sertifikater utstedt under sertifiseringsordningen, slik det er lagt opp til i implementeringen av sertifiseringsordningen EUCC.

12 Merknader til bestemmelsene i lovforslaget

Til § 1

Bestemmelsen angir lovens formål og reflekterer at loven både omfatter NIS-direktivets formål og skal legge til rette for å gjennomføre cybersikkerhetsforordningen. Lovens formål er i første punktum å bidra til å sikre grunnleggende krav til digital sikkerhet i virksomheter med særlig betydning for samfunnet ved å forebygge, avdekke og motvirke uønskede hendelser i nettverks- og informasjonssystemer som brukes for å levere samfunnsviktige tjenester.

Virksomheter med særlig betydning for samfunnet peker tilbake på det saklige virkeområdet, herunder tilbydere av samfunnsviktige tjenester innenfor de gitte sektorene og tilbydere av digitale tjenester.

Lovens formål bygger på NIS-direktivets formål, som er å styrke den digitale sikkerheten i EØS. I direktivets artikkel 1 nr. 1 fremgår det at direktivet fastsetter «tiltak med sikte på å oppnå et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i Unionen for å forbedre virkemåten til det indre marked». Fortalen gir en nærmere beskrivelse av direktivets bakgrunn, se særlig fortalepunkt 1 til 3.

Lovens formål knytter seg til opprettholdelse av tjenesteleveranser fra samfunnsviktige tjenester. Dette gjenspeiles i sikkerhets- og varslingskravene som stilles til tilbydere av samfunnsviktige tjenester i §§ 7 og 8 og til tilbydere av digitale tjenester i §§ 10 og 11.

Tilbyder av samfunnsviktige tjenester defineres i § 6 og tilbyder av digitale tjenester defineres i § 9.

Lovens formål i andre punktum er å legge til rette for sikkerhet i IKT-produkter, IKT-tjenester og IKT-prosesser. Ordlyden er ment å omfatte cybersikkerhetsforordningens bestemmelser om sikkerhetssertifisering.

Departementet viser ellers til de generelle merknadene i punkt 3.5.

Til § 2

Lovens § 2 angir lovens saklige virkeområde. Virkeområdet til loven tilsvarer NIS-direktivet artikkel 1 nr. 2 bokstav d.

I *første ledd bokstav a* fremgår det at loven gjelder for tilbydere av samfunnsviktige tjenester innenfor angitte samfunnssektorer. Disse sektorene er energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur. Tilbydere av samfunnsviktige tjenester er definert i lovforslaget § 6. I direktivet er tilbydere av samfunnsviktige tjenester definert i artikkel 4 nr. 4, jf. artikkel 5 nr. 2. Sektorene er listet opp i direktivets vedlegg II.

For tilbydere av samfunnsviktige tjenester vil terskelverdier eller andre kriterier som fastsettes i forskrift for identifisering, avgrense virkeområdet til tilbyderne som opererer innenfor en av sektorene angitt i § 2 første ledd bokstav a, og som i tillegg anses som en «tilbyder av en samfunnsviktig tjeneste» i lovens og direktivets forstand, jf. § 6 og artikkel 4 nr. 4, jf. artikkel 5 nr. 2. Dette innebærer at det kun er visse virksomheter innenfor de nevnte sektorene som vil være underlagt loven.

I *første ledd bokstav b* er det angitt at loven gjelder for tilbydere av digitale tjenester, med en henvisning til definisjonen av tilbyder av digitale tjenester i § 9. Tilbyder av digitale tjenester er definert i lovforslaget § 9 første ledd som virksomheter som tilbyr tjenester som definert i ehandelsloven § 1 andre ledd bokstav a og b i form av nettbaserte markedsplasser, nettbaserte søkemotorer eller skytjenester. I direktivet er tilbydere av digitale tjenester definert i artikkel 4 nr. 6, jf. artikkel 4 nr. 5. Direktivet viser til direktiv (EU) 2015/1535 artikkel 1 nr. 1 bokstav b og til direktivets vedlegg III. Direktiv (EU) 2015/1535 artikkel 1 nr. 1 bokstav b er gjennomført i norsk rett ved nevnte ehandelsloven § 1 andre ledd bokstav a og b, og det vises derfor til denne bestemmelsen for nærmere avgrensning av tilbydere av digitale tjenester. For tilbydere av digitale tjenester er virkeområdet konkret og uttømmende angitt, og

det vil derfor ikke oppstilles terskelverdier for identifisering i forskrift, slik som for tilbydere av samfunnsviktige tjenester.

I *andre ledd* følger et unntak fra lovens virkeområde for virksomheter som er omfattet av lov 15. juni 2018 nr. 44 om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked (lov om elektroniske tillitstjenester). Virksomheter som er omfattet av lov om elektroniske tillitstjenester vil ikke være omfattet av denne loven eller NIS-direktivet.

I *tredje ledd* oppstilles det en hjemmel for Kongen til å gi forskrift med nærmere bestemmelser om og unntak fra lovens virkeområde. Dette innebærer også at Kongen i forskrift kan gi myndighet til å utpeke enkeltvirksomheter som ikke tilfredsstiller terskelverdiene eller andre kriterier som defineres i forskrift, men som det av andre årsaker er viktig å underlegge regelverket.

Departementet viser ellers til de generelle merknadene i punkt 3.5.

Til § 3

I lovens § 3 reguleres lovens geografiske virkeområde. Bestemmelsen gjennomfører NIS-direktivet artikkel 18 nr. 1.

I *første ledd bokstav a* fremgår det at loven gjelder for tilbydere av samfunnsviktige tjenester som er etablert i Norge.

I *første ledd bokstav b* fremgår det at loven gjelder for tilbydere av digitale tjenester som har sitt hovedkontor i Norge, eller som har eller skal ha en representant etter § 12. Alternativet med representant gjelder for tilbydere som tilbyr digitale tjenester i Norge, men som ikke har hovedkontor i Norge.

I *tredje ledd* fremgår det at Kongen i forskrift kan bestemme at loven helt eller delvis skal gjelde for Svalbard, Jan Mayen og i bilandene.

Departementet viser ellers til de generelle merknadene i punkt 4.5.

Til § 4

I § 4 angis definisjoner.

I *første ledd nr. 1 bokstav a til c* defineres «nettverks- og informasjonssystemer». Definisjonen sammenfaller med tilsvarende definisjon i NIS-direktivet artikkel 4 nr. 1 bokstav a til c.

I *første ledd nr. 2* defineres «sikkerheten i nettverks- og informasjonssystemer». Definisjonen sammenfaller med tilsvarende definisjon i NIS-direktivet artikkel 4 nr. 2.

I *første ledd nr. 3* defineres «hendelse» som enhver hendelse med negativ virkning på sikkerheten i nettverks- og informasjonssystemer. Definisjonen sammenfaller med tilsvarende definisjon i direktivet artikkel 4 nr. 7 med unntak av at «reell negativ virkning» er erstattet med «negativ virkning» da «reell» anses overflødig.

Departementet viser ellers til de generelle merknadene i punkt 3.5.

Til § 5

I § 5 reguleres forholdet til andre lover. Dersom det stilles krav om sikkerhet og varsling i annen lov eller forskrift som minst tilsvarer kravene etter denne loven, skal annen lov eller forskrift benyttes. For virksomhetene som er underlagt slikt regelverk, vil det å bli omfattet av denne lovens virkeområde ikke medføre endringer. Bestemmelsen har en todelt funksjon. Dels gjennomfører den direktivets bestemmelse i artikkel 1 nr. 7 om at EØS-basert regelverk går foran direktivet dersom sikkerhets- og varslingskravene tilsvarer kravene i direktivet. Bestemmelsen vil imidlertid også gjelde for nasjonale sektorspesifikke regler om sikkerhet og varsling som i utgangspunktet ikke er EØS-baserte, men som likevel oppfyller NIS-direktivets krav. I slike tilfeller vil NIS-direktivets krav til sikkerhet og varsling bli ivaretatt av de sektorspesifikke reglene i stedet for de generelle kravene i lov om digital sikkerhet.

Anvendelse av § 5 vil ikke direkte unnta de aktuelle virksomhetene fra lovens virkeområde. Identifiseringsprosessen skal fortsatt gjennomføres, og virksomhetene vil underlegges direktivet og loven. Konsekvensene av å bli underlagt vil imidlertid i praksis være begrenset, gitt at regelverket man er underlagt har tilsvarende eller strengere sikkerhetskrav.

Departementet viser ellers til de generelle merknadene i punkt 3.5.1.

Til § 6

Paragraf 6 omhandler tilbydere av samfunnsviktige tjenester. Bestemmelsen gjennomfører NIS-direktivets artikkel 5 nr. 2 og artikkel 6.

I *første ledd bokstav a til c* defineres «tilbyder av en samfunnsviktig tjeneste» ved at tre kumulative kriterier må være oppfylt. Det første kriteriet, som er tilsvarende direktivet artikkel 5 nr. 2 bokstav a, er at virksomheten må tilby en tjeneste som er viktig for opprettholdelsen av kritiske samfunnsmessige eller økonomiske aktiviteter. I hen-

hold til fortalepunkt 20 er det tilstrekkelig å fastslå at virksomheten leverer en slik tjeneste som er opplistet i direktivet vedlegg II. Det er kun den delen av virksomheten som leverer den aktuelle tjenesten som omfattes. For eksempel vil trafikkstyringen på en stor flyplass omfattes, mens butikkområdet ikke omfattes.

Det andre kriteriet, som er tilsvarende direktivet artikkel 5 nr. 2 bokstav b, er at tjenesteleveransen må være avhengig av nettverks- og informasjonssystemer. Begrepet nettverks- og informasjonssystemer defineres i artikkel 4 nr. 1, og gjentas i lovforslaget § 4 første ledd nr. 1.

Det tredje kriteriet, som er tilsvarende direktivet artikkel 5 nr. 2 bokstav c, er at en hendelse i virksomhetens nettverks- og informasjonssystemer ville hatt betydelig forstyrrende virkning på leveransen av den samfunnsviktige tjenesten. Vurderingstemaet er tjenesteleveranse i en samfunnssammenheng, og ikke virksomhetens tjenesteleveranse isolert sett. Det er altså spørsmål om i hvilken grad det går utover samfunnets tilgang på en viss tjeneste, at den aktuelle virksomheten ikke leverer sitt bidrag til totalen som normalt.

I *andre ledd bokstav a til g* oppstilles det en ikke uttømmende liste med momenter som det skal tas utgangspunkt i ved vurderingen av om en hendelse kan få betydelig forstyrrende innvirkning på tjenesteleveransen.

Det bemerkes at opplistingen av momenter det skal tas utgangspunkt i ved vurderingen av om en hendelse kan få betydelig forstyrrende innvirkning på tjenesteleveransen slik at virksomheten defineres som en tilbyder av en samfunnsviktig tjeneste, avviker noe fra de momenter det skal tas utgangspunkt i ved vurdering av hvorvidt en hendelse skal varsles, jf. lovforslaget §§ 8 og 11.

Departementet viser ellers til de generelle merknadene i punkt 3.5.2.

Til § 7

I § 7 oppstilles krav til sikkerhet for tilbydere av samfunnsviktige tjenester. Bestemmelsen gjennomfører NIS-direktivet artikkel 14 nr. 1 og 2.

Etter *første ledd* skal en tilbyder av en samfunnsviktig tjeneste gjennomføre en risikovurdering av nettverks- og informasjonssystemer som benyttes for å levere tjenesten.

Etter *andre ledd* skal tilbyderen iverksette hensiktsmessige og proporsjonale tekniske og organisatoriske tiltak som samlet skal sørge for et sikkerhetsnivå som er tilpasset risikoen. Ved vurderingen skal det blant annet ses hen til den teknologiske utviklingen.

Etter *tredje ledd* skal tilbyderen iverksette proporsjonale tiltak for å forebygge, avdekke og redusere konsekvensene av hendelser med det formål å opprettholde tjenesteleveransen.

Bestemmelsene om sikkerhet er funksjonsbaserte og sikter til forsvarlig sikkerhet. Det nærmere innholdet i sikkerhetskravene vil bli spesifisert i forskrift, jf. § 18 bokstav a. Sikkerhetskravene kan være tilfredsstilt ved å følge anerkjente standarder, generelle eller sektorspesifikke retningslinjer eller prinsipper for digital sikkerhet. Virksomhetene må vurdere om de gjennom allerede gjeldende tiltak tilfredsstiller lovens krav til sikkerhet, eller om det må iverksettes andre tiltak for å oppfyllet kravene basert på gjennomført risikovurdering.

Ved vurderingen av hva som er et forsvarlig sikkerhetsnivå skal det ses hen til den teknologiske utviklingen, både med tanke på nye trusler og sårbarheter og oppdatering av tiltak eller iverksetting av nye tiltak.

Gjennomføringsforordningen presiserer nærmere hva som ligger i sikkerhetskrav og hva som skal til for at en hendelse er betydelig og faller inn under varslingsplikten for tilbydere av digitale tjenester. Denne vil gjelde som forskrift i Norge og kan tjene som veiledning også for tilbydere av samfunnsviktige tjenester.

Departementet viser ellers til de generelle merknadene i punkt 6.5.

Til § 8

I § 8 oppstilles krav om varsling for tilbydere av samfunnsviktige tjenester. Sammen med utfyllende forskrifter gjennomfører bestemmelsen NIS-direktivet artikkel 14 nr. 3 og 4.

I *første punktum* fremgår det at tilbyderen uten unødig opphold skal varsle det organ Kongen utpeker om hendelser som virker betydelig inn på tjenesteleveransen.

Hva som utgjør en «hendelse» i lovens forstand er definert i § 4 nr. 3. Varslingsplikten etter loven gjelder ikke for enhver hendelse som har betydelig innvirkning på tjenesteleveransen, men avgrenses til ethvert tilfelle av negativ virkning på sikkerheten i nettverks- og informasjonssystemer. Videre er varslingsplikten knyttet til tjenesteleveransen. Varslingsplikten gjelder altså for ethvert tilfelle av negativ virkning på sikkerheten i nettverks- og informasjonssystemer som har betydelig innvirkning på opprettholdelsen av tjenesteleveransen.

I *andre punktum* angis momenter som skal vektlegges ved vurderingen av om innvirkningen er betydelig. Det skal legges vekt på antall brukere som påvirkes, hendelsens varighet og størrelsen på det geografiske området som berøres av hendelsen.

Gjennomføringsforordningen presiserer nærmere hva som ligger i sikkerhetskrav og hva som skal til for at en hendelse er betydelig og faller inn under varslingsplikten for tilbydere av digitale tjenester. Denne vil gjelde som forskrift i Norge og kan tjene som veiledning også for tilbydere av samfunnsviktige tjenester.

Kravene til det nærmere innholdet i varselet vil bli angitt i forskrift, jf. § 18 bokstav a.

Departementet viser ellers til de generelle merknadene i punkt 7.5.

Til § 9

Paragraf 9 omhandler tilbydere av digitale tjenester. Bestemmelsen gjennomfører NIS-direktivet artikkel 4 nr. 5 og 6.

I *første til fjerde ledd* defineres tilbydere av digitale tjenester, nettbaserte markedsplasser, nettbaserte søkemotorer og skytjenester. Definisjonene bygger på tilsvarende definisjoner i NIS-direktivet artikkel 1 nr. 5, 17, 18 og 19.

En nettbasert markedsplass er en digital tjeneste som gjør det mulig for forbrukere og næringsdrivende å inngå nettbaserte salgs- eller tjenesteavtaler med næringsdrivende, enten på nettstedet til den nettbaserte markedsplassen eller på nettstedet til en næringsdrivende som bruker datatjenester som leveres av den nettbaserte markedsplassen. Applikasjonsbutikker trekkes i fortalepunkt 15 frem som en type butikk som faller inn i denne kategorien.

En nettbasert søkemotor er en digital tjeneste som gjør det mulig for brukere å foreta søk på i prinsippet alle nettsteder på et bestemt språk, på grunnlag av en forespørsel om et hvilket som helst emne i form av et nøkkelord, en setning eller andre inndata, og som viser lenker hvor det er mulig å finne informasjon om det forespurte innholdet.

En skytjeneste er en digital tjeneste som gir tilgang til en skalerbar og fleksibel samling av delbare databehandlingsressurser.

I *femte ledd* gis det hjemmel til at Kongen kan gi forskrift med nærmere bestemmelser om hvilke virksomheter som skal regnes som tilbydere av digitale tjenester.

Departementet viser ellers til de generelle merknadene i punkt 3.5.3.

Til § 10

Krav om sikkerhet for tilbydere av digitale tjenester reguleres i § 10. Bestemmelsen gjennomfører NIS-direktivet artikkel 16 nr. 1 og 2. Kravene er likelydende sikkerhetskravene som stilles til tilbydere av samfunnsviktige tjenester.

I *første ledd* oppstilles et krav om at tilbyderen av en digital tjeneste skal gjennomføre en risikovurdering av nettverks- og informasjonssystemer som benyttes for å levere tjenesten.

Etter *andre ledd* skal tilbyderen iverksette hensiktsmessige og proporsjonale tekniske og organisatoriske sikkerhetstiltak som samlet skal sørge for et sikkerhetsnivå som er tilpasset risikoen. Videre fremgår det at ved vurderingen av hva som er et forsvarlig sikkerhetsnivå skal tilbyderen se hen til den teknologiske utviklingen og ta hensyn til momentene listet opp i bokstav a til e. Momentene er sikkerheten i systemer og utstyr/anlegg (bokstav a), hendelseshåndtering (bokstav b), styring av opprettholdelse av tjenesteleveransen (bokstav c), overvåking, revisjon og testing (bokstav d) og anerkjente internasjonale standarder (bokstav e).

Det følger av direktivets fortalepunkt 49 at det skal stilles mindre strenge sikkerhetskrav til tilbydere av digitale tjenester enn til tilbydere av samfunnsviktige tjenester. Videre fremgår det at tilbydere av digitale tjenester, på grunn av sin tverrnasjonale karakter, bør være underlagt en mer harmonisert tilnærming i EU. Nærmere presisering av sikkerhetskravene for tilbydere av digitale tjenester er presisert i gjennomføringsforordningen som skal gjelde som forskrift til loven.

Det følger av *tredje ledd* at tilbyderen skal iverksette tiltak for å forebygge, avdekke og redusere konsekvensene av hendelser, for å opprettholde tjenesteleveransen.

Departementet viser ellers til de generelle merknadene i punkt 6.5.

Til § 11

Krav om varsling for tilbydere av digitale tjenester reguleres i § 11. Sammen med forskrifter gjennomfører bestemmelsen NIS-direktivet artikkel 16 nr. 3 og 4.

I *første punktum* fremgår det at tilbyderen av en digital tjeneste skal varsle det organ Kongen utpeker om hendelser som har betydelig innvirkning på tjenesteleveransen.

Hva som utgjør en «hendelse» i lovens forstand er definert i § 4 nr. 3. Varslingsplikten etter

loven gjelder ikke for enhver hendelse som har betydelig innvirkning på opprettholdelsen av tjenesteleveransen, men avgrenses til ethvert tilfelle av reell negativ virkning på sikkerheten i nettverks- og informasjonssystemer. Varslingsplikten gjelder altså for ethvert tilfelle av reell negativ virkning på sikkerheten i nettverks- og informasjonssystemer som har betydelig innvirkning på opprettholdelsen av tjenesteleveransen.

Etter *andre punktum* skal det ved vurderingen av om innvirkningen er betydelig legges vekt på antall brukere som påvirkes av hendelsen, dens varighet, størrelsen på det geografiske området som berøres, omfanget av funksjonalitetssvikten i tjenesten og omfanget av innvirkningen på økonomisk og samfunnsmessig aktivitet.

De nærmere kravene til innholdet i varselet vil fremgå av forskrift, jf. § 18 bokstav a. Gjennomføringsforordningen, som skal gjelde som forskrift, presiserer også hva som skal til for at en hendelse har betydelig virkning.

Departementet viser ellers til de generelle merknadene i punkt 7.5.

Til § 12

I § 12 fastsettes det en plikt for tilbydere av digitale tjenester som ikke har sitt hovedkontor i Norge eller en EØS-stat, og som tilbyr digitale tjenester i Norge, om å utpeke en representant i Norge, med mindre tilbyderen har utpekt en representant i en annen EØS-stat hvor tjenestene tilbys. Bestemmelsen kommer kun på spissen i tilfeller hvor en tilbyder tilbyr digitale tjenester i Norge uten å utpeke en representant i en EØS-stat. Bestemmelsen gjennomfører NIS-direktivet artikkel 18 nr. 2.

Departementet viser ellers til de generelle merknadene i punkt 4.5.

Til § 13

I § 13 fremgår det at Kongen utpeker en eller flere tilsynsmyndigheter som skal føre tilsyn med tilbydere av samfunnsviktige og digitale tjenester. Den nærmere gjennomføringen av tilsynet, og eventuelle begrensninger av tilsynet med tilbydere av digitale tjenester, vil bli regulert i forskrift, jf. § 18 bokstav b. Sammen med forskrifter gjennomfører bestemmelsen NIS-direktivet artikkel 8 nr. 1 og 2.

Departementet viser ellers til de generelle merknadene i punkt 8.5.

Til § 14

I § 14 stilles det krav til tilbyderne om opplysningsplikt og å gi tilgang til lokaler og utstyr i forbindelse med tilsyn. Bestemmelsen gjennomfører NIS-direktivet artikkel 15 nr. 1 og 2 og artikkel 17 nr. 1 og 2.

Det følger av *første ledd* at tilbyderne skal gi tilsynsmyndigheten de opplysninger den krever for å utføre sine oppgaver og gi tilgang til virksomhetens lokaler og utstyr og yte nødvendig bistand ved tilsynsmyndighetens undersøkelser.

Etter *andre ledd* gjelder opplysningsplikten og medvirkningsplikten etter første og andre ledd uten hinder av lovbestemt taushetsplikt.

Departementet viser ellers til de generelle merknadene i punkt 9.5.

Til § 15

I § 15 gis tilsynsmyndigheten hjemmel til å gi pålegg om retting. Bestemmelsen gjennomfører NIS-direktivet artikkel 15 nr. 3.

Det følger av *første punktum* at ved overtredelse av bestemmelser gitt i eller i medhold av loven kan tilsynsmyndigheten gi tilbydere pålegg om at forholdet skal bringes i orden.

I *andre punktum* fremgår det at tilsynsmyndigheten skal sette en frist for oppfyllelse av pålegget.

Departementet viser ellers til de generelle merknadene i punkt 9.5.

Til § 16

Tvangsmulkt reguleres i § 16.

I *første ledd første punktum* fremgår det at for å sikre at pålegg etter § 15 blir oppfylt, kan tilsynsmyndigheten ilegge en tvangsmulkt.

I *første ledd andre punktum* fremgår det at tvangsmulkten kan fastsettes som løpende mulkt eller som et engangsbeløp.

I *andre ledd* fremgår det at tilsynsmyndigheten i særlige tilfeller kan frafalle påløpt tvangsmulkt.

Departementet viser ellers til de generelle merknadene i punkt 9.5.

Til § 17

Lovens § 17 regulerer overtredelsesgebyr. Bestemmelsen gjennomfører NIS-direktivet artikkel 21.

I *første ledd* fremgår det at tilsynsmyndigheten kan ilegge en tilbyder overtredelsesgebyr dersom tilbyderen eller noen som handler på dennes vegne har overtrådt §§ 7, 8, 10, 11 eller 14.

Det fremgår i *andre ledd* at dersom den ansvarlige for overtredelsesgebyret er et foretak som inngår i et konsern, hefter foretakets morselskap og morselskapet i det konsern selskapet er en del av for beløpet.

I *tredje ledd første punktum* er det fastsatt at adgangen til å pålegge overtredelsesgebyr foreldes etter fem år.

I *tredje ledd andre punktum* fremgår det at fristen avbrytes når tilsynsmyndigheten gir forhåndsvarsel om eller fatter vedtak om overtredelsesgebyr.

Departementet viser ellers til de generelle merknadene i punkt 9.5.

Til § 18

Lovens § 18 er en fellesbestemmelse om hva som kan reguleres videre i forskrift. Loven for øvrig har også noen steder egne forskriftshjemler knyttet til enkelte bestemmelser.

I *bokstav a* er det oppstilt en hjemmel til at Kongen kan gi forskrift med nærmere bestemmelser om krav til sikkerhet og varsling i samsvar med §§ 7, 8, 10 og 11.

I *bokstav b* er det oppstilt en hjemmel til at Kongen kan gi forskrift med nærmere bestemmelser om tilsyn med tilbydere underlagt loven, med henvisning til lovens § 13 om tilsyn. Slike nærmere bestemmelser kan for eksempel være regler som innskrenker tilsynsadgangen overfor tilbydere av digitale tjenester slik som forutsatt i direktivet artikkel 17 nr. 1.

I *bokstav c* er det oppstilt en hjemmel til at Kongen kan gi forskrift om opplysningsplikt og tilgang til lokaler og utstyr, jf. § 14.

I *bokstav d* er det oppstilt en hjemmel til at Kongen kan gi forskrift om ileggelse og utmåling av tvangsmulkt og overtredelsesgebyr jf. §§ 16 og 17. Slik forskrift kan regulere tvangsmulktens størrelse og varighet, om gjennomføring av tvangsmulkten og om klage. For overtredelsesgebyr kan forskriften regulere blant annet vilkår for å ilegge overtredelsesgebyr, om størrelsen på overtredelsesgebyret, om rente og tilleggsgebyr dersom overtredelsesgebyret ikke blir betalt ved forfall og om frafall av ilagt overtredelsesgebyr.

I *bokstav e* er det oppstilt en hjemmel til at Kongen kan gi forskrift om at den som forsettlig eller uaktsomt overtrer forskrift gitt i medhold av bokstav a, kan ilegges overtredelsesgebyr. Bestemmelsen sørger for at det kan fastsettes at også overtredelse av forskriftens krav om sikkerhet og varsling kan utløse overtredelsesgebyr.

I *bokstav f* er det oppstilt en hjemmel til at Kongen kan gi forskrift om gjennomføring av forpliktelser som følger av EØS-avtalen og andre internasjonale avtaler som understøtter lovens regler og formål. Det vil i første omgang være aktuelt å inkorporere gjennomføringsforordning 2018/151 om spesifisering av NIS-direktivet artikkel 16 nr. 1 og nr. 4. Bestemmelsen legger også til rette for gjennomføring av senere rettsakter som understøtter lovens formål.

I *bokstav g* er det oppstilt en hjemmel til at Kongen kan gi forskrift om behandling av personopplysninger. Rettsgrunnlag for behandling av personopplysninger er lovens angivelse av oppgaver samt personvernforordningens bestemmelser om rettsgrunnlag. De nærmere bestemmelsene om formål, behandlingsansvar, hvilke personopplysninger som kan behandles, videre-behandling, utlevering og sletting vil fremgå av forskrift.

I *bokstav h* er det oppstilt en hjemmel til at Kongen kan gi forskrift om nasjonalt kontaktpunkt for sikkerhet i nettverks- og informasjonssystemer. Bestemmelsen tydeliggjør at et slikt kontaktpunkt også skal utpekes, i tillegg til tilsynsmyndighet og myndighet som skal motta varsler. Sammen med forskrifter gjennomfører bestemmelsen NIS-direktivet artikkel 8 nr. 3.

Til § 19

Lovens § 19 er ment å tydeliggjøre hjemmelen til å gjennomføre cybersikkerhetsforordningen ved forskrift. Bestemmelsen benyttes til å fastsette supplerende og utfyllende regler til cybersikkerhetsforordningen der det er aktuelt. Den vil også kunne benyttes til å gjennomføre delegerte rettsakter fra EU-kommisjonen innen sikkerhetssertifisering.

I bestemmelsen er det oppstilt en hjemmel til at Kongen kan gi forskrift om sikkerhetssertifisering av IKT-produkter, IKT-tjenester og IKT-prosesser for å gjennomføre forpliktelser etter EØS-avtalen. Med sikkerhetssertifisering menes cybersikkerhetssertifisering slik det er angitt i cybersikkerhetsforordningen.

I bokstav a til c er det en ikke uttømmende liste over hva det kan gis forskrift om.

Etter *bokstav a* kan det gis forskrift om utpeking av sertifiseringsmyndighet. Med «sertifiseringsorganer» menes i denne sammenheng samsvarsorganer som utfører sertifisering i tråd med cybersikkerhetssertifiseringsordninger, jf. artikkel 60 i (EU) 2019/881 cybersikkerhetsforordningen.

Etter *bokstav b* kan det gis forskrift om tilsyn med sertifiseringsorganer som tilbyr sikkerhetssertifisering av IKT-produkter, IKT-tjenester og IKT-prosesser. Det anses nødvendig med en egen hjemmel for tilsyn med disse tilbyderne som ikke nødvendigvis vil være de samme som tilbydere av samfunnsviktige tjenester eller digitale tjenester. I forskriften kan det gis bestemmelser om hvem som kan føre tilsyn, hvilken medvirkningsplikt som gjelder for partene det føres tilsyn med, og om stedlig adgang.

Etter *bokstav c* kan det gis forskrift om pålegg om retting, tvangsmulkt og overtredelsesgebyr ved overtredelse av krav til sikkerhetssertifisering. Også her er det nødvendig med egne hjemler da de aktuelle pliktsubjektene ikke nødvendigvis vil være de samme som tilbydere av samfunnsviktige tjenester og digitale tjenester. Det vil i første omgang være aktuelt med bestemmelser om pålegg og sanksjoner knyttet til overtredelse av cybersikkerhetssertifiseringsordninger vedtatt gjennom gjennomføringsrettsakter, jf. artikkel 49 i (EU) 2019/881 cybersikkerhetsforordningen. Sanksjonene skal være effektive, stå i rimelig forhold til bruddet og ha avskrekkende effekt.

Departementet viser ellers til omtalen i punkt 2.5.

Til § 20

Bestemmelsen åpner for at deler av loven kan tre i kraft til forskjellige tidspunkt.

Justis- og beredskapsdepartementet

t i l r å r :

At Deres Majestet godkjenner og skriver under et framlagt forslag til proposisjon til Stortinget om lov om digital sikkerhet (digitalsikkerhetsloven) og samtykke til godkjenning av EØS-komiteens beslutninger nr. 21/2023 og 22/2023 om innlemmelse i EØS-avtalen av direktiv (EU) 2016/1148 og forordningene (EU) 2018/151 og (EU) 2019/881.

Vi HARALD, Norges Konge,

s t a d f e s t e r :

Stortinget blir bedt om å gjøre vedtak til lov om digital sikkerhet (digitalsikkerhetsloven) og vedtak om samtykke til godkjenning av EØS-komiteens beslutninger nr. 21/2023 og 22/2023 om innlemmelse i EØS-avtalen av direktiv (EU) 2016/1148 og forordningene (EU) 2018/151 og (EU) 2019/881 i samsvar med et vedlagt forslag.

A
Forslag
til lov om digital sikkerhet (digitalsikkerhetsloven)

Kapittel 1. Innledende bestemmelser

§ 1 *Formål*

Loven skal bidra til å sikre grunnleggende krav til digital sikkerhet i virksomheter med særlig betydning for samfunnet ved å forebygge, avdekke og motvirke uønskede hendelser i nettverks- og informasjonssystemer som brukes for å levere samfunnsviktige tjenester og digitale tjenester. Loven skal også legge til rette for sikkerhet i IKT-produkter, IKT-tjenester og IKT-prosesser.

§ 2 *Saklig virkeområde*

Loven gjelder for

a. tilbydere av samfunnsviktige tjenester etter § 6 i sektorene energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur
b. tilbydere av digitale tjenester etter § 9.

Loven gjelder ikke for virksomheter som er omfattet av lov om elektroniske tillitstjenester.

Kongen kan gi forskrift med nærmere bestemmelser om og unntak fra lovens virkeområde.

§ 3 *Geografisk virkeområde*

Loven gjelder for

a. tilbydere av samfunnsviktige tjenester som er etablert i Norge
b. tilbydere av digitale tjenester som har sitt hovedkontor i Norge, eller som har eller skal ha en representant i Norge etter § 12.

Kongen kan gi forskrift om lovens anvendelse for Svalbard, Jan Mayen og bilandene og fastsette særlige regler som er nødvendige av hensyn til de stedlige forholdene.

§ 4 *Definisjoner*

I denne loven menes med

1. nettverks- og informasjonssystemer:
   a. elektronisk kommunikasjonsnett som nevnt i ekomloven § 1-5 nr. 2
   b. en enhet eller en gruppe av sammenkoblede eller beslektede enheter som behandler digitale data automatisk ved hjelp av et program
   c. digitale data som lagres, behandles, innhentes eller overføres ved hjelp av elementer som nevnt i bokstav a eller b for at dataene skal kunne driftes, vernes, beskyttes eller vedlikeholdes.
2. sikkerheten i nettverks- og informasjonssystemer: evnen nettverk eller informasjonssystemer har til å tåle, på et gitt tillitsnivå, enhver handling som går ut over tilgjengeligheten, autentisiteten, integriteten eller tilliten til lagrede, overførte eller behandlede data eller tilknyttede tjenester som tilbys eller er tilgjengelige via slike nettverks- og informasjonssystemer
3. hendelse: enhver hendelse med negativ virkning på sikkerheten i nettverks- og informasjonssystemer.

§ 5 *Forholdet til andre lover som stiller krav om sikkerhet og varsling*

Kravene om sikkerhet og varsling i §§ 7, 8, 10 og 11 gjelder så langt det ikke er fastsatt tilsvarende eller strengere krav i eller i medhold av annen lov.

Kapittel 2. Krav til tilbydere av samfunnsviktige tjenester

§ 6 *Tilbydere av samfunnsviktige tjenester*

Som tilbyder av en samfunnsviktig tjeneste regnes virksomheter som

a. leverer en tjeneste som er viktig for å opprettholde kritiske samfunnsmessige eller økonomiske aktiviteter
b. er avhengig av nettverks- og informasjonssystemer for å levere tjenesten, og
c. kan få tjenesteleveransen betydelig forstyrret av en hendelse.

Ved vurderingen av om en hendelse kan betydelig forstyrre en tjenesteleveranse, skal det særlig legges vekt på

a. antallet brukere som er avhengig av tjenesten
b. i hvilken grad andre samfunnssektorer som er nevnt i § 2, er avhengig av tjenesten
c. hvilken virkning en hendelse kan ha i form av omfang og varighet for økonomiske og sam-

funnsmessige aktiviteter eller samfunnssikkerheten
d. virksomhetens markedsandel
e. størrelsen på det geografiske området som kan bli påvirket av en hendelse
f. den berørte virksomhetens betydning for at det er tilstrekkelig tilgang på tjenesten, tatt i betraktning hvilke alternativer som finnes
g. særlige sektorspesifikke forhold.

Kongen kan gi forskrift om hvilke virksomheter som skal regnes om tilbydere av samfunnsviktige tjenester.

§ 7 *Krav om sikkerhet for tilbydere av samfunnsviktige tjenester*

En tilbyder av en samfunnsviktig tjeneste skal gjennomføre en risikovurdering av nettverks- og informasjonssystemer som benyttes for å levere tjenesten.

Tilbyderen skal iverksette hensiktsmessige og proporsjonale tekniske og organisatoriske sikkerhetstiltak som samlet skal sørge for et sikkerhetsnivå som er tilpasset risikoen. Ved vurderingen av hva som er et forsvarlig sikkerhetsnivå, skal det blant annet ses hen til den teknologiske utviklingen.

Tilbyderen skal iverksette proporsjonale tiltak for å forebygge, avdekke og redusere konsekvensene av hendelser, slik at tjenesteleveransen kan opprettholdes.

§ 8 *Krav om varsling for tilbydere av samfunnsviktige tjenester*

En tilbyder av en samfunnsviktig tjeneste skal uten unødig opphold og uten hinder av taushetsplikt varsle det organet Kongen utpeker, om hendelser som virker betydelig inn på tjenesteleveransen. Ved vurderingen av om innvirkningen er betydelig, skal det blant annet legges vekt på antallet brukere som påvirkes, hendelsens varighet og størrelsen på det geografiske området som berøres.

Kapittel 3. Krav til tilbydere av digitale tjenester

§ 9 *Tilbydere av digitale tjenester*

Som tilbyder av en digital tjeneste regnes virksomheter som tilbyr tjenester som definert i ehandelsloven § 1 andre ledd bokstav a og b i form av nettbaserte markedsplasser, nettbaserte søkemotorer eller skytjenester.

Med nettbasert markedsplass menes en tjeneste som gjør det mulig for forbrukere og næringsdrivende å inngå nettbaserte salgs- eller tjenesteavtaler med næringsdrivende, enten på nettstedet til den nettbaserte markedsplassen eller på nettstedet til en næringsdrivende som bruker datatjenester som leveres av den nettbaserte markedsplassen.

Med nettbasert søkemotor menes en tjeneste som gjør det mulig for brukere å foreta søk på i prinsippet alle nettsteder eller nettsteder på et bestemt språk, på grunnlag av et nøkkelord, en setning eller andre inndata, og som viser lenker hvor det er mulig å finne informasjon om det forespurte innholdet.

Med skytjeneste menes en tjeneste som gir tilgang til en skalerbar og fleksibel samling av delbare databehandlingsressurser.

Kongen kan gi forskrift om hvilke virksomheter som skal regnes som tilbydere av digitale tjenester.

§ 10 *Krav om sikkerhet for tilbydere av digitale tjenester*

En tilbyder av en digital tjeneste skal gjennomføre en risikovurdering av nettverks- og informasjonssystemer som benyttes for å levere tjenesten.

Tilbyderen skal iverksette hensiktsmessige og proporsjonale tekniske og organisatoriske sikkerhetstiltak som samlet skal sørge for et sikkerhetsnivå som er tilpasset risikoen. Ved vurderingen av hva som er et forsvarlig sikkerhetsnivå, skal det blant annet ses hen til den teknologiske utviklingen og tas hensyn til
a. sikkerheten i systemer, utstyr og anlegg
b. hendelseshåndtering
c. styring av opprettholdelse av tjenesteleveransen
d. overvåking, revisjon og testing
e. anerkjente internasjonale standarder.

Tilbyderen skal iverksette proporsjonale tiltak for å forebygge, avdekke og redusere konsekvensene av hendelser, slik at tjenesteleveransen kan opprettholdes.

§ 11 *Krav om varsling for tilbydere av digitale tjenester*

En tilbyder av en digital tjeneste skal uten unødig opphold og uten hinder av taushetsplikt varsle det organ Kongen utpeker om hendelser som virker betydelig inn på tjenesteleveransen. Ved vurderingen av om innvirkningen er betydelig, skal det legges vekt på antall brukere som påvirkes, hendelsens varighet, størrelsen på det geografiske området som berøres, omfanget av funksjonalitetssvikten i tjenesten og omfanget av innvirkningen på økonomisk og samfunnsmessig aktivitet.

§ 12 *Plikt til å utpeke en representant i Norge*

En tilbyder av digitale tjenester som ikke har sitt hovedkontor i Norge eller en annen EØS-stat, og som tilbyr digitale tjenester i Norge, skal utpeke en representant i Norge, med mindre tilbyderen har utpekt en representant i en annen EØS-stat hvor tjenestene tilbys.

Kapittel 4. Tilsyn og administrative reaksjoner

§ 13 *Tilsyn*

Kongen utpeker en eller flere tilsynsmyndigheter som skal føre tilsyn med tilbydere som omfattes av loven.

§ 14 *Opplysningsplikt og tilgang til lokaler og utstyr*

Tilbydere og de som handler på vegne av en tilbyder, har plikt til å gi de opplysningene som tilsynsmyndigheten krever for å utføre sine oppgaver, og gi tilsynsmyndigheten tilgang til virksomhetens lokaler og utstyr og yte nødvendig bistand ved tilsynsmyndighetens undersøkelser.

Første ledd gjelder uten hinder av lovbestemt taushetsplikt.

§ 15 *Pålegg om retting*

Ved overtredelse av bestemmelser gitt i eller i medhold av denne loven kan tilsynsmyndigheten gi tilbydere pålegg om at forholdet skal bringes i orden. Når det gis pålegg, skal det settes en frist for oppfyllelse.

§ 16 *Tvangsmulkt*

Tilsynsmyndigheten kan treffe vedtak om tvangsmulkt for å sikre at pålegg etter § 15 blir oppfylt. Tvangsmulkten kan fastsettes som en løpende mulkt eller som et engangsbeløp.

Tilsynsmyndigheten kan i særlige tilfeller frafalle påløpt tvangsmulkt.

§ 17 *Overtredelsesgebyr*

Tilsynsmyndigheten kan ilegge overtredelsesgebyr dersom en tilbyder eller noen som handler på dennes vegne, forsettlig eller uaktsomt overtrer §§ 7, 8, 10, 11 eller 14.

Dersom den ansvarlige for overtredelsesgebyret er et foretak som inngår i et konsern, hefter foretakets morselskap og morselskapet i det konsern selskapet er en del av, subsidiært for beløpet.

Adgangen til å ilegge overtredelsesgebyr foreldes fem år etter at overtredelsen er opphørt. Fristen avbrytes ved at myndigheten gir forhåndsvarsel om eller fatter vedtak om overtredelsesgebyr.

Kapittel 5. Utfyllende regler mv.

§ 18 *Forskrifter*

Kongen kan gi forskrift om

a. krav til sikkerhet og varsling i samsvar med §§ 7, 8, 10 og 11, herunder hva som regnes som tilsvarende krav etter § 5
b. gjennomføring av tilsyn med tilbydere underlagt loven
c. opplysningsplikt og tilgang til lokaler og utstyr etter § 14
d. ileggelse og utmåling av tvangsmulkt og overtredelsesgebyr
e. at den som forsettlig eller uaktsomt overtrer forskrift gitt i medhold av bokstav a, kan ilegges overtredelsesgebyr
f. gjennomføring av forpliktelser som følger av EØS-avtalen og andre internasjonale avtaler, og som understøtter lovens regler eller formål
g. behandling av personopplysninger, blant annet om formålet med behandlingen, behandlingsansvar, hvilke personopplysninger som kan behandles, viderebehandling, utlevering og sletting
h. nasjonalt kontaktpunkt for sikkerhet i nettverks- og informasjonssystemer.

Kapittel 6. Sikkerhetssertifisering

§ 19 *Sikkerhetssertifisering av informasjons- og kommunikasjonsteknologi*

Kongen kan gi forskrift om sikkerhetssertifisering av IKT-produkter, IKT-tjenester og IKT-prosesser for å gjennomføre forpliktelser etter EØS-avtalen. Dette omfatter også

a. utpeking av sertifiseringsmyndighet
b. tilsyn med sertifiseringsorganer som tilbyr sikkerhetssertifisering av IKT-produkter, IKT-tjenester og IKT-prosesser
c. pålegg om retting, tvangsmulkt og overtredelsesgebyr ved overtredelse av krav til sikkerhetssertifisering.

Kapittel 7. Sluttbestemmelser

§ 20 *Ikrafttredelse*

Loven trer i kraft fra den tiden Kongen bestemmer. De enkelte bestemmelsene kan settes i kraft til ulik tid.

B

Forslag

til vedtak om samtykke til godkjenning av EØS-komiteens beslutninger nr. 21/2023 og 22/2023 om innlemmelse i EØS-avtalen av direktiv (EU) 2016/1148 og forordningene (EU) 2018/151 og (EU) 2019/881

Stortinget samtykker til godkjenning av

1. EØS-komiteens beslutning nr. 21/2023 av 3. februar 2023 om innlemmelse i EØS-avtalen av Europaparlaments- og rådsdirektiv (EU) 2016/1148 av 6. juli 2016 om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i hele Unionen og Kommisjonens gjennomføringsforordning (EU) 2018/151 av 30. januar 2018 om fastsettelse av regler for anvendelse av europaparlaments- og rådsdirektiv (EU) 2016/1148 med hensyn til ytterligere spesifisering av de elementene som tilbydere av digitale tjenester skal ta hensyn til for å håndtere risikoene knyttet til sikkerheten i nettverks- og informasjonssystemer, og av parametrene for å avgjøre om en hendelse har en betydelig innvirkning.
2. EØS-komiteens beslutning nr. 22/2023 av 3. februar 2023 om innlemmelse i EØS-avtalen av Europaparlaments- og rådsforordning (EU) 2019/881 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).

Vedlegg 1

EØS-komiteens beslutning nr. 21/2023 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

EØS-KOMITEEN HAR –

under henvisning til avtalen om Det europeiske økonomiske samarbeidsområde, heretter kalt EØS-avtalen, særlig artikkel 98,

og ut fra følgende betraktninger:

1) Europaparlaments- og rådsdirektiv (EU) 2016/1148 av 6. juli 2016 om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i hele Unionen[1] skal innlemmes i EØS-avtalen.
2) Kommisjonens gjennomføringsforordning (EU) 2018/151 av 30. januar 2018 om fastsettelse av regler for anvendelse av europaparlaments- og rådsdirektiv (EU) 2016/1148 med hensyn til ytterligere spesifisering av de elementene som tilbydere av digitale tjenester skal ta hensyn til for å håndtere risikoene knyttet til sikkerheten i nettverks- og informasjonssystemer, og av parametrene for å avgjøre om en hendelse har en betydelig innvirkning[2] skal innlemmes i EØS-avtalen.
3) For at EØS-avtalen skal fungere godt, må avtalens protokoll 37 utvides til å omfatte samarbeidsgruppen opprettet ved direktiv (EU) 2016/1148.
4) EØS-avtalens vedlegg XI og protokoll 37 bør derfor endres –

TRUFFET DENNE BESLUTNING:

Artikkel 1

I EØS-avtalens vedlegg XI, etter nr. 5cp (europaparlaments- og rådsforordning (EU) nr. 526/2013), tilføyes følgende:

«5cpa. **32016 L 1148:** Europaparlaments- og rådsdirektiv (EU) 2016/1148 av 6. juli 2016 om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i hele Unionen (EUT L 194 av 19.7.2016, s. 1).

Nærmere regler for EFTA-statenes tilknytning i samsvar med EØS-avtalens artikkel 101:

EFTA-statene skal delta fullt ut i samarbeidsgruppen og skal der ha de samme rettighetene og pliktene som EUs medlemsstater, unntatt stemmerett.

5cpaa. **32018 R 0151:** Kommisjonens gjennomføringsforordning (EU) 2018/151 av 30. januar 2018 om fastsettelse av regler for anvendelse av europaparlaments- og rådsdirektiv (EU) 2016/1148 med hensyn til ytterligere spesifisering av de elementene som tilbydere av digitale tjenester skal ta hensyn til for å håndtere risikoene knyttet til sikkerheten i nettverks- og informasjonssystemer, og av parametrene for å avgjøre om en hendelse har en betydelig innvirkning (EUT L 26 av 31.1.2018, s. 48).»

---

1 EUT L 194 av 19.7.2016, s. 1.

2 EUT L 26 av 31.1.2018, s. 48.

Artikkel 2

I EØS-avtalens protokoll 37 skal nytt nummer lyde:

«47. Samarbeidsgruppen (europaparlaments- og rådsdirektiv (EU) 2016/1148 av 6. juli 2016 om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i hele Unionen).»

Artikkel 3

Teksten til direktiv (EU) 2016/1148 og gjennomføringsforordning (EU) 2018/151 på islandsk og norsk, som vil bli kunngjort i EØS-tillegget til *Den europeiske unions tidende*, skal gis gyldighet.

Artikkel 4

Denne beslutning trer i kraft 4. februar 2023, forutsatt at alle meddelelser etter EØS-avtalens artikkel 103 nr. 1 er inngitt[3].

Artikkel 5

Denne beslutning skal kunngjøres i EØS-avdelingen av og EØS-tillegget til *Den europeiske unions tidende*.

Utferdiget i Brussel 3. februar 2023.

For EØS-komiteen

Nicolas von Lingen
Formann

[3] Forfatningsrettslige krav angitt.

Vedlegg 2

EØS-komiteens beslutning nr. 22/2023 av 3. februar 2023 om endring av EØS-avtalens vedlegg IX (Elektronisk kommunikasjon, audiovisuelle tjenester og informasjonssamfunnstjenester) og protokoll 37 om listen omhandlet i artikkel 101

EØS-KOMITEEN HAR –

under henvisning til avtalen om Det europeiske økonomiske samarbeidsområde, heretter kalt EØS-avtalen, særlig artikkel 98,

og ut fra følgende betraktninger:

1) Europaparlaments- og rådsforordning (EU) 2019/881 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)[1] skal innlemmes i EØS-avtalen.
2) Forordning (EU) 2019/881 opphever europaparlaments- og rådsforordning (EU) nr. 526/2013[2], som er innlemmet i EØS-avtalen, og som følgelig skal oppheves i EØS-avtalen.
3) EØS-avtalens vedlegg XI og protokoll 37 bør derfor endres –

TRUFFET DENNE BESLUTNING:

Artikkel 1

I EØS-avtalens vedlegg XI skal teksten i nr. 5cp (europaparlaments- og rådsforordning (EU) nr. 526/2013) lyde:

«**32019 R 0881:** Europaparlaments- og rådsforordning (EU) 2019/881 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) (EUT L 151 av 7.6.2019, s. 15).

Forordningens bestemmelser skal for denne avtales formål gjelde med følgende tilpasninger:

a) Med mindre annet er fastsatt under, og uten at det berører bestemmelsene i avtalens protokoll 1, skal betegnelsen 'medlemsstat(er)' og andre betegnelser i forordningen som viser til deres myndigheter, i tillegg til den betydning de har i forordningen, også omfatte EFTA-statene og deres myndigheter.
b) Med hensyn til EFTA-statene skal Byrået, slik og når det er hensiktsmessig, bistå EFTAs overvåkingsorgan eller eventuelt Den faste komité i utførelsen av deres respektive oppgaver.
c) Med hensyn til EFTA-statene skal henvisninger til unionsretten forstås som henvisninger til EØS-avtalen.
d) I artikkel 14 skal nytt nummer lyde:
'5. EFTA-statene skal delta fullt ut i styret og skal der ha de samme rettighetene og pliktene som EUs medlemsstater, unntatt stemmerett.'
e) I artikkel 28 skal nytt nummer lyde:
'4. Ved anvendelse av denne forordningen skal forordning (EF) nr. 1049/2001 få anvendelse på alle Byråets dokumenter som også angår EFTA-statene.'
f) I artikkel 30 skal nytt nummer lyde:
'3. EFTA-statene skal delta i bidraget fra Unionen nevnt i nr. 1 bokstav a). For dette formålet skal framgangsmåtene fastsatt i EØS-avtalens artikkel 82 nr. 1 bokstav a) og protokoll 32 få tilsvarende anvendelse.'
g) I artikkel 34 skal nytt ledd lyde:
'Som unntak fra artikkel 12 nr. 2 bokstav a) og artikkel 82 nr. 3 bokstav a) i Tilsettingsvilkår for andre tjenestemenn i Den

[1] EUT L 151 av 7.6.2019, s. 15.
[2] EUT L 165 av 18.6.2013, s. 41.

europeiske union kan statsborgere i EFTA-stater som nyter fulle borgerrettigheter, tilsettes på kontrakt av Byråets daglige leder.'

h) I artikkel 35 skal nytt ledd lyde:

'EFTA-statene skal tilstå Byrået og dets ansatte privilegier og immunitet tilsvarende de som er omhandlet i protokollen om Den europeiske unions privilegier og immunitet.'

i) I artikkel 40 skal nytt nummer lyde:

'3. Som unntak fra artikkel 12 nr. 2 bokstav e), artikkel 82 nr. 3 bokstav e) og artikkel 85 nr. 3 i Tilsettingsvilkår for andre tjenestemenn i Den europeiske union skal språkene nevnt i EØS-avtalens artikkel 129 nr. 1 anses av Byrået, med hensyn til sine ansatte, som et av Unionens språk nevnt i artikkel 55 nr. 1 i traktaten om Den europeiske union.'

j) I artikkel 62 skal nytt nummer lyde:

'6. EFTA-statene skal delta fullt ut, uten stemmerett, i ECCG.'»

Artikkel 2

I EØS-avtalens protokoll 37 skal nytt nummer lyde:

«48. Den europeiske cybersikkerhetssertifiseringsgruppen (europaparlaments- og rådsforordning (EU) 2019/881).»

Artikkel 3

Teksten til forordning (EU) 2019/881 på islandsk og norsk, som vil bli kunngjort i EØS-tillegget til *Den europeiske unions tidende*, skal gis gyldighet.

Artikkel 4

Denne beslutning trer i kraft 4. februar 2023, forutsatt at alle meddelelser etter EØS-avtalens artikkel 103 nr. 1 er inngitt[3], eller på den dag EØS-komiteens beslutning nr. 21/2023 av 3. februar 2023[4] trer i kraft, alt etter hva som inntreffer sist.

Artikkel 5

Denne beslutning skal kunngjøres i EØS-avdelingen av og EØS-tillegget til *Den europeiske unions tidende*.

Utferdiget i Brussel 3. februar 2023.

For EØS-komiteen

Nicolas von Lingen
Formann

Felleserklæring fra avtalepartene i forbindelse med EØS-komiteens beslutning nr. 22/2023 som innlemmer europaparlaments- og rådsforordning (EU) 2019/881 i EØS-avtalen

Partene erkjenner at innlemmingen av denne rettsakten ikke berører den direkte anvendelsen av protokoll 7 om Den europeiske unions privilegier og immunitet på statsborgere i EFTA-stater på territoriet til den enkelte medlemsstat i Den europeiske union i henhold til artikkel 11 i nevnte protokoll.

---

[3] Forfatningsrettslige krav angitt.

[4] Ennå ikke kunngjort.

Vedlegg 3

Europaparlaments- og rådsdirektiv (EU) 2016/1148 av 6. juli 2016 om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i hele Unionen

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],

etter den ordinære regelverksprosessen[2] og

ut fra følgende betraktninger:

1) Nettverks- og informasjonssystemer og nettverks- og informasjonstjenester har en viktig rolle i samfunnet. Deres pålitelighet og sikkerhet er grunnleggende for økonomisk og samfunnsmessig virksomhet, og særlig for det indre markeds virkemåte.
2) Omfanget, hyppigheten og virkningen av sikkerhetshendelser er økende og utgjør en alvorlig trussel mot virkemåten til nettverks- og informasjonssystemer. Disse systemene kan også bli mål for tilsiktede skadelige handlinger beregnet på å skade eller forstyrre driften av systemene. Slike hendelser kan være til hinder for utøvelse av økonomisk virksomhet, skape betydelige økonomiske tap, undergrave brukernes tillit og få store negative konsekvenser for Unionens økonomi.
3) Nettverks- og informasjonssystemer, særlig Internett, er grunnleggende for å gjennomføre bevegelighet over landegrensene for varer, tjenester og personer. På grunn av det tverrnasjonale aspektet kan betydelige forstyrrelser i disse systemene, enten de er tilsiktet eller utilsiktet og uansett hvor de finner sted, påvirke de enkelte medlemsstatene og Unionen som helhet. Sikkerheten i nettverks- og informasjonssystemer er derfor avgjørende for et velfungerende indre marked.
4) På grunnlag av den store framdriften innenfor det europeiske forum for medlemsstater med hensyn til å fremme drøftinger og utveksling av god praksis, herunder utarbeiding av prinsipper for et europeisk samarbeid i tilfelle datarelaterte kriser, bør det opprettes en samarbeidsgruppe bestående av representanter for medlemsstatene, Kommisjonen og Den europeiske unions byrå for nettverks- og informasjonssikkerhet («ENISA») for å støtte og lette strategisk samarbeid mellom medlemsstatene om sikkerhet i nettverks- og informasjonssystemer. For at gruppen skal være effektiv og inkluderende, er det viktig at alle medlemsstater oppfyller et minstekrav til ressurser og har en strategi som sikrer et høyt nivå for sikkerhet i nettverks- og informasjonssystemer på eget territorium. I tillegg bør ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester være underlagt sikkerhets- og meldingskrav med henblikk på å fremme en kultur for risikohåndtering og sikre rapportering av de mest alvorlige hendelsene.
5) De eksisterende ressursene er ikke tilstrekkelige til å sikre et høyt nivå for sikkerhet i nettverks- og informasjonssystemene i Unionen. Medlemsstatene har svært ulike beredskapsnivåer, noe som har ført til en usammenhengende tilnærming i hele Unionen. Dette fører til ulike vernenivåer for forbrukere og foretak, og undergraver det generelle nivået for sikkerhet i nettverks- og informasjonssystemer i Unionen. Mangelen på felles krav til ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester gjør det i sin tur umulig å opprette en global og effektiv ordning for samarbeid på unionsplan. Universiteter og forsk-

---

1 EUT C 271 av 19.9 2013, s. 133.

2 Europaparlamentets holdning av 13. mars 2014 (ennå ikke offentliggjort i EUT) og Rådets holdning ved første behandling av 17. mai 2016 (ennå ikke offentliggjort i EUT). Europaparlamentets holdning av 6. juli 2016 (ennå ikke offentliggjort i EUT).

ningssentre er avgjørende for å anspore til forskning, utvikling og innovasjon på disse områdene.

6) Effektive tiltak for å løse utfordringer knyttet til sikkerhet i nettverks- og informasjonssystemer krever derfor en global tilnærming på unionsplan som omfatter felles minstekrav til kapasitetsoppbygging og planlegging, utveksling av opplysninger, samarbeid og felles sikkerhetskrav til ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester. Ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester er imidlertid ikke forhindret fra å gjennomføre sikkerhetstiltak som er strengere enn dem som er fastsatt i dette direktiv.
7) For å dekke alle relevante hendelser og risikoer bør dette direktiv få anvendelse på både ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester. Forpliktelsene som innføres for ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester, bør imidlertid ikke få anvendelse på foretak som leverer offentlige kommunikasjonsnett eller offentlig tilgjengelige elektroniske kommunikasjonstjenester i henhold til europaparlaments- og rådsdirektiv 2002/21/EF[3], som omfattes av de særlige kravene til sikkerhet og integritet som er fastsatt i nevnte direktiv, og heller ikke på ytere av tillitstjenester i henhold til europaparlaments- og rådsforordning (EU) nr. 910/2014[4], som omfattes av sikkerhetskravene fastsatt i nevnte forordning.
8) Dette direktiv bør ikke berøre muligheten hver enkelt medlemsstat har til å treffe nødvendige tiltak for å sikre vern av grunnleggende sikkerhetsinteresser, opprettholde offentlig orden og sikkerhet samt muliggjøre etterforskning, avsløring og rettslig forfølging av straffbare handlinger. I samsvar med artikkel 346 i traktaten om Den europeiske unions virkemåte (TEUV) er ingen medlemsstat forpliktet til å gi opplysninger dersom den finner at det vil være i strid med dens grunnleggende sikkerhetsinteresser. I denne sammenheng er rådsbeslutning 2013/488/EU[5] og avtaler om taushetsplikt eller uformelle avtaler om taushetsplikt, som «Traffic Light Protocol», relevante.
9) Visse økonomiske sektorer er allerede regulert eller kan reguleres i framtiden ved sektorspesifikke unionsrettsakter som omfatter regler knyttet til sikkerhet i nettverks- og informasjonssystemer. Når disse unionsrettsaktene inneholder bestemmelser om innføring av krav til sikkerhet i nettverks- og informasjonssystemer eller meldinger om hendelser, bør disse bestemmelsene få anvendelse dersom de inneholder krav som i praksis minst tilsvarer forpliktelsene i dette direktiv. Medlemsstatene bør i så fall anvende bestemmelsene i slike sektorspesifikke unionsrettsakter, herunder bestemmelser som berører jurisdiksjon, og bør ikke gjennomføre identifikasjonsprosessen for ytere av samfunnsviktige tjenester som definert i dette direktiv. I den forbindelse bør medlemsstatene gi Kommisjonen opplysninger om anvendelsen av slike *lex specialis*. For å avgjøre om kravene til sikkerhet i nettverks- og informasjonssystemer og meldinger om hendelser som inngår i sektorspesifikke unionsrettsakter, tilsvarer dem som er fastsatt i dette direktiv, bør det tas hensyn bare til bestemmelsene i relevante unionsrettsakter og deres anvendelse i medlemsstatene.
10) I sektoren for transport på vannveier omfatter sikkerhetskravene til rederier, fartøyer, havneanlegg, havner og sjøtrafikksentraler i henhold til unionsrettsakter all virksomhet, herunder radio- og telekommunikasjonsutstyr, datasystemer og nettverk. De obligatoriske prosedyrene som skal følges, omfatter blant annet rapportering av alle hendelser, og bør derfor anses som *lex specialis*, i den utstrekning disse kravene minst tilsvarer de tilsvarende bestemmelsene i dette direktiv.
11) Når medlemsstatene identifiserer operatører i sektoren for transport på vannveier, bør de ta hensyn til eksisterende og kommende internasjonale regler og retningslinjer utarbeidet særlig av Den internasjonale sjøfartsorganisasjon, med sikte på å skape en enhetlig tilnærming for individuelle sjøtransportoperatører.
12) Regulering av og tilsyn med sektorene for bankvirksomhet og infrastrukturer i finansmarkedene er svært harmonisert på unionsplan gjennom Unionens primærrett og avledet

---

[3] Europaparlaments- og rådsdirektiv 2002/21/EF av 7. mars 2002 om felles rammeregler for elektroniske kommunikasjonsnett og -tjenester (rammedirektivet) (EFT L 108 av 24.4.2002, s. 33).

[4] 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).

[5] Rådsbeslutning 2013/488/EU av 23. september 2013 om sikkerhetsregler for vern av graderte EU-opplysninger (EUT L 274 av 15.10.2013, s. 1).

regelverk samt standarder utviklet i samarbeid med de europeiske tilsynsmyndighetene. Innenfor bankunionen sikres anvendelsen og tilsynet med disse kravene gjennom den felles tilsynsordningen. For medlemsstater som ikke er en del av bankunionen, sikres dette av medlemsstatenes relevante banktilsynsmyndigheter. På andre områder av tilsynet med finanssektoren bidrar også Det europeiske finanstilsynssystem til å sikre en høy grad av ensartethet og sammenfall i tilsynspraksis. Den europeiske verdipapir- og markedstilsynsmyndighet fører også direkte tilsyn med visse foretak, nærmere bestemt kredittvurderingsbyråer og transaksjonsregistre.

13) Operasjonell risiko er en viktig del av reguleringen av og tilsynet med sektorene for bankvirksomhet og infrastrukturer i finansmarkedet. Den omfatter all virksomhet, herunder nettverks- og informasjonssystemers sikkerhet, funksjonsdyktighet og robusthet. Kravene til disse systemene, som ofte går lenger enn kravene fastsatt i dette direktiv, er fastsatt i en rekke unionsrettsakter, herunder regler for adgang til å utøve virksomhet som kredittinstitusjon og tilsyn med kredittinstitusjoner og verdipapirforetak samt regler for tilsynskrav for kredittinstitusjoner og verdipapirforetak, som omfatter krav med hensyn til operasjonell risiko, regler for markeder for finansielle instrumenter, som omfatter krav med hensyn til risikovurdering for verdipapirforetak og for regulerte markeder, regler for OTC-derivater, sentrale motparter og transaksjonsregistre, som omfatter krav med hensyn til operasjonell risiko for sentrale motparter og transaksjonsregistre, og regler for forbedring av oppgjørssystemet for verdipapirer i Unionen og om verdipapirsentraler, som omfatter krav med hensyn til operasjonell risiko. Videre er krav til melding om hendelser en del av vanlig tilsynspraksis i finanssektoren og inngår ofte i tilsynshåndbøker. Medlemsstatene bør vurdere disse reglene og kravene i sin søknad om *lex specialis*.

14) Som Den europeiske sentralbank bemerker i sin uttalelse av 25. juli 2014[6] berører ikke dette direktiv ordningen som er fastsatt i unionsretten for Eurosystemets tilsyn med betalings- og oppgjørssystemer. Det vil være hensiktsmessig for myndigheter med ansvar for slikt tilsyn å utveksle erfaringer om spørsmål som gjelder sikkerhet i nettverks- og informasjonssystemer, med vedkommende myndigheter i henhold til dette direktiv. Det samme gjelder for medlemmer i Det europeiske system av sentralbanker som står utenfor euroområdet og som fører slikt tilsyn med betalings- og oppgjørssystemer på grunnlag av nasjonale lover og forskrifter.

15) En nettbasert markedsplass gjør det mulig for forbrukere og næringsdrivende å inngå nettbaserte salgs- eller tjenesteavtaler med næringsdrivende, og er det endelige bestemmelsesstedet for inngåelse av slike avtaler. Den bør ikke omfatte nettbaserte tjenester som fungerer bare som en formidler av tredjemannstjenester hvor det er mulig å inngå en avtale i siste instans. Den bør derfor ikke omfatte nettbaserte tjenester som sammenligner prisen på bestemte produkter eller tjenester fra forskjellige næringsdrivende, og deretter omdirigerer brukeren til den foretrukne næringsdrivende for å kjøpe produktet. Datatjenester som leveres av den nettbaserte markedsplassen, kan omfatte behandling av transaksjoner, sammenslåing av data eller profilering av brukere. Programbutikker, som fungerer som nettbutikker med henblikk på digital distribusjon av programmer eller programvare fra tredjemann, skal anses som en type nettbasert markedsplass.

16) En nettbasert søkemotor gjør det i prinsippet mulig for brukeren å foreta søk på alle nettsteder på grunnlag av et søk innenfor et hvilket som helst emne. Den kan også være rettet mot nettsteder på et bestemt språk. Definisjonen av en nettbasert søkemotor som er fastsatt i dette direktiv, bør ikke omfatte søkefunksjoner som er begrenset til innholdet på et bestemt nettsted, uansett om søkefunksjonen drives av en ekstern søkemotor. Den bør heller ikke omfatte nettbaserte tjenester som sammenligner prisen på bestemte produkter eller tjenester fra forskjellige næringsdrivende, og deretter omdirigerer brukeren til den foretrukne næringsdrivende for å kjøpe produktet.

17) Skytjenester omfatter et bredt spekter av aktiviteter som kan leveres i henhold til ulike modeller. Med henblikk på dette direktiv omfatter «skytjenester» tjenester som gir tilgang til en skalerbar og fleksibel samling av delbare databehandlingsressurser. Disse databehandlingsressursene omfatter ressurser som nettverk, servere eller annen infrastruktur, lagring, programmer og tjenester. Begrepet «skalerbar» henspiller på databehandlingsressurser som tilbyderen av skytjenester for-

[6] EUT C 352 av 7.10.2014, s. 4.

deler på en fleksibel måte, uavhengig av ressursenes geografiske plassering, for å håndtere svingninger i etterspørselen. Begrepet «fleksibel samling» brukes til å beskrive databehandlingsressurser som stilles til rådighet og utnyttes avhengig av etterspørsel, slik at tilgjengelige ressurser raskt kan økes eller minskes i takt med arbeidsmengden. Begrepet «delbar» brukes til å beskrive databehandlingsressurser som leveres til flere brukere som har felles tilgang til tjenesten, men hvor databehandlingen foretas separat for hver enkelt bruker, selv om tjenesten leveres fra samme elektroniske utstyr.

18) Funksjonen til et samtrafikkpunkt på Internettverk (IXP) er å sammenkople nettverk. Et IXP gir ikke netttilgang og fungerer ikke som transittleverandør eller transittoperatør. Et IXP besørger heller ikke andre tjenester uten tilknytning til samtrafikk, men dette hindrer ikke en IXP-operatør i å yte andre tjenester. Formålet med et IXP er å sammenkople nettverk som er teknisk og organisatorisk atskilt. Begrepet «autonomt system» brukes til å beskrive et teknisk frittstående nettverk.

19) Medlemsstatene bør ha ansvar for å fastsette hvilke foretak som oppfyller kriteriene i definisjonen av yter av samfunnsviktige tjenester. For å sikre en ensartet tilnærming bør definisjonen av yter av samfunnsviktige tjenester anvendes konsekvent av alle medlemsstatene. For dette formål inneholder dette direktiv bestemmelser om vurdering av foretak som er virksomme i bestemte sektorer og delsektorer, opprettelse av en liste over samfunnsviktige tjenester, overveielse av en felles liste over forhold på tvers av sektorer for å avgjøre om en hendelse vil kunne ha en betydelig forstyrrende virkning, en samrådsprosess som involverer relevante medlemsstater når det gjelder foretak som yter tjenester i mer enn én medlemsstat, og støtte til samarbeidsgruppen i identifikasjonsprosessen. For å sikre at eventuelle endringer i markedet gjenspeiles riktig bør listen over identifiserte ytere gjennomgås jevnlig av medlemsstatene og ajourføres ved behov. Til slutt bør medlemsstatene framlegge for Kommisjonen de nødvendige opplysninger for å vurdere i hvilken grad denne felles metoden har gjort det mulig for medlemsstatene å anvende definisjonen på en ensartet måte.

20) I forbindelse med identifisering av ytere av samfunnsviktige tjenester bør medlemsstatene, minst for hver delsektor som er omhandlet i dette direktiv, vurdere hvilke tjenester som må anses som grunnleggende for å opprettholde viktig samfunnsmessig og økonomisk virksomhet, samt om foretakene som er oppført på listen over de sektorer og delsektorer som er nevnt i dette direktiv og yter disse tjenestene, oppfyller kriteriene for identifikasjon av ytere. Ved vurderingen av hvorvidt et foretak yter en tjeneste som er grunnleggende for å opprettholde viktig samfunnsmessig eller økonomisk virksomhet, er det tilstrekkelig å undersøke hvorvidt foretaket yter en tjeneste som er oppført på listen over samfunnsviktige tjenester. Videre bør det dokumenteres at ytingen av den samfunnsviktige tjenesten er avhengig av nettverks- og informasjonssystemer. Avslutningsvis bør medlemsstatene, når de vurderer om en hendelse vil kunne ha en betydelig forstyrrende virkning på ytingen av tjenesten, ta hensyn til en rekke forhold på tvers av sektorer samt til eventuelle sektorspesifikke forhold.

21) For å identifisere ytere av samfunnsviktige tjenester innebærer virksomhet i en medlemsstat en effektiv og faktisk utøvelse av aktivitet gjennom en stabil struktur. En slik strukturs juridiske form, enten det dreier seg om en filial eller et datterforetak med status som juridisk person, er ikke av avgjørende betydning i den forbindelse.

22) Det er mulig at foretak som driver virksomhet i de sektorer og delsektorer som er nevnt i dette direktiv, yter både samfunnsviktige og ikke-samfunnsviktige tjenester. I sektoren for lufttransport yter for eksempel lufthavner tjenester som en medlemsstat kan anse som samfunnsviktige, som styring av rullebaner, men også en rekke tjenester som kan anses som ikke-samfunnsviktige, som tilrettelagte handleområder. Ytere av samfunnsviktige tjenester bør være underlagt de særlige sikkerhetskravene bare med hensyn til de tjenestene som anses som samfunnsviktige. For å identifisere ytere bør medlemsstatene derfor utarbeide en liste over tjenester som anses som samfunnsviktige.

23) Listen bør inneholde alle tjenester som ytes på territoriet til en medlemsstat som oppfyller kravene i dette direktiv. Medlemsstatene bør ha mulighet til å supplere den eksisterende listen ved å tilføye nye tjenester. Listen over tjenester bør fungere som et referansepunkt for medlemsstatene og gjøre det mulig å identifisere ytere av samfunnsviktige tjenester. Formålet med listen er å identifisere de typer av samfunnsviktige tjenester i en bestemt sek-

tor som er nevnt i dette direktiv, slik at de kan holdes atskilt fra ikke-samfunnsviktige tjenester som et foretak med virksomhet i en bestemt sektor kan være ansvarlig for. Listen over tjenester som hver enkelt medlemsstat oppretter, vil kunne bidra ytterligere til vurderingen av lovgivningsmessig praksis i hver medlemsstat med sikte på å sikre en overordnet sammenheng i identifikasjonsprosessen mellom medlemsstatene.

24) Når et foretak yter en samfunnsviktig tjeneste i to eller flere medlemsstater, bør disse medlemsstatene delta i bilaterale eller multilaterale drøftinger med hverandre i forbindelse med identifikasjonsprosessen. Denne samrådsprosessen er ment å hjelpe dem med å vurdere om den aktuelle yteren er av kritisk betydning når det gjelder virkninger på tvers av landegrensene, hvilket gir hver berørte medlemsstat mulighet til å framlegge sine synspunkter med hensyn til risikoene forbundet med de tjenestene som ytes. I denne prosessen bør de berørte medlemsstatene ta hensyn til hverandres synspunkter og bør i den forbindelse kunne be om bistand fra samarbeidsgruppen.

25) Som følge av identifikasjonsprosessen bør medlemsstatene vedta nasjonale tiltak for å fastsette hvilke foretak som er underlagt forpliktelser med hensyn til sikkerhet i nettverks- og informasjonssystemer. Dette kan oppnås ved å vedta en liste over alle ytere av samfunnsviktige tjenester eller ved å vedta nasjonale tiltak, herunder objektive målbare kriterier, for eksempel yterens produksjon eller antall brukere, som gjør det mulig å bestemme hvilke foretak som er underlagt forpliktelser med hensyn til sikkerhet i nettverks- og informasjonssystemer. De nasjonale tiltakene, uansett om de allerede er vedtatt eller om de vedtas innenfor rammen av dette direktiv, bør omfatte alle rettslige tiltak, administrative tiltak og strategier som gjør det mulig å identifisere ytere av samfunnsviktige tjenester i henhold til dette direktiv.

26) For å gi en indikasjon på hvilken betydning identifiserte ytere av samfunnsviktige tjenester har i den berørte sektoren, bør medlemsstatene ta hensyn til yternes antall og størrelse, for eksempel når det gjelder markedsandeler eller mengden som er produsert eller levert, uten å være forpliktet til å gi videre opplysninger som viser hvilke ytere som er identifisert.

27) For å avgjøre om en hendelse vil kunne ha en betydelig forstyrrende virkning på en samfunnsviktig tjeneste bør medlemsstatene ta hensyn til en rekke ulike forhold, for eksempel antall brukere som er avhengige av tjenesten til private eller yrkesmessige formål. Bruken av nevnte tjeneste kan skje direkte, indirekte eller gjennom formidling. Når medlemsstatene skal vurdere i hvilken grad og hvor lenge en hendelse vil kunne påvirke økonomisk og samfunnsmessig virksomhet eller offentlig sikkerhet, bør de også vurdere hvor lang tid det sannsynligvis vil ta før avbruddet får en negativ virkning.

28) I tillegg til forhold på tvers av sektorer bør de også vurdere sektorspesifikke forhold for å avgjøre om en hendelse vil kunne ha en betydelig forstyrrende virkning på ytingen av en samfunnsviktig tjeneste. Med hensyn til energileverandører kan slike forhold for eksempel omfatte mengden eller andelen elektrisitet som er produsert nasjonalt; for oljeleverandører mengden olje per dag; for lufttransport, herunder lufthavner og luftfartsselskaper, jernbanetransport og sjøhavner, den nasjonale andelen av trafikkmengden og antall passasjerer eller størrelsen på fraktvirksomheten per år; for bankvirksomhet eller finansmarkedenes infrastrukturer deres betydning for systemet på grunnlag av samlede eiendeler eller forholdet mellom samlede eiendeler og BNP; for helsesektoren antall pasienter som tjenesteyteren pleier per år; for produksjon, behandling og forsyning av vann mengden, antall og typer brukere som forsynes, herunder for eksempel sykehus, organisasjoner i offentlig sektor eller enkeltpersoner, samt om det finnes alternative vannkilder som dekker samme geografiske område.

29) For å oppnå og opprettholde et høyt nivå av sikkerhet i nettverks- og informasjonssystemer bør hver medlemsstat ha en nasjonal strategi for sikkerhet i nettverks- og informasjonssystemer som definerer strategiske mål og konkrete politiske tiltak som skal gjennomføres.

30) På bakgrunn av forskjellene i nasjonale styringsstrukturer og for å verne eksisterende sektorspesifikke ordninger eller Unionens tilsyns- og reguleringsorganer, og for å unngå dobbeltarbeid, bør medlemsstatene kunne utpeke mer enn én vedkommende nasjonal myndighet med ansvar for å utføre oppgavene knyttet til sikkerhet i nettverks- og informasjonssystemer hos ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester i henhold til dette direktiv.

31) For å legge til rette for samarbeid og kommunikasjon over landegrensene og gjøre det mulig å gjennomføre dette direktiv effektivt må hver medlemsstat, uten at det berører sektorspesifikke regelverk, utpeke et nasjonalt felles kontaktpunkt med ansvar for å samordne spørsmål knyttet til sikkerhet i nettverks- og informasjonssystemer og samarbeid over landegrensene på unionsplan. Vedkommende myndigheter og de felles kontaktpunktene bør ha tilstrekkelige tekniske, økonomiske og menneskelige ressurser til å sikre at de kan utføre sine oppgaver på en effektiv og formålstjenlig måte, og dermed nå målene for dette direktiv. Ettersom dette direktiv har som mål å forbedre det indre markeds virkemåte ved å skape tillit og tiltro, må medlemsstatenes organer kunne samarbeide effektivt med økonomiske aktører og ha en struktur som er forenlig med dette.
32) Vedkommende myndigheter eller enheter for håndtering av digitale hendelser («CSIRT-enheter») bør motta meldinger om hendelser. De felles kontaktpunktene bør ikke motta meldinger om eventuelle hendelser direkte, med mindre de også fungerer som en vedkommende myndighet eller en CSIRT-enhet. En vedkommende myndighet eller en CSIRT-enhet bør imidlertid kunne gi det felles kontaktpunktet i oppgave å videreformidle meldinger om hendelser til de felles kontaktpunktene i andre berørte medlemsstater.
33) For å sikre at medlemsstatene og Kommisjonen får opplysninger på en effektiv måte bør det felles kontaktpunktet sende en sammenfattende rapport til samarbeidsgruppen, og rapporten bør anonymiseres for å sikre fortrolig behandling av meldingene og identiteten til ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester, ettersom opplysninger om identiteten til melderen ikke er påkrevd for utvekslingen av beste praksis i samarbeidsgruppen. Den sammenfattende rapporten bør omfatte opplysninger om antall mottatte meldinger og arten av de meldte hendelsene, for eksempel type sikkerhetsbrudd, alvorlighetsgrad eller varighet.
34) Medlemsstatene bør ha tilstrekkelige tekniske og organisatoriske ressurser til å forebygge, avdekke, håndtere og begrense virkningen av hendelser og risikoer knyttet til nettverks- og informasjonssystemer. Medlemsstatene bør derfor sikre at de har velfungerende CSIRT-enheter, også kjent som CERT-enheter, som oppfyller grunnleggende krav og kan sikre effektive og kompatible ressurser til å håndtere eventuelle hendelser og risikoer og sikre effektivt samarbeid på unionsplan. For at alle typer ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester skal kunne dra nytte av slike ressurser og slikt samarbeid, bør medlemsstatene sikre at alle typer omfattes av en utpekt CSIRT-enhet. Med tanke på betydningen av internasjonalt samarbeid på området datasikkerhet bør CSIRT-enheter kunne delta i internasjonale samarbeidsnett i tillegg til CSIRT-nettverket som opprettes ved dette direktiv.
35) Ettersom de fleste nettverks- og informasjonssystemer drives privat, er samarbeidet mellom offentlig og privat sektor avgjørende. Ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester bør oppmuntres til å opprette egne uformelle samarbeidsordninger for å sikre sikkerheten i nettverks- og informasjonssystemer. Samarbeidsgruppen bør ved behov kunne innby berørte parter til drøftinger. For å oppmuntre effektivt til utveksling av opplysninger og beste praksis er det viktig å sikre at samarbeidet ikke innebærer ulemper for ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester som deltar i slik utveksling.
36) ENISA bør bistå medlemsstatene og Kommisjonen ved å gi sakkunnskap og råd og ved å fremme utveksling av beste praksis. Særlig ved anvendelsen av dette direktiv bør Kommisjonen og medlemsstatene kunne rådføre seg med ENISA. For å bygge opp kapasitet og kunnskap blant medlemsstatene bør samarbeidsgruppen også fungere som et verktøy for utveksling av beste praksis, drøftinger av medlemsstatenes ressurser og beredskap og, på frivillig grunnlag, bistå sine medlemmer med å evaluere nasjonale strategier for sikkerhet i nettverks- og informasjonssystemer, bygge opp kapasiteten og evaluere øvelser knyttet til sikkerheten i nettverks- og informasjonssystemer.
37) Når det er hensiktsmessig, bør medlemsstatene kunne anvende eller tilpasse eksisterende organisasjonsstrukturer eller strategier ved anvendelsen av dette direktiv.
38) De respektive oppgavene til samarbeidsgruppen og ENISA er innbyrdes avhengige og utfyller hverandre. Generelt bør ENISA bistå samarbeidsgruppen med utførelsen av dens oppgaver i samsvar med ENISAs mål som fastsatt i europaparlaments- og rådsforordning (EU) nr. 526/2013[7], som er å bistå Unionens institusjoner, organer, kontorer og byråer og

medlemsstatene med å gjennomføre den politikken som er nødvendig for å oppfylle de lovfestede og forskriftsmessige kravene til sikkerhet i nettverks- og informasjonssystemer i henhold til gjeldende og framtidige unionsrettsakter. ENISA bør særlig yte bistand på de områder som svarer til ENISAs egne oppgaver som fastsatt i forordning (EU) nr. 526/2013, som er å analysere strategier for sikkerhet i nettverks- og informasjonssystemer, støtte organiseringen og gjennomføringen av øvelser på unionsplan som gjelder sikkerhet i nettverks- og informasjonssystemer, samt utveksle opplysninger og beste praksis med hensyn til holdningsskapende tiltak og opplæring. ENISA bør også delta i utarbeidingen av retningslinjer for sektorspesifikke kriterier som skal brukes til å fastsette betydningen til virkningen av en hendelse.

39) For å fremme avansert sikkerhet for nettverks- og informasjonssystemer bør samarbeidsgruppen ved behov samarbeide med Unionens relevante institusjoner, organer, kontorer og byråer for å utveksle kunnskap og beste praksis samt gi råd om sikkerhetsaspekter ved nettverks- og informasjonssystemer som kan påvirke deres arbeid, idet det tas hensyn til eksisterende ordninger for utveksling av opplysninger som omfattes av restriksjoner. Når samarbeidsgruppen samarbeider med myndigheter som har ansvar for håndheving av loven, om sikkerhetsaspekter ved nettverkverks- og informasjonssystemer som kan påvirke deres arbeid, bør samarbeidsgruppen respektere eksisterende informasjonskanaler og etablerte nettverk.

40) Opplysninger om hendelser blir stadig mer verdifulle for allmennheten og foretak, særlig små og mellomstore bedrifter. I noen tilfeller er allerede disse opplysningene tilgjengelige via nettsteder på nasjonalt plan, på språket i en bestemt stat, og først og fremst om hendelser og tilfeller med en nasjonal dimensjon. Ettersom foretak i stadig større grad driver virksomhet på tvers av landegrensene og borgere bruker nettbaserte tjenester, bør opplysninger om hendelser finnes i aggregert form på unionsplan. CSIRT-nettverkets sekretariat oppfordres til å opprette et nettsted eller ha en særskilt side på et eksisterende nettsted der generelle opplysninger om større hendelser som har funnet sted i hele Unionen, gjøres tilgjengelig for allmennheten med særlig fokus på foretakenes interesser og behov. CSIRT-enheter som deltar i CSIRT-nettverket, oppfordres til frivillig å oppgi opplysningene som skal offentliggjøres på nettstedet, uten at de omfatter fortrolige eller følsomme opplysninger.

41) Dersom opplysninger anses som fortrolige i samsvar med Unionens og nasjonale regler for forretningshemmeligheter, bør denne fortroligheten ivaretas ved gjennomføring av virksomhet og oppfyllelse av mål i henhold til dette direktiv.

42) Øvelser som simulerer hendelsesscenarioer i sanntid, er avgjørende for å teste medlemsstatenes beredskap og samarbeid når det gjelder sikkerhet i nettverks- og informasjonssystemer. Øvelsesserien CyberEurope, som ENISA samordner med deltakelse fra medlemsstatene, er et nyttig verktøy for å teste og utarbeide anbefalinger om hvordan håndtering av hendelser på unionsplan bør forbedres over tid. Ettersom medlemsstatene for øyeblikket ikke er forpliktet til verken å planlegge eller delta i øvelser, bør opprettelsen av CSIRT-nettverket i henhold til dette direktiv gi medlemsstatene mulighet til å delta i øvelser på grunnlag av nøyaktig planlegging og strategiske valg. Samarbeidsgruppen som opprettes i henhold til dette direktiv, bør drøfte de strategiske beslutningene om øvelser, særlig, men ikke utelukkende med hensyn til hyppigheten av øvelsene og utformingen av scenarioene. ENISA bør i samsvar med sitt mandat støtte organiseringen og gjennomføringen av øvelser på unionsplan ved å bistå samarbeidsgruppen og CSIRT-nettverket med sakkunnskap og råd.

43) Tatt i betraktning at sikkerhetsproblemene som påvirker nettverks- og informasjonssystemer, har en global dimensjon, er det behov for tettere internasjonalt samarbeid for å forbedre sikkerhetsstandarder og utveksling av opplysninger, og for å fremme en felles global tilnærming til sikkerhetsspørsmål.

44) Ansvaret for å sikre sikkerheten i nettverks- og informasjonssystemer ligger i stor grad hos ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester. En kultur for risikohåndtering, som omfatter risikovurdering og gjennomføring av sikkerhetstiltak som står i forhold til risikoene, bør fremmes og utvikles gjennom passende lovgivningsmes-

---

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

sige krav og frivillige bransjeordninger. Å skape pålitelige like vilkår er også avgjørende for at samarbeidsgruppen og CSIRT-nettverket skal fungere effektivt, for å sikre effektivt samarbeid fra alle medlemsstater.

45) Dette direktiv får anvendelse bare på offentlige forvaltninger som er identifisert som ytere av samfunnsviktige tjenester. Det er derfor medlemsstatenes ansvar å sikre sikkerheten i nettverks- og informasjonssystemer hos offentlige forvaltninger som ikke omfattes av dette direktivs virkeområde.

46) Risikohåndteringstiltak omfatter tiltak for å identifisere eventuelle risikoer for hendelser med sikte på å forebygge, avdekke og håndtere hendelser og begrense deres virkninger. Sikkerheten i nettverks- og informasjonssystemer omfatter sikkerheten til lagrede, overførte og behandlede data.

47) Vedkommende myndigheter bør fortsatt ha mulighet til å vedta nasjonale retningslinjer om hvilke omstendigheter som forplikter ytere av samfunnsviktige tjenester til å melde hendelser.

48) Mange foretak i Unionen er avhengige av tilbydere av digitale tjenester for å levere tjenestene sine. Ettersom visse digitale tjenester kan være en viktig ressurs for brukerne, herunder ytere av samfunnsviktige tjenester, og disse brukerne ikke alltid har tilgjengelige alternativer, bør dette direktiv også få anvendelse på tilbydere av slike tjenester. Sikkerheten, kontinuiteten og påliteligheten til den typen digitale tjenester som er nevnt i dette direktiv, er for mange foretak avgjørende for å fungere godt. Et avbrudd i en slik digital tjeneste vil kunne hindre levering av andre tjenester som er avhengige av den, og dermed påvirke viktig økonomisk og samfunnsmessig virksomhet i Unionen. Slike digitale tjenester kan derfor være avgjørende for at foretak som er avhengige av dem, skal fungere godt, og særlig for disse foretakenes deltakelse i det indre marked og handel over landegrensene i hele Unionen. Tilbydere av digitale tjenester som omfattes av dette direktiv, er de tilbydere som anses å tilby digitale tjenester som mange foretak i Unionen i økende grad er avhengige av.

49) Tilbydere av digitale tjenester bør sikre et sikkerhetsnivå som står i forhold til graden av risiko forbundet med de digitale tjenestene de leverer, tatt i betraktning tjenestenes betydning for andre foretaks virksomhet i Unionen. Graden av risiko for ytere av samfunnsviktige tjenester, som ofte er avgjørende for å opprettholde viktig samfunnsmessig og økonomisk virksomhet, er i praksis høyere enn for tilbydere av digitale tjenester. Sikkerhetskravene til tilbydere av digitale tjenester bør derfor være mindre strenge. Tilbydere av digitale tjenester bør stå fritt til å treffe tiltak som de anser som hensiktsmessige for å håndtere risikoene knyttet til sikkerheten i sine nettverks- og informasjonssystemer. Tilbydere av digitale tjenester bør på grunn av sin tverrnasjonale karakter være underlagt en mer harmonisert tilnærming på unionsplan. Fastsettelsen og gjennomføringen av slike tiltak bør fremmes ved gjennomføringsrettsakter.

50) Selv om maskinvareprodusenter og programvareutviklere verken er ytere av samfunnsviktige tjenester eller tilbydere av digitale tjenester, øker produktene deres sikkerheten i nettverks- og informasjonssystemer. De spiller derfor en viktig rolle med hensyn til å gjøre ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester i stand til å sikre sine nettverks- og informasjonssystemer. Slike maskinvare- og programvareprodukter omfattes allerede av gjeldende regler om produktansvar.

51) Tekniske og organisatoriske tiltak som pålegges ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester, bør ikke forutsette at et bestemt kommersielt produkt innen informasjons- og kommunikasjonsteknologi utformes, utvikles eller produseres på en bestemt måte.

52) Ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester bør sikre sikkerheten i nettverks- og informasjonssystemene som de bruker. Dette er først og fremst private nettverks- og informasjonssystemer som ivaretas av internt IT-personell eller der sikkerhetsoppgavene er satt ut. Sikkerhets- og meldingskravene bør få anvendelse på berørte ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester, uansett om de utfører vedlikehold av nettverks- og informasjonssystemene sine internt eller setter det ut.

53) For å unngå en uforholdsmessig stor økonomisk og administrativ byrde for ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester bør kravene stå i forhold til risikoen som det berørte nettverks- og informasjonssystemet utgjør, idet det tas hensyn til nåværende utviklingstrinn i teknikken for slike tiltak. Når det gjelder tilbydere av digitale tjenester bør disse kravene ikke få anvendelse på svært små og små bedrifter.

54) Når offentlige forvaltninger i medlemsstatene bruker tjenester som tilbys av tilbydere av digitale tjenester, særlig skytjenester, vil de kanskje kreve at tilbydere av slike tjenester sørger for ytterligere sikkerhetstiltak utover de som tilbydere av digitale tjenester normalt ville tilby i samsvar med kravene i dette direktiv. De bør kunne gjøre dette ved hjelp av avtaleforpliktelser.

55) Definisjonene av nettbaserte markedsplasser, nettbaserte søkemotorer og skytjenester i dette direktiv er spesifikke for dette direktiv og berører ikke andre dokumenter.

56) Dette direktiv bør ikke hindre medlemsstatene i å vedta nasjonale tiltak som krever at offentlige organer fastsetter særskilte sikkerhetskrav når de inngår avtaler om skytjenester. Slike nasjonale tiltak bør få anvendelse på det berørte offentlige organet og ikke på tilbyderen av skytjenester.

57) Tatt i betraktning de grunnleggende forskjellene mellom ytere av samfunnsviktige tjenester, særlig deres direkte forbindelse med fysisk infrastruktur, og tilbydere av digitale tjenester, særlig deres grensekryssende karakter, bør dette direktiv differensieres med hensyn til harmonisering når det gjelder disse to gruppene av foretak. For ytere av samfunnsviktige tjenester bør medlemsstatene kunne identifisere de relevante aktørene og innføre strengere krav enn dem som er fastsatt i dette direktiv. Medlemsstatene bør ikke identifisere tilbydere av digitale tjenester, ettersom dette direktiv bør få anvendelse på alle tilbydere av digitale tjenester som omfattes av dette direktivs virkeområde. I tillegg bør dette direktiv og gjennomføringsrettsaktene som vedtas i henhold til det, sikre et høyt nivå av harmonisering for tilbydere av digitale tjenester med hensyn til sikkerhets- og meldingskrav. Dette bør gjøre det mulig å behandle tilbydere av digitale tjenester på en ensartet måte i hele Unionen, på en måte som står i forhold til deres karakter og graden av risiko de kan stå overfor.

58) Dette direktiv bør ikke være til hinder for at medlemsstatene innfører sikkerhets- og meldingskrav for foretak som ikke er tilbydere av digitale tjenester innenfor dette direktivs virkeområde, uten at dette berører medlemsstatenes forpliktelser i henhold til unionsretten.

59) Vedkommende myndigheter bør ta behørig hensyn til nødvendigheten av å bevare uformelle og pålitelige kanaler for utveksling av opplysninger. Ved offentliggjøring av hendelser som rapporteres til vedkommende myndigheter, bør allmennhetens interesse av å bli informert om trusler veies behørig opp mot mulige negative konsekvenser for omdømmet og økonomien til de ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester som rapporterer hendelser. Ved gjennomføringen av meldingsplikten bør vedkommende myndigheter og CSIRT-enhetene rette særlig oppmerksomhet mot behovet for å holde opplysninger om produkters sårbarhet strengt fortrolige inntil det sendes ut egnede sikkerhetsoppdateringer.

60) Tilbydere av digitale tjenester bør omfattes av et mindre omfattende og reaktivt tilsyn i ettertid som er tilpasset deres type tjenester og virksomhet. Den berørte vedkommende myndighet bør derfor bare treffe tiltak når den har mottatt dokumentasjon, for eksempel fra tilbyderen av digitale tjenester selv, fra en annen vedkommende myndighet, herunder en vedkommende myndighet i en annen medlemsstat, eller av en bruker av tjenesten, på at en tilbyder av digitale tjenester ikke oppfyller kravene i dette direktiv, særlig etter en hendelse. Den vedkommende myndigheten bør derfor ikke ha en generell plikt til å føre tilsyn med tilbydere av digitale tjenester.

61) Vedkommende myndigheter bør ha de nødvendige midler til å utføre sine oppgaver, herunder myndighet til å innhente tilstrekkelige opplysninger for å vurdere graden av sikkerhet i nettverks- og informasjonssystemer.

62) Hendelser kan oppstå som følge av kriminell virksomhet, og forebygging, etterforskning og rettsforfølging av dette støttes av samordning og samarbeid mellom ytere av samfunnsviktige tjenester, tilbydere av digitale tjenester, vedkommende myndigheter og myndigheter med ansvar for håndheving av loven. Dersom det er mistanke om at en hendelse er knyttet til alvorlig kriminell virksomhet i henhold til unionsretten eller nasjonal lovgivning, bør medlemsstatene oppmuntre ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester til å rapportere hendelser av antatt alvorlig strafferettslig art til de relevante myndigheter med ansvar for håndheving av loven. Dersom det er relevant, er det ønskelig at samordningen mellom forskjellige medlemsstaters vedkommende myndigheter og myndigheter med ansvar for håndheving av loven gjøres lettere av Det europeiske senter for bekjempelse av datakriminalitet (EC3) og ENISA.

63) Personopplysninger settes i mange tilfeller i fare som følge av hendelser. I den forbindelse bør vedkommende myndigheter og personvernmyndigheter samarbeide og utveksle opplysninger om alle relevante forhold for å håndtere eventuelle brudd på personopplysningssikkerheten som følge av hendelser.

64) Jurisdiksjon med hensyn til tilbydere av digital tjenester bør tilskrives den medlemsstaten der den berørte tilbyderen av digitale tjenester har sitt hovedforetak i Unionen, som i prinsippet svarer til det sted der tilbyderen har sitt hovedkontor i Unionen. En virksomhet innebærer en effektiv og faktisk utøvelse av aktivitet gjennom en stabil struktur. En slik strukturs juridiske form, enten det dreier seg om en filial eller et datterforetak med status som juridisk person, er ikke av avgjørende betydning i den forbindelse. Dette kriteriet bør ikke være avhengig av om nettverks- og informasjonssystemer fysisk befinner seg på et bestemt sted; forekomst og bruk av slike systemer utgjør ikke i seg selv et slikt hovedforetak og er derfor ikke kriterier for å fastsette hovedforetaket.

65) En tilbyder av digital tjenester som ikke er etablert i Unionen, og som tilbyr tjenester i Unionen, bør utpeke en representant. For å avgjøre om en slik tilbyder av digitale tjenester tilbyr tjenester i Unionen, bør det fastslås om det er åpenbart at tilbyderen av digitale tjenester planlegger å tilby tjenester til personer i én eller flere medlemsstater. Det forhold alene at et nettsted tilhørende tilbyderen av digitale tjenester eller en formidler, eller en e-postadresse og andre kontaktopplysninger, er tilgjengelige i Unionen, eller at det brukes et språk som vanligvis brukes i tredjestaten der tilbyderen av digitale tjenester er etablert, er ikke tilstrekkelig til å fastslå en slik hensikt. Imidlertid kan forhold som for eksempel bruk av et språk eller en valuta som vanligvis brukes i én eller flere medlemsstater med mulighet til å bestille tjenester på det aktuelle språket, eller omtale av kunder eller brukere i Unionen, gjøre det klart at tilbyderen av digitale tjenester planlegger å tilby tjenester innenfor Unionen. Representanten bør handle på vegne av tilbyderen av digitale tjenester, og det bør være mulig for vedkommende myndigheter eller CSIRT-enhetene å kontakte representanten. Representanten bør utpekes uttrykkelig gjennom skriftlig fullmakt fra tilbyderen av digitale tjenester til å opptre på dennes vegne med hensyn til sistnevntes forpliktelser i henhold til dette direktiv, herunder rapportering av hendelser.

66) Standardisering av sikkerhetskrav er en markedsdrevet prosess. For å sikre en ensartet anvendelse av sikkerhetsstandarder bør medlemsstatene oppmuntre til overholdelse av eller samsvar med angitte standarder for å sikre et høyt nivå av sikkerhet i nettverks- og informasjonssystemer på unionsplan. ENISA bør bistå medlemsstatene med råd og retningslinjer. Det kan derfor være nyttig å utarbeide utkast til harmoniserte standarder, og dette bør gjøres i samsvar med europaparlaments- og rådsforordning (EU) nr. 1025/2012[8].

67) Foretak som faller utenfor dette direktivs virkeområde, kan oppleve hendelser som virker betydelig inn på de tjenestene de tilbyr. Dersom disse foretakene mener det er i offentlighetens interesse å melde forekomsten av slike hendelser, bør de kunne gjøre dette på frivillig grunnlag. Disse meldingene bør behandles av vedkommende myndighet eller CSIRT-enheten når slik behandling ikke utgjør en uforholdsmessig stor eller urimelig byrde for de berørte medlemsstatene.

68) For å sikre ensartede vilkår for gjennomføringen av dette direktiv bør Kommisjonen gis gjennomføringsmyndighet til å fastsette de saksbehandlingsregler som er nødvendige for samarbeidsgruppens virksomhet, og de sikkerhets- og meldingskrav som skal gjelde for tilbydere av digitale tjenester. Denne myndighet bør utøves i samsvar med europaparlaments- og rådsforordning (EU) nr. 182/2011[9]. Når den vedtar gjennomføringsrettsakter om de saksbehandlingsregler som er nødvendige for samarbeidsgruppens virksomhet, bør Kommisjonen ta størst mulig hensyn til uttalelsen fra ENISA.

69) Når den vedtar gjennomføringsrettsakter om sikkerhetskravene til tilbydere av digitale tjenester, bør Kommisjonen ta størst mulig hen-

---

[8] 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).

[9] 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).

syn til uttalelsen fra ENISA og rådføre seg med berørte parter. I tillegg oppfordres Kommisjonen til å ta hensyn til følgende eksempler: når det gjelder sikkerhet for systemer og anlegg: fysisk sikkerhet og miljøsikkerhet, forsyningssikkerhet, kontroll av tilgang til nettverks- og informasjonssystemer og integriteten til nettverks- og informasjonssystemer; når det gjelder håndtering av hendelser: prosedyrer for hendelseshåndtering, kapasitet til å påvise hendelser, hendelsesrapportering og kommunikasjon; når det gjelder styring av driftskontinuitet: strategi for opprettholdelse av tjenester samt beredskapsplaner, kapasitet til gjenoppretting etter katastrofer; og når det gjelder overvåking, revisjon og testing: strategier for overvåking og loggføring, planer for beredskapsøvelser, testing av nettverks- og informasjonstjenester, sikkerhetsvurderinger og overvåking av samsvar.

70) Ved gjennomføringen av dette direktiv bør Kommisjonen samarbeide etter behov med relevante sektorkomiteer og relevante organer som er opprettet på unionsplan på de områdene som omfattes av dette direktiv.

71) Kommisjonen bør med jevne mellomrom ta dette direktiv opp til ny vurdering i samråd med berørte parter, særlig for å bestemme om det er nødvendig å endre det for å ta hensyn til samfunnsutviklingen, den politiske utvikling, den teknologiske utviklingen eller markedssituasjonen.

72) Utveksling av opplysninger om risikoer og hendelser innenfor samarbeidsgruppen og nettverket av CSIRT-enheter og overholdelse av kravet om å melde hendelser til vedkommende nasjonale myndigheter eller CSIRT-enhetene, kan kreve behandling av personopplysninger. En slik behandling bør være i samsvar med europaparlaments- og rådsdirektiv 95/46/EF[10] og europaparlaments- og rådsforordning (EF) nr. 45/2001[11]. Ved anvendelsen av dette direktiv bør europaparlaments- og rådsforordning (EF) nr. 1049/2001[12] få anvendelse i nødvendig omfang.

73) EUs datatilsyn er blitt rådspurt i samsvar med artikkel 28 nr. 2 i forordning (EF) nr. 45/2001 og avga uttalelse 14. juni 2013[13].

74) Ettersom målet for dette direktiv, som er å oppnå et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i hele Unionen, ikke kan nås i tilstrekkelig grad av medlemsstatene og derfor på grunn av tiltakets virkninger bedre kan nås på unionsplan, kan Unionen treffe tiltak i samsvar med nærhetsprinsippet som fastsatt i traktatens artikkel 5. I samsvar med forholdsmessighetsprinsippet fastsatt i nevnte artikkel, går dette direktiv ikke lenger enn det som er nødvendig for å nå dette målet.

75) Dette direktiv er forenlig med de grunnleggende rettighetene og de prinsippene som er anerkjent i Den europeiske unions pakt om grunnleggende rettigheter, særlig respekt for privatliv og kommunikasjon, vern av personopplysninger, adgang til å utøve virksomhet, eiendomsretten, retten til effektiv klageadgang for en domstol og retten til å bli hørt. Dette direktiv bør gjennomføres i samsvar med nevnte rettigheter og prinsipper –

VEDTATT DETTE DIREKTIV:

Kapittel I

Alminnelige bestemmelser

Artikkel 1

Formål og virkeområde

1. I dette direktiv fastsettes tiltak med sikte på å oppnå et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i Unionen for å forbedre virkemåten til det indre marked.
2. I den forbindelse blir det i dette direktiv
   a) fastsatt at alle medlemsstater er forpliktet til å vedta en nasjonal strategi for sikkerhet i nettverks- og informasjonssystemer,
   b) opprettet en samarbeidsgruppe med henblikk på å støtte og fremme strategisk samarbeid og utveksling av opplysninger mellom medlemsstatene og skape tiltro og tillit blant dem,
   c) opprettet et nettverk av enheter for håndtering av digitale hendelser («CSIRT-nett-

[10] Europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (EFT L 281 av 23.11.1995, s. 31).

[11] Europaparlaments- og rådsforordning (EF) nr. 45/2001 av 18. desember 2000 om personvern i forbindelse med behandling av personopplysninger i Fellesskapets institusjoner og organer og om fri utveksling av slike opplysninger (EFT L 8 av 8.12.2001, s. 1).

[12] 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).

[13] EUT C 32 av 4.2.2014, s. 19.

verk») for å bidra til å skape tiltro og tillit blant medlemsstatene og for å fremme et raskt og effektivt driftsmessig samarbeid,
   d) fastsatt sikkerhets- og meldingskrav til ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester,
   e) fastsatt at medlemsstatene må utpeke vedkommende nasjonale myndigheter, felles kontaktpunkter og CSIRT-enheter som pålegges oppgaver knyttet til sikkerhet i nettverks- og informasjonssystemer.
3. Sikkerhets- og meldingskravene fastsatt i dette direktiv får ikke anvendelse på foretak som omfattes av kravene i artikkel 13a og 13b i direktiv 2002/21/EF, eller på ytere av tillitstjenester som omfattes av kravene i artikkel 19 i forordning (EU) nr. 910/2014.
4. Dette direktiv får anvendelse uten at det berører rådsdirektiv 2008/114/EF[14] og europaparlaments- og rådsdirektiv 2011/93/EU[15] og 2013/40/EU[16].
5. Uten at det berører artikkel 346 i TEUV skal opplysninger som er fortrolige i henhold til Unionens og nasjonale regler, som for eksempel regler for forretningshemmeligheter, utveksles med Kommisjonen og andre relevante myndigheter bare dersom utvekslingen er nødvendig for anvendelsen av dette direktiv. Utvekslingen skal begrense seg til opplysninger som er relevante og står i forhold til formålet. Slik utveksling av opplysninger skal sikre at opplysningene behandles fortrolig og beskytte sikkerhets- og forretningsinteressene til ytere av samfunnsviktige tjenester og tilbydere av digitale tjenester.
6. Dette direktiv berører ikke tiltak som medlemsstatene treffer for å ivareta sine grunnleggende statsfunksjoner, særlig for å ivareta nasjonal sikkerhet, herunder tiltak for å verne opplysninger hvis offentliggjøring medlemsstatene anser å stride mot deres vesentlige sikkerhetsinteresser, og for å opprettholde lov og orden, særlig for å muliggjøre etterforskning, avsløring og rettslig forfølging av straffbare handlinger.
7. Dersom en sektorspesifikk unionsrettsakt krever at ytere av samfunnsviktige tjenester eller tilbydere av digitale tjenester enten skal sikre sikkerheten i sine nettverks- og informasjonssystemer eller melde hendelser, forutsatt at slike krav i praksis minst tilsvarer forpliktelsene fastsatt i dette direktiv, skal bestemmelsene i den sektorspesifikke unionsrettsakten få anvendelse.

Artikkel 2

Behandling av personopplysninger

1. Personopplysninger som behandles i henhold til dette direktiv, skal behandles i samsvar med direktiv 95/46/EF.
2. Personopplysninger som behandles av Unionens institusjoner og organer i henhold til dette direktiv, skal behandles i samsvar med forordning (EF) nr. 45/2001.

Artikkel 3

Minsteharmonisering

Uten at det berører artikkel 16 nr. 10 og deres forpliktelser i henhold til unionsretten kan medlemsstatene vedta eller opprettholde bestemmelser med sikte på å oppnå et høyere nivå for sikkerhet i nettverks- og informasjonssystemer.

Artikkel 4

Definisjoner

I dette direktiv menes med:
1) «nettverks- og informasjonssystem»
   a) et elektronisk kommunikasjonsnett i henhold i artikkel 2 bokstav a) i direktiv 2002/21/EF,
   b) en innretning eller gruppe av innbyrdes forbundne eller tilknyttede innretninger, hvorav én eller flere av dem ved hjelp av et program utfører automatisk behandling av digitale data, eller
   c) digitale data som lagres, behandles, innhentes eller overføres med elementene som omfattes av bokstav a) og b) i forbindelse med drift, bruk, vern og vedlikehold,
2) «sikkerhet i nettverks- og informasjonssystemer» den evnen nettverk eller informasjonssystemer har til å tåle, på et gitt tillitsnivå, enhver handling som går ut over tilgjengeligheten, autentisiteten, integriteten eller tilliten

---

[14] Rådsdirektiv 2008/114/EF av 8. desember 2008 om identifisering og utpeking av europeisk kritisk infrastruktur og vurdering av behovet for å beskytte den bedre (EUT L 345 av 23.12.2008, s. 75).

[15] Europaparlaments- og rådsdirektiv 2011/93/EU av 13. desember 2011 om bekjempelse av seksuelt misbruk og seksuell utnytting av barn og barnepornografi, og om erstatning av Rådets rammebeslutning 2004/68/JIS (EUT L 335 av 17.12.2011, s. 1).

[16] Europaparlaments- og rådsdirektiv 2013/40/EU av 12. august 2013 om angrep på informasjonssystemer, og om erstatning av Rådets rammebeslutning 2005/222/JIS (EUT L 218 av 14.8.2013, s. 8).

til lagrede eller overførte eller behandlede data eller tilknyttede tjenester som tilbys eller er tilgjengelige via slike nettverks- og informasjonssystemer,

3) «nasjonal strategi for sikkerhet i nettverks- og informasjonssystemer» en ramme med strategiske mål og prioriteringer for sikkerhet i nettverks- og informasjonssystemer på nasjonalt plan,
4) «yter av samfunnsviktige tjenester» et offentlig eller privat foretak av en type som er nevnt i vedlegg II, og som oppfyller kriteriene fastsatt i artikkel 5 nr. 2,
5) «digital tjeneste» en tjeneste som definert i artikkel 1 nr. 1 bokstav b) i europaparlaments- og rådsdirektiv (EU) 2015/1535[17] og av en type oppført i vedlegg III,
6) «tilbyder av digitale tjenester» enhver juridisk person som leverer en digital tjeneste,
7) «hendelse» enhver hendelse som har en reell negativ virkning på sikkerheten i nettverks- og informasjonssystemer,
8) «hendelseshåndtering» alle prosedyrer som støtter påvisning, analyse og begrensning av en hendelse samt all tilknyttet innsats,
9) «risiko» enhver rimelig identifiserbar omstendighet eller hendelse med en mulig negativ virkning på sikkerheten i nettverks- og informasjonssystemer,
10) «representant» enhver fysisk eller juridisk person etablert i Unionen som er uttrykkelig utpekt til å handle på vegne av en tilbyder av digitale tjenester som ikke er etablert i Unionen, som vedkommende nasjonale myndighet eller en CSIRT-enhet eventuelt kan henvende seg til i stedet for tilbyderen av digitale tjenester med hensyn til forpliktelsene som tilbyderen av digitale tjenester har i henhold til dette direktiv,
11) «standard» en standard som definert i artikkel 2 nr. 1 i forordning (EU) nr. 1025/2012,
12) «spesifikasjon» en teknisk spesifikasjon som definert i artikkel 2 nr. 4 i forordning (EU) nr. 1025/2012,
13) «samtrafikkpunkt på Internett (IXP)» en nettstruktur som muliggjør sammenkopling av mer enn to uavhengige og selvstendige systemer, først og fremst for å legge til rette for samtrafikk på Internett; et IXP sørger for sammenkopling bare for selvstendige systemer; et IXP krever ikke at internettrafikk som passerer mellom to deltakende selvstendige systemer, passerer gjennom et tredje selvstendig system, og det verken endrer eller griper forstyrrende inn i slik trafikk,
14) «domenenavnsystem (DNS)» et hierarkisk oppbygget navngivingssystem i et nettverk som håndterer forespørsler om domenenavn,
15) «tilbyder av DNS-tjenester» et foretak som leverer DNS-tjenester på Internett,
16) «registerenhet for toppdomener» et foretak som forvalter og driver registrering av domenenavn på Internett under et bestemt toppdomene (TLD),
17) «nettbasert markedsplass» en digital tjeneste som gjør det mulig for forbrukere og/eller næringsdrivende som definert i henholdsvis bokstav a) og b) i artikkel 4 nr. 1 i europaparlaments- og rådsdirektiv 2013/11/EU[18], å inngå nettbaserte salgs- eller tjenesteavtaler med næringsdrivende enten på nettstedet til den nettbaserte markedsplassen eller på en næringsdrivendes nettsted som bruker datatjenester som leveres av den nettbaserte markedsplassen,
18) «nettbasert søkemotor» et digital tjeneste som gjør det mulig for brukere å foreta søk på i prinsippet alle nettsteder eller nettsteder på et bestemt språk, på grunnlag av en forespørsel om et hvilket som helst emne i form av et nøkkelord, en setning eller andre inndata, og som viser lenker hvor det er mulig å finne informasjon om det forespurte innholdet,
19) «skytjeneste» en digital tjeneste som gir tilgang til en skalerbar og fleksibel samling av delbare databehandlingsressurser.

Artikkel 5

Identifikasjon av ytere av samfunnsviktige tjenester

1. Innen 9. november 2018 skal medlemsstatene for hver sektor og delsektor som er nevnt i vedlegg II, identifisere de ytere av samfunnsviktige tjenester som er etablert på deres territorium.
2. Kriteriene for identifisering av ytere av samfunnsviktige tjenester i henhold til artikkel 4 nr. 4 skal være som følger:

[17] 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).

[18] Europaparlaments- og rådsdirektiv 2013/11/EU av 21. mai 2013 om alternativ tvisteløsning i forbrukersaker og om endring av forordning (EF) nr. 2006/2004 og direktiv 2009/22/EF (ATF-direktivet) (EUT L 165 av 18.6.2013, s. 63).

a) Et foretak yter en tjeneste som er grunnleggende for å opprettholde viktig samfunnsmessig og/eller økonomisk virksomhet.
b) Ytingen av tjenesten avhenger av nettverks- og informasjonssystemer.
c) En hendelse vil få en betydelig forstyrrende virkning på ytingen av tjenesten.

3. Med henblikk på nr. 1 skal hver medlemsstat utarbeide en liste over tjenestene nevnt i nr. 2 bokstav a).
4. Med henblikk på nr. 1, dersom et foretak yter en tjeneste nevnt i nr. 2 bokstav a) i to eller flere medlemsstater, skal disse medlemsstatene delta i samråd med hverandre. Samrådet skal finne sted før det tas en beslutning om identifikasjon.
5. Medlemsstatene skal regelmessig og minst hvert annet år etter 9. mai 2018 gjennomgå og eventuelt ajourføre listen over identifiserte ytere av samfunnsviktige tjenester.
6. Rollen til samarbeidsgruppen skal i samsvar med oppgavene nevnt i artikkel 11 være å hjelpe medlemsstatene med å være konsekvente i arbeidet med å identifisere ytere av samfunnsviktige tjenester.
7. Med henblikk på gjennomgåelsen nevnt i artikkel 23 skal medlemsstatene innen 9. november 2018 og deretter hvert annet år framlegge for Kommisjonen de opplysninger som er nødvendige for å vurdere gjennomføringen av dette direktiv, særlig ensartetheten i medlemsstatenes metoder for å identifisere ytere av samfunnsviktige tjenester. Opplysningene skal minst omfatte følgende:
   a) nasjonale tiltak som gjør det mulig å identifisere ytere av samfunnsviktige tjenester,
   b) listen over tjenester nevnt i nr. 3,
   c) antall ytere av samfunnsviktige tjenester som er identifisert for hver sektor som er nevnt i vedlegg II, med angivelse av deres betydning i forhold til denne sektoren,
   d) terskelverdier, dersom slike finnes, for å bestemme det relevante forsyningsnivået i forhold til antall brukere som er avhengig av tjenesten som nevnt i artikkel 6 nr. 1 bokstav a), eller i forhold til betydningen av denne yteren av samfunnsviktige tjenester som nevnt i artikkel 6 nr. 1 bokstav f).

   For å bidra til at det foreligger sammenlignbare opplysninger, kan Kommisjonen, idet det tas størst mulig hensyn til uttalelsen fra ENISA, vedta egnede tekniske retningslinjer for parametrene for de opplysninger som er nevnt i dette nummer.

Artikkel 6

Betydelig forstyrrende virkning

1. Når medlemsstatene skal fastsette betydningen av en forstyrrende virkning som nevnt i artikkel 5 nr. 2 bokstav c), skal de ta hensyn til minst følgende tverrsektorielle forhold:
   a) antall brukere som er avhengige av tjenesten som ytes av det berørte foretaket,
   b) avhengigheten til andre sektorer nevnt i vedlegg II av tjenesten som ytes av foretaket,
   c) virkningen som hendelser vil kunne ha med hensyn til omfang og varighet på økonomisk og samfunnsmessig virksomhet eller offentlig sikkerhet,
   d) foretakets markedsandel,
   e) størrelsen på det geografiske området som vil kunne bli berørt av en hendelse,
   f) foretakets betydning for å opprettholde et tilstrekkelig tjenestenivå, idet det tas hensyn til tilgjengeligheten av alternative metoder for å yte tjenesten.
2. For å avgjøre om en hendelse vil kunne ha en betydelig forstyrrende virkning skal medlemsstatene også, når det er hensiktsmessig, ta hensyn til sektorspesifikke forhold.

Kapittel II

Nasjonale rammer for sikkerhet i nett- og informasjonssystemer

Artikkel 7

Nasjonal strategi for sikkerhet i nettverks- og informasjonssystemer

1. Hver medlemsstat skal vedta en nasjonal strategi for sikkerhet i nettverks- og informasjonssystemer som definerer strategiske mål og en egnet politikk og egnede lovgivningsmessige tiltak med henblikk på å oppnå og opprettholde et høyt nivå av sikkerhet i nettverks- og informasjonssystemer, og som minst omfatter sektorene nevnt i vedlegg II og tjenestene nevnt i vedlegg III. Den nasjonale strategien for sikkerhet i nettverks- og informasjonssystemer skal særlig omhandle følgende:
   a) målene og prioriteringene i den nasjonal strategien for sikkerhet i nettverks- og informasjonssystemer,
   b) en forvaltningsramme for å nå målene for og prioriteringene i den nasjonale strategien for sikkerhet i nettverks- og informasjonssystemer, herunder offentlige orga-

ners og andre relevante aktørers roller og ansvarsområder,

c) en liste over tiltak knyttet til beredskap, innsats og gjenoppretting, herunder samarbeid mellom offentlig og privat sektor,
d) en angivelse av utdanningsprogrammer, holdningsskapende tiltak og opplæringsprogrammer forbundet med den nasjonale strategien for sikkerhet i nettverks- og informasjonssystemer,
e) en angivelse av forsknings- og utviklingsplaner forbundet med den nasjonale strategien for sikkerhet i nettverks- og informasjonssystemer,
f) en risikovurderingsplan for å identifisere eventuelle risikoer,
g) en liste over de ulike aktørene som deltar i gjennomføringen av den nasjonale strategien for sikkerhet i nettverks- og informasjonssystemer.

2. Medlemsstatene kan be om bistand fra ENISA for å utvikle nasjonale strategier for sikkerhet i nettverks- og informasjonssystemer.
3. Medlemsstatene skal underrette Kommisjonen om sine nasjonale strategier for sikkerhet nettverks- og informasjonssystemer innen tre måneder etter at de er vedtatt. I den forbindelse kan medlemsstatene utelukke elementer i strategien som gjelder nasjonal sikkerhet.

Artikkel 8

Vedkommende nasjonale myndigheter og et felles kontaktpunkt

1. Hver medlemsstat skal utpeke én eller flere vedkommende nasjonale myndigheter for sikkerhet i nettverks- og informasjonssystemer («vedkommende myndighet»), som minst omfatter sektorene nevnt i vedlegg II og tjenestene nevnt i vedlegg III. Medlemsstatene kan overlate denne rollen til én eller flere eksisterende myndigheter.
2. Vedkommende myndigheter skal overvåke anvendelsen av dette direktiv på nasjonalt plan.
3. Hver medlemsstat skal utpeke et nasjonalt felles kontaktpunkt for sikkerhet i nettverks- og informasjonssystemer («felles kontaktpunkt»). Medlemsstatene kan overlate denne rollen til en eksisterende myndighet. Dersom en medlemsstat utpeker bare én vedkommende myndighet, skal denne vedkommende myndigheten også være det felles kontaktpunktet.
4. Det felles kontaktpunktet skal fungere som et mellomledd for å sikre samarbeidet over landegrensene mellom medlemsstatenes myndigheter og relevante myndigheter i andre medlemsstater og med samarbeidsgruppen nevnt i artikkel 11 og CSIRT-nettverket omhandlet i artikkel 12.
5. Medlemsstatene skal sikre at vedkommende myndigheter og de felles kontaktpunktene har tilstrekkelige ressurser til å kunne utføre effektivt og formålstjenlig oppgavene de blir pålagt og dermed nå målene i dette direktiv. Medlemsstatene skal sikre at de utpekte representantene i samarbeidsgruppen samarbeider på en effektiv, formålstjenlig og sikker måte.
6. Vedkommende myndigheter og det felles kontaktpunktet skal, når det er hensiktsmessig og i samsvar med nasjonal lovgivning, rådføre seg og samarbeide med den relevante nasjonale myndighet med ansvar for håndheving av loven og med nasjonale personvernmyndigheter.
7. Hver medlemsstat skal uten opphold underrette Kommisjonen om utpekingen av vedkommende myndighet og det felles kontaktpunktet, deres oppgaver og eventuelle senere endringer av dem. Hver medlemsstat skal offentliggjøre utpekingen av vedkommende myndighet og det felles kontaktpunktet. Kommisjonen skal offentliggjøre listen over utpekte felles kontaktpunkter.

Artikkel 9

Enheter for håndtering av digitale hendelser (CSIRT-enheter)

1. Hver medlemsstat skal utpeke en eller flere CSIRT-enheter som skal oppfylle kravene i nr. 1 i vedlegg I, som minst omfatter sektorene nevnt i vedlegg II og tjenestene nevnt i vedlegg III, og som har ansvar for å håndtere risikoer og hendelser i samsvar med en klart definert prosess. En CSIRT-enhet kan opprettes som en del av en vedkommende myndighet.
2. Medlemsstatene skal sikre at CSIRT-enheter har tilstrekkelige ressurser til å kunne utføre sine oppgaver effektivt som fastsatt i nr. 2 i vedlegg I.

   Medlemsstatene skal sikre et effektivt, formålstjenlig og sikkert samarbeid mellom deres CSIRT-enheter og CSIRT-nettverket nevnt i artikkel 12.
3. Medlemsstatene skal sikre at deres CSIRT-enheter har tilgang til en egnet, sikker og

robust kommunikasjons- og informasjonsinfrastruktur på nasjonalt plan.

4. Medlemsstatene skal underrette Kommisjonen om CSIRT-enhetenes oppgaver samt de viktigste elementene i CSIRT-enhetenes prosedyrer for hendelseshåndtering.
5. Medlemsstatene kan be om bistand fra ENISA til å opprette nasjonale CSIRT-enheter.

Artikkel 10

Samarbeid på nasjonalt plan

1. Dersom vedkommende myndighet, det felles kontaktpunktet og CSIRT-enheten i en medlemsstat er atskilte enheter, skal de samarbeide med hensyn til oppfyllelsen av forpliktelsene fastsatt i dette direktiv.
2. Medlemsstatene skal sikre at enten vedkommende myndigheter eller CSIRT-enhetene mottar meldinger om hendelser som inngis i henhold til dette direktiv. Dersom en medlemsstat beslutter at CSIRT-enheter ikke skal motta meldinger, skal CSIRT-enhetene, i den grad det er nødvendig for at de skal kunne utføre sine oppgaver, gis tilgang til opplysninger om hendelser som meldes av ytere av samfunnsviktige tjenester i henhold til artikkel 14 nr. 3 og 5, eller av tilbydere av digitale tjenester i henhold til artikkel 16 nr. 3 og 6.
3. Medlemsstatene skal sikre at vedkommende myndigheter eller CSIRT-enhetene underretter de felles kontaktpunktene om meldinger om hendelser som inngis i henhold til dette direktiv.

   Innen 9. august 2018, og deretter hvert år, skal det felles kontaktpunktet framlegge en sammenfattende rapport for samarbeidsgruppen om de mottatte meldingene, herunder antall meldinger og arten av meldte hendelser, og de tiltak som er truffet i samsvar med artikkel 14 nr. 3 og 5 og artikkel 16 nr. 3 og 6.

Kapittel III

Samarbeid

Artikkel 11

Samarbeidsgruppe

1. For å støtte og fremme strategisk samarbeid og utveksling av opplysninger mellom medlemsstatene og skape tiltro og tillit, og med sikte på å oppnå et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i Unionen, opprettes det herved en samarbeidsgruppe.

   Samarbeidsgruppen skal utføre sine oppgaver på grunnlag av toårig arbeidsprogrammer som nevnt i nr. 3 annet ledd.
2. Samarbeidsgruppen skal bestå av representanter for medlemsstatene, Kommisjonen og ENISA.

   Når det er relevant kan samarbeidsgruppen innby representanter for berørte parter til å delta i dens arbeid.

   Kommisjonen skal ivareta sekretariatet.
3. Samarbeidsgruppen skal ha følgende oppgaver:
   a) gi strategisk veiledning om virksomheten til CSIRT-nettverket opprettet i henhold til artikkel 12,
   b) utveksle beste praksis for utveksling av opplysninger om melding av hendelser som nevnt i artikkel 14 nr. 3 og 5 og artikkel 16 nr. 3 og 6,
   c) utveksle beste praksis mellom medlemsstatene og, i samarbeid med ENISA, bistå medlemsstatene i å bygge opp kapasitet for å sikre sikkerheten i nettverks- og informasjonssystemer,
   d) drøfte ressurser og beredskap i medlemsstatene og, på frivillig grunnlag, evaluere nasjonale strategier for sikkerhet i nettverks- og informasjonssystemer og effektiviteten til CSIRT-enheter, samt identifisere beste praksis,
   e) utveksle opplysninger og beste praksis med hensyn til holdningsskapende tiltak og opplæring,
   f) utveksle opplysninger og beste praksis med hensyn til forskning og utvikling knyttet til sikkerhet i nettverks- og informasjonssystemer,
   g) når det er relevant, utveksle erfaringer vedrørende spørsmål om sikkerheten i nettverks- og informasjonssystemer med Unionens berørte institusjoner, organer, kontorer og byråer,
   h) drøfte standardene og spesifikasjonene nevnt i artikkel 19, med representanter for relevante europeiske standardiseringsorganisasjoner,
   i) samle inn opplysninger om beste praksis i forbindelse med risikoer og hendelser,
   j) undersøke, på årsbasis, de sammenfattende rapportene nevnt i artikkel 10 nr. 3 annet ledd,
   k) drøfte arbeidet som er gjort med hensyn til øvelser i forbindelse med sikkerhet i nettverks- og informasjonssystemer, utdanningsprogrammer og opplæring, herunder arbeid utført av ENISA,

l) med ENISAs bistand utveksle beste praksis med hensyn til medlemsstatenes identifikasjon av ytere av samfunnsviktige tjenester, herunder i forbindelse med gjensidig avhengighet over landegrensene, vedrørende risikoer og hendelser,

m) drøfte metoder for rapportering av meldte hendelser som nevnt i artikkel 14 og 16.

Innen 9. februar 2018 og deretter hvert annet år skal samarbeidsgruppen utarbeide et arbeidsprogram med hensyn til tiltak som skal treffes for å gjennomføre dens mål og oppgaver, som skal være i samsvar med målene i dette direktiv.

4. Med henblikk på gjennomgåelsen nevnt i artikkel 23 skal samarbeidsgruppen innen 9. august 2018, og deretter hvert halvannet år, utarbeide en rapport om de erfaringer som er gjort med det strategiske samarbeidet i henhold til denne artikkel.
5. Kommisjonen skal vedta gjennomføringsrettsakter som fastsetter de saksbehandlingsregler som er nødvendige for samarbeidsgruppens virksomhet. Disse gjennomføringsrettsaktene skal vedtas etter framgangsmåten med undersøkelseskomité nevnt i artikkel 22 nr. 2.

I henhold til første ledd skal Kommisjonen oversende det første utkastet til gjennomføringsrettsakt for komiteen nevnt i artikkel 22 nr. 1 innen 9. februar 2017.

Artikkel 12

CSIRT-nettverk

1. For å bidra til å skape tiltro og tillit blant medlemsstatene, og for å fremme et raskt og effektivt driftsmessig samarbeid, opprettes det herved et nettverk av nasjonale CSIRT-enheter.
2. CSIRT-nettverket skal bestå av representanter for medlemsstatenes CSIRT-enheter og CERT-EU. Kommisjonen skal delta i CSIRT-nettverket som observatør. ENISA skal ivareta sekretariatet og aktivt støtte samarbeidet mellom CSIRT-enhetene.
3. CSIRT-nettverket skal ha følgende oppgaver:
   a) utveksle opplysninger om CSIRT-enhetenes tjenester, drift og samarbeidsmuligheter,
   b) på anmodning fra en CSIRT-representant fra en medlemsstat som kan bli berørt av en hendelse, utveksle og drøfte saker som berører ikke-kommersielt følsomme opplysninger knyttet til hendelsen og tilknyttede risikoer; en CSIRT-enhet fra en medlemsstat kan imidlertid nekte å bidra til diskusjonen dersom det er fare for at det kan påvirke undersøkelsen av hendelsen negativt,
   c) utveksle og gjøre tilgjengelig ikke-fortrolige opplysninger om enkeltstående hendelser på frivillig grunnlag,
   d) på anmodning fra en representant for en medlemsstats CSIRT-enhet, drøfte og, om mulig, finne en samordnet innsats for en hendelse som er blitt avdekket i medlemsstatens jurisdiksjon,
   e) gi medlemsstatene støtte til å løse grensekryssende hendelser på grunnlag av frivillig gjensidig bistand,
   f) drøfte, undersøke og identifisere ytterligere former for driftsmessig samarbeid, herunder med hensyn til
      i) kategorier av risikoer og hendelser,
      ii) tidlige varslinger,
      iii) gjensidig bistand,
      iv) prinsipper og nærmere regler for samordning, når medlemsstatene setter inn tiltak mot grensekryssende risikoer og hendelser,
   g) underrette samarbeidsgruppen om sin virksomhet og om ytterligere former for driftsmessig samarbeid som er drøftet i henhold til bokstav f), og be om veiledning om dette,
   h) drøfte erfaringer fra øvelsene vedrørende sikkerhet i nettverks- og informasjonssystemer, herunder dem som organiseres av ENISA,
   i) på anmodning fra en gitt CSIRT-enhet, drøfte denne CSIRT-enhetens ressurser og beredskap,
   j) utarbeide retningslinjer for å lette sammenfallet mellom driftspraksiser med hensyn til anvendelsen av bestemmelsene om driftsmessig samarbeid i denne artikkel.
4. Med henblikk på gjennomgåelsen nevnt i artikkel 23 skal CSIRT-nettverket innen 9. august 2018, og deretter hvert halvannet år, utarbeide en rapport om de erfaringer som er gjort med det driftsmessige samarbeidet, herunder konklusjoner og anbefalinger, i henhold til denne artikkel. Denne rapporten skal også oversendes til samarbeidsgruppen.
5. CSIRT-nettverket skal fastsette sin egen forretningsorden.

Artikkel 13

Internasjonalt samarbeid

Unionen kan i samsvar med artikkel 218 i TEUV inngå internasjonale avtaler med tredjestater eller internasjonale organisasjoner og dermed muliggjøre og tilrettelegge for å delta i noen av samarbeidsgruppens aktiviteter. I slike avtaler skal det tas hensyn til behovet for å sikre tilstrekkelig vern av opplysninger.

Kapittel IV

Sikkerhet i nett- og informasjonssystemer som brukes av ytere av samfunnsviktige tjenester

Artikkel 14

Sikkerhetskrav og melding om hendelser

1. Medlemsstatene skal sikre at ytere av samfunnsviktige tjenester treffer hensiktsmessige og rimelige tekniske og organisatoriske tiltak for å håndtere risikoene knyttet til sikkerheten i nettverks- og informasjonssystemer som de bruker i sin virksomhet. Under henvisning til nåværende utviklingstrinn i teknikken skal disse tiltakene sikre et nivå for sikkerhet i nettverks- og informasjonssystemer som står i forhold til risikoen.
2. Medlemsstatene skal sikre at ytere av samfunnsviktige tjenester treffer egnede tiltak for å forebygge og minimere virkningen av hendelser som påvirker sikkerheten i nettverks- og informasjonssystemer som brukes til å yte slike samfunnsviktige tjenester, med sikte på å sikre kontinuiteten i disse tjenestene.
3. Medlemsstatene skal sikre at ytere av samfunnsviktige tjenester uten unødig opphold underretter vedkommende myndighet eller CSIRT-enheten om hendelser som virker betydelig inn på kontinuiteten i de samfunnsviktige tjenestene de yter. Meldinger skal inneholde opplysninger som gjør det mulig for vedkommende myndighet eller CSIRT-enheten å fastslå om hendelsen har virkninger over landegrensene. Meldingen skal ikke innebære økt ansvar for melderen.
4. Med henblikk på å fastslå omfanget av virkningen av en hendelse skal det tas hensyn særlig til følgende parametrer:
   a) antall brukere som påvirkes av forstyrrelsen i den samfunnsviktige tjenesten,
   b) hendelsens varighet,
   c) størrelsen på det geografiske området som berøres av hendelsen.
5. På grunnlag av opplysningene i meldingen fra yteren av samfunnsviktige tjenester skal vedkommende myndighet eller CSIRT-enheten underrette andre berørte medlemsstater dersom hendelsen virker betydelig inn på kontinuiteten i samfunnsviktige tjenester i nevnte medlemsstat. I den forbindelse skal vedkommende myndighet eller CSIRT-enheten, i samsvar med unionsretten eller nasjonal lovgivning som er i samsvar med unionsretten, ivareta sikkerhets- og forretningsinteressene til yteren av samfunnsviktige tjenester, samt sikre at opplysningene i meldingen behandles fortrolig.

   Når omstendighetene tillater det, skal vedkommende myndighet eller CSIRT-enheten gi yteren av samfunnsviktige tjenester som innga meldingen, relevante opplysninger om oppfølgingen av meldingen, f.eks. opplysninger som kan bidra til effektiv hendelseshåndtering.

   På anmodning fra vedkommende myndighet eller CSIRT-enheten skal det felles kontaktpunktet videresende meldinger som nevnt i første ledd, til felles kontaktpunkter i andre berørte medlemsstater.
6. Etter å ha rådspurt yteren av samfunnsviktige tjenester som innga meldingen, kan vedkommende myndighet eller CSIRT-enheten informere offentligheten om konkrete hendelser dersom offentlighetens kjennskap til disse er nødvendig for å forebygge en hendelse eller håndtere en hendelse som pågår.
7. Vedkommende myndigheter som opptrer sammen innenfor samarbeidsgruppen, kan utarbeide og vedta retningslinjer om under hvilke omstendigheter ytere av samfunnsviktige tjenester er pålagt å melde hendelser, herunder parametrene for å fastsette omfanget av virkningen av en hendelse som nevnt i nr. 4.

Artikkel 15

Gjennomføring og håndheving

1. Medlemsstatene skal sikre at vedkommende myndigheter har de nødvendige fullmakter og virkemidler til å vurdere om ytere av samfunnsviktige tjenester oppfyller sine forpliktelser i henhold til artikkel 14 og virkningene av dette på sikkerheten i nettverks- og informasjonssystemer.
2. Medlemsstatene skal sikre at vedkommende myndigheter har fullmakter og virkemidler til å kreve at ytere av samfunnsviktige tjenester sørger for

a) de opplysninger som er nødvendige for å vurdere sikkerheten i nettverks- og informasjonssystemene deres, herunder en dokumentert sikkerhetspolitikk,
b) dokumentasjon på effektiv gjennomføring av en sikkerhetspolitikk, for eksempel resultatene av en sikkerhetsrevisjon utført av vedkommende myndighet eller en kvalifisert inspektør og, i sistnevnte tilfelle, stille resultatene og den underliggende dokumentasjonen til rådighet for vedkommende myndighet.

Når det anmodes om slike opplysninger eller dokumentasjon, skal vedkommende myndighet angi formålet med anmodningen og presisere hvilke opplysninger som kreves.

3. På grunnlag av vurderingen av opplysninger eller resultater av sikkerhetsrevisjoner nevnt i nr. 2, kan vedkommende myndighet gi bindende instrukser til ytere av samfunnsviktige tjenester om å utbedre de påviste manglene.
4. Vedkommende myndighet skal samarbeide tett med personvernmyndigheter når de håndterer hendelser som innebærer brudd på personopplysningssikkerheten.

Kapittel V

Sikkerhet i nett- og informasjonssystemer som brukes av tilbydere av digitale tjenester

Artikkel 16

Sikkerhetskrav og melding om hendelser

1. Medlemsstatene skal sikre at tilbydere av digitale tjenester identifiserer og treffer hensiktsmessige og rimelige tekniske og organisatoriske tiltak for å håndtere risikoene knyttet til sikkerheten i nettverks- og informasjonssystemer som de bruker når de leverer tjenester nevnt i vedlegg III, i Unionen. Under henvisning til nåværende utviklingstrinn i teknikken skal disse tiltakene sikre et nivå for sikkerhet i nettverks- og informasjonssystemer som står i forhold til risikoen, idet det tas hensyn til følgende elementer:
   a) sikkerheten i systemer og anlegg,
   b) hendelseshåndtering,
   c) styring av driftskontinuitet,
   d) overvåking, revisjon og testing,
   e) overholdelse av internasjonale standarder.
2. Medlemsstatene skal sikre at tilbydere av digitale tjenester treffer tiltak for å forebygge og minimere virkningen av hendelser som påvirker sikkerheten i deres nettverks- og informasjonssystemer, på tjenestene nevnt i vedlegg III og som tilbys i Unionen, med sikte på å sikre kontinuiteten i disse tjenestene.
3. Medlemsstatene skal sikre at tilbydere av digitale tjenester uten unødig opphold gir vedkommende myndighet eller CSIRT-enheten melding om enhver hendelse som virker betydelig inn på leveringen av en tjeneste som nevnt i vedlegg III og som de tilbyr i Unionen. Meldinger skal inneholde opplysninger som gjør det mulig for vedkommende myndighet eller CSIRT-enheten å fastslå omfanget av eventuelle virkninger over landegrensene. Meldingen skal ikke innebære økt ansvar for melderen.
4. Med henblikk på å fastslå om virkningen av en hendelse er betydelig, skal det tas hensyn særlig til følgende parametrer:
   a) antall brukere som påvirkes av hendelsen, særlig brukere som er avhengige av tjenesten for å kunne yte egne tjenester,
   b) hendelsens varighet,
   c) størrelsen på det geografiske området som berøres av hendelsen,
   d) omfanget av driftsforstyrrelser i tjenesten,
   e) omfanget av virkningen på økonomisk og samfunnsmessig virksomhet.

   Plikten til å melde en hendelse skal få anvendelse bare dersom tilbyderen av digitale tjenester har tilgang til opplysningene som trengs for å vurdere virkningen av en hendelse opp mot parametrene nevnt i første ledd.
5. Dersom en yter av samfunnsviktige tjenester er avhengig av en tredjemannstilbyder av digitale tjenester for å yte en tjeneste som er grunnleggende for å opprettholde viktig samfunnsmessig og økonomisk virksomhet, skal yteren av samfunnsviktige tjenester melde enhver betydelig virkning på kontinuiteten i den samfunnsviktige tjenesten som skyldes en hendelse som påvirker tilbyderen av digitale tjenester.
6. Dersom det er relevant, særlig dersom hendelsen nevnt i nr. 3 berører to eller flere medlemsstater, skal vedkommende myndighet eller CSIRT-enheten underrette de øvrige berørte medlemsstatene. I den forbindelse skal vedkommende myndigheter, CSIRT-enheten og felles kontaktpunkter, i samsvar med unionsretten eller nasjonal lovgivning som er i samsvar med unionsretten, ivareta sikkerhets- og forretningsinteressene til tilbyderen av digitale tjenester, samt sikre at opplysningene behandles fortrolig.
7. Etter å ha rådspurt den berørte tilbyderen av digitale tjenester, kan vedkommende myndig-

het eller CSIRT-enheten og, eventuelt, myndighetene eller CSIRT-enhetene i andre berørte medlemsstater, informere offentligheten om konkrete hendelser eller kreve at tilbyderen av digitale tjenester gjør det, dersom offentlighetens kjennskap til disse er nødvendig for å forebygge en hendelse eller håndtere en hendelse som pågår, eller dersom offentliggjøring av hendelsen ellers er i offentlighetens interesse.

8. Kommisjonen skal vedta gjennomføringsrettsakter for å angi nærmere elementene som er nevnt i nr. 1 og parametrene som er oppført i nr. 4 i denne artikkel. Disse gjennomføringsrettsaktene skal vedtas etter framgangsmåten med undersøkelseskomité nevnt i artikkel 22 nr. 2 innen 9. august 2017.
9. Kommisjonen kan vedta gjennomføringsrettsakter om fastsettelse av formater og framgangsmåter som får anvendelse på meldingskrav. Disse gjennomføringsrettsaktene skal vedtas etter framgangsmåten med undersøkelseskomité nevnt i artikkel 22 nr. 2.
10. Uten at det berører artikkel 1 nr. 6 skal medlemsstatene ikke pålegge tilbydere av digitale tjenester ytterligere sikkerhets- eller meldingskrav.
11. Kapittel V får ikke anvendelse på svært små og små bedrifter som definert i kommisjonsrekommandasjon 2003/361/EF[19].

Artikkel 17

Gjennomføring og håndheving

1. Medlemsstatene skal sikre at vedkommende myndigheter ved behov griper inn gjennom tilsynstiltak i ettertid, når det foreligger dokumentasjon på at en tilbyder av digitale tjenester ikke oppfyller kravene fastsatt i artikkel 16. Slik dokumentasjon kan sendes inn av en vedkommende myndighet i en annen medlemsstat der tjenesten leveres.
2. Med henblikk på nr. 1 skal vedkommende myndigheter ha de nødvendige fullmakter og virkemidler til å kreve at tilbydere av digitale tjenester
   a) gir de opplysninger som er nødvendige for å vurdere sikkerheten i nettverks- og informasjonssystemene deres, herunder en dokumentert sikkerhetspolitikk,
   b) utbedrer enhver eventuell manglende oppfyllelse av kravene fastsatt i artikkel 16.
3. Dersom en tilbyder av digitale tjenester har sitt hovedforetak eller en representant i en medlemsstat, men sine nettverks- og informasjonssystemer i en eller flere andre medlemsstater, skal vedkommende myndighet i medlemsstaten der hovedforetaket eller representanten befinner seg og vedkommende myndigheter i de andre medlemsstatene samarbeide og bistå hverandre ved behov. Nevnte bistand og samarbeid kan omfatte utveksling av opplysninger mellom de berørte vedkommende myndigheter og anmodninger om å treffe tilsynstiltakene nevnt i nr. 2.

Artikkel 18

Jurisdiksjon og territorialitetsprinsippet

1. For dette direktivs formål skal en tilbyder av digitale tjenester anses å være underlagt jurisdiksjonen i den medlemsstat hvor den har sitt hovedforetak. En tilbyder av digitale tjenester skal anses å ha sitt hovedforetak i en medlemsstat når den har sitt hovedkontor i denne medlemsstaten.
2. En tilbyder av digitale tjenester som ikke er etablert i Unionen, men som tilbyr tjenestene nevnt i vedlegg III i Unionen, skal utpeke en representant i Unionen. Representanten skal være etablert i en av medlemsstatene hvor tjenestene tilbys. Tilbyderen av digitale tjenester skal anses som underlagt jurisdiksjonen til medlemsstaten hvor representanten er etablert.
3. Når tilbyderen av digitale tjenester utpeker en representant, skal dette ikke berøre eventuelle rettslige skritt mot selve tilbyderen av digitale tjenester.

Kapittel VI

Standardisering og frivillig melding

Artikkel 19

Standardisering

1. For å fremme en ensartet gjennomføring av artikkel 14 nr. 1 og 2 og artikkel 16 nr. 1 og 2 skal medlemsstatene, uten å pålegge eller innebære forskjellsbehandling til fordel for bruk av en bestemt type teknologi, oppmuntre til bruk av europeiske eller internasjonalt anerkjente standarder og spesifikasjoner som er relevante for sikkerheten i nettverks- og informasjonssystemer.

[19] Kommisjonsrekommandasjon 2003/361/EF av 6. mai 2003 om definisjonen av svært små, små og mellomstore bedrifter (EFT L 124 av 20.5.2003, s. 36).

2. ENISA skal i samarbeid med medlemsstatene utarbeide råd og retningslinjer for de tekniske områdene som skal tas i betraktning i forbindelse med nr. 1, samt om allerede eksisterende standarder, herunder medlemsstatenes nasjonale standarder, som vil gjøre det mulig å dekke disse områdene.

Artikkel 20

Frivillig melding

1. Uten at det berører artikkel 3 kan foretak som ikke er blitt identifisert som ytere av samfunnsviktige tjenester, og som ikke er tilbydere av digitale tjenester, på frivillig grunnlag melde hendelser som virker betydelig inn på kontinuiteten i tjenestene de yter.
2. Når medlemsstatene behandler meldinger, skal de opptre etter framgangsmåten fastsatt i artikkel 14. Medlemsstatene kan prioritere behandlingen av obligatoriske meldinger over frivillige meldinger. Frivillige meldinger skal behandles bare dersom slik behandling ikke utgjør en uforholdsmessig stor eller urimelig byrde for medlemsstatene.

   Frivillig melding skal ikke innebære at melderforetaket pålegges eventuelle forpliktelser som det ikke hadde vært omfattet av dersom det ikke hadde gitt meldingen.

Kapittel VII

Sluttbestemmelser

Artikkel 21

Sanksjoner

Medlemsstatene skal fastsette regler for sanksjoner mot overtredelser av de nasjonale bestemmelsene som er vedtatt i henhold til dette direktiv, og treffe alle nødvendige tiltak for å sikre at de gjennomføres. De fastsatte sanksjonene skal være virkningsfulle, stå i forhold til overtredelsen og virke avskrekkende. Medlemsstatene skal innen 9. mai 2018 underrette Kommisjonen om disse bestemmelsene og tiltakene og umiddelbart underrette den om eventuelle senere endringer.

Artikkel 22

Komitéframgangsmåte

1. Kommisjonen skal bistås av komiteen for sikkerhet i nettverks- og informasjonssystemer. Nevnte komité skal være en komité i henhold til forordning (EU) nr. 182/2011.
2. Når det vises til dette nummer, får artikkel 5 i forordning (EU) nr. 182/2011 anvendelse.

Artikkel 23

Gjennomgåelse

1. Innen 9. mai 2019 skal Kommisjonen framlegge en rapport for Europaparlamentet og Rådet med en vurdering av sammenhengen i metoden som medlemsstatene har truffet med hensyn til identifisering av ytere av samfunnsviktige tjenester.
2. Kommisjonen skal regelmessig gjennomgå virkningen av dette direktiv og framlegge en rapport for Europaparlamentet og Rådet. For dette formål, og med sikte på en ytterligere fremming av strategisk og driftsmessig samarbeid, skal Kommisjonen ta hensyn til rapportene fra Samarbeidsgruppen og CSIRT-nettverket om de erfaringer som er gjort på strategisk og driftsmessig plan. I sin gjennomgåelse skal Kommisjonen også vurdere listene i vedlegg II og III, og sammenhengen i identifiseringen av ytere av samfunnsviktige tjenester og tjenester i sektorene nevnt i vedlegg II. Den første rapporten skal framlegges innen 9. mai 2021.

Artikkel 24

Overgangsbestemmelser

1. Uten at det berører artikkel 25 og med sikte på å gi medlemsstatene ytterligere muligheter til hensiktsmessig samarbeid i løpet av perioden for innarbeiding i nasjonal lovgivning, skal Samarbeidsgruppen og CSIRT-nettverket begynne å utføre oppgavene fastsatt i henholdsvis artikkel 11 nr. 3 og artikkel 12 nr. 3 innen 9. februar 2017.
2. I perioden fra 9. februar 2017 til 9. november 2018, og med henblikk på å støtte medlemsstatene i å bruke en konsekvent metode for å identifisere ytere av samfunnsviktige tjenester, skal Samarbeidsgruppen drøfte framgangsmåten for, innholdet i og typen av nasjonale tiltak som gjør det mulig å identifisere ytere av samfunnsviktige tjenester innenfor en bestemt sektor i samsvar med kriteriene fastsatt i artikkel 5 og 6. Samarbeidsgruppen skal også, på anmodning fra en medlemsstat, drøfte særlige utkast til nasjonale tiltak i medlemsstaten som gjør det mulig å identifisere ytere av samfunnsviktige tjenester innenfor en bestemt sektor i samsvar med kriteriene fastsatt i artikkel 5 og 6.

3. Innen 9. februar 2017 og ved anvendelsen av denne artikkel skal medlemsstatene sikre hensiktsmessig representasjon i Samarbeidsgruppen og CSIRT-nettverket.

Artikkel 25

Innarbeiding i nasjonal lovgivning

1. Medlemsstatene skal innen 9. mai 2018 vedta og kunngjøre de lover og forskrifter som er nødvendige for å etterkomme dette direktiv. De skal umiddelbart underrette Kommisjonen om dette.

   De skal anvende disse bestemmelsene fra 10. mai 2018.

   Når disse bestemmelsene vedtas av medlemsstatene, skal de inneholde en henvisning til dette direktiv, eller det skal vises til direktivet når de kunngjøres. Nærmere regler for henvisningen fastsettes av medlemsstatene.
2. Medlemsstatene skal oversende Kommisjonen teksten til de viktigste internrettslige bestemmelser som de vedtar på det området dette direktiv omhandler.

Artikkel 26

Ikrafttredelse

Dette direktiv trer i kraft den 20. dagen etter at det er kunngjort i *Den europeiske unions tidende*.

Artikkel 27

Adressater

Dette direktiv er rettet til medlemsstatene.

Utferdiget i Strasbourg 6. juli 2016.

For Europaparlamentet	*For Rådet*
M. SCHULZ	I. KORČOK
President	*Formann*

Vedlegg I

Krav til enheter for håndtering av digitale hendelser (CSIRT) og deres oppgaver

Kravene til CSIRT-enheter og deres oppgaver skal være tilstrekkelig og tydelig definert og underbygget gjennom nasjonal politikk og/eller lovgivning. De skal omfatte følgende:

1) Krav til CSIRT-enheter:
   a) CSIRT-enheter skal sikre et høyt tilgjengelighetsnivå for kommunikasjonstjenestene sine ved å unngå svake punkter («single points of failure»), og skal til enhver tid ha flere muligheter for å bli kontaktet og til å kontakte andre. Videre skal kommunikasjonskanalene tydelig angis og være godt kjent for brukergruppen og samarbeidspartnere.
   b) CSIRT-enhetenes lokaler og underliggende informasjonssystemer skal være plassert på et sikkert sted.
   c) Driftskontinuitet:
      i) CSIRT-enheter skal være utstyrt med et egnet system for å håndtere og videreformidle anmodninger, for å lette overleveringer.
      ii) CSIRT-enheter skal ha tilstrekkelig personale til å sikre tilgjengelighet hele døgnet.
      iii) CSIRT-enheter skal ha en infrastruktur med garantert kontinuerlig drift. For dette formål skal overflødige systemer og reservearbeidsområder være tilgjengelige.
   d) CSIRT-enheter skal ha mulighet til å delta, dersom de ønsker det, i internasjonale samarbeidsnettverk.
2) CSIRT-enhetenes oppgaver:
   a) CSIRT-enhetenes oppgaver skal minst omfatte følgende:
      i) overvåke hendelser på nasjonalt plan,
      ii) sørge for tidlig varsling, alarmer, meldinger og formidling av opplysninger til berørte parter om risikoer og hendelser,
      iii) iverksette tiltak ved hendelser,
      iv) sørge for dynamisk risiko- og hendelsesanalyse og situasjonsforståelse,
      v) delta i CSIRT-nettverkene.
   b) CSIRT-enheter skal inngå et samarbeid med privat sektor.
   c) For å legge til rette for samarbeid skal CSIRT-enheter fremme vedtakelse og bruk av en felles eller standardisert praksis for
      i) prosedyrer for håndtering av hendelser og risikoer,
      ii) systemer for klassifisering av hendelser, risikoer og opplysninger.

Vedlegg II

Typer av foretak med henblikk på artikkel 4 nr. 4

Sektor	Delsektor	Type foretak
1. Energi	a) Elektrisitet:	– Elektrisitetsforetak som definert i artikkel 2 nr. 35 i europaparlaments- og rådsdirektiv 2009/72/EF[1], som ivaretar «forsyning» i henhold til definisjonen i artikkel 2 nr. 19 i nevnte direktiv – Operatører av distribusjonsnett som definert i artikkel 2 nr. 6 i direktiv 2009/72/EF – Operatører av overføringsnett som definert i artikkel 2 nr. 4 i direktiv 2009/72/EF
	b) Olje	– Operatører av oljerørledninger – Operatører av anlegg for produksjon, raffinering, behandling, lagring og transport av olje
	c) Gass	– Forsyningsforetak som definert i artikkel 2 nr. 8 i europaparlaments- og rådsdirektiv 2009/73/EF[2] – Operatører av distribusjonsnett som definert i artikkel 2 nr. 6 i direktiv 2009/73/EF – Operatører av overføringsnett som definert i artikkel 2 nr. 4 i direktiv 2009/73/EF – Operatører av lagringsnett som definert i artikkel 2 nr. 10 i direktiv 2009/73/EF – Operatører av LNG-nett som definert i artikkel 2 nr. 12 i direktiv 2009/73/EF – Naturgassforetak som definert i artikkel 2 nr. 1 i direktiv 2009/73/EF – Operatører av raffinerings- og behandlingsanlegg for naturgass
2. Transport	a) Lufttransport	– Luftfartsselskaper som definert i artikkel 3 nr. 4 i europaparlaments- og rådsforordning (EF) nr. 300/2008[3] – Lufthavnadministrasjoner som definert i artikkel 2 nr. 2 i europaparlaments- og rådsdirektiv 2009/12/EF[4], lufthavner som definert i artikkel 2 nr. 1 i nevnte direktiv, herunder de viktigste lufthavnene oppført i avsnitt 2 i vedlegg II til europaparlaments- og rådsforordning (EU) nr. 1315/2013[5], og foretak som driver tilhørende anlegg i lufthavner – Operatører innen trafikkstyring som yter flygekontrolltjenester (ATC) som definert i artikkel 2 nr. 1 i europaparlaments- og rådsforordning (EF) nr. 549/2004[6]

Sektor	Delsektor	Type foretak
	b) Jernbanetransport	– Infrastrukturforvaltninger som definert i artikkel 3 nr. 2 i europaparlaments- og rådsdirektiv 2012/34/EU[7] – Jernbaneforetak som definert i artikkel 3 nr. 1 i direktiv 2012/34/EU, herunder operatører av serviceanlegg som definert i artikkel 3 nr. 12 i direktiv 2012/34/EU
	c) Transport på vannveier	– Foretak som driver passasjertrafikk og godstransport på innlands vannveier, til sjøs og langs kysten, i samsvar med definisjonen av sjøtransport i vedlegg I til europaparlaments- og rådsforordning (EF) nr. 725/2004[8], med unntak av de enkelte fartøyene som drives av disse foretakene – Administrasjoner i havner som definert i artikkel 3 nr. 1 europaparlaments- og rådsdirektiv 2005/65/EF[9], herunder havneanlegg som definert i artikkel 2 nr. 11 i forordning (EF) nr. 725/2004, samt foretak som driver anlegg og utstyr i havner – Operatører av sjøtrafikksentraler som definert i artikkel 3 bokstav o) i europaparlaments- og rådsdirektiv 2002/59/EF[10]
	d) Veitransport	– Veimyndigheter som definert i artikkel 2 nr. 12 i delegert kommisjonsforordning (EU) 2015/962[11] med ansvar for trafikkstyring – Operatører av intelligente transportsystemer som definert i artikkel 4 nr. 1 i europaparlaments- og rådsdirektiv 2010/40/EU[12]
3. Bankvirksomhet		– Kredittinstitusjoner som definert i artikkel 4 nr. 1 i europaparlaments- og rådsforordning (EU) nr. 575/2013[13]
4. Finans-markedenes infrastrukturer		– Operatører av handelsplasser som definert i artikkel 4 nr. 24) i europaparlaments- og rådsdirektiv 2014/65/EU[14] – Sentrale motparter som definert i artikkel 2 nr. 1 i europaparlaments- og rådsforordning (EU) nr. 648/2012[15]
5. Helsesektoren	Helsetjenestemiljøer (herunder sykehus og private klinikker)	– Helsetjenesteytere som definert i artikkel 3 bokstav g) i europaparlaments- og rådsdirektiv 2011/24/EU[16]
6. Forsyning og distribusjon av drikkevann		Leverandører og distributører av drikkevann som definert i artikkel 2 nr. 1 bokstav a) i rådsdirektiv 98/83/EF[17], men unntatt distributører hvis distribusjon av drikkevann bare utgjør en del av deres generelle virksomhet, som består av distribusjon av andre råvarer og varer og ikke anses som samfunnsviktige tjenester

Sektor	Delsektor	Type foretak
7. Digital infrastruktur		– IXP-er – Tilbydere av DNS-tjenester – Registerenheter for toppdomener

[1] Europaparlaments- og rådsdirektiv 2009/72/EF av 13. juli 2009 om felles regler for det indre marked for elektrisk kraft og om oppheving av direktiv 2003/54/EF (EUT L 211 av 14.8.2009, s. 55).

[2] Europaparlaments- og rådsdirektiv 2009/73/EF av 13. juli 2009 om felles regler for det indre marked for naturgass og om oppheving av direktiv 2003/55/EF (EUT L 211 av 14.8.2009, s. 94).

[3] Europaparlaments- og rådsforordning (EF) nr. 300/2008 av 11. mars 2008 om felles bestemmelser om sikkerhet i sivil luftfart og om oppheving av forordning (EF) nr. 2320/2002 (EUT L 97 av 9.4.2008, s. 72).

[4] Europaparlaments- og rådsdirektiv 2009/12/EF av 11. mars 2009 om lufthamnavgifter (EUT L 70 av 14.3.2009, s. 11).

[5] Europaparlaments- og rådsforordning (EU) nr. 1315/2013 av 11. desember 2013 om unionsretningslinjer for utviklingen av et transeuropeisk transportnett og om oppheving av beslutning nr. 661/2010/EU (EUT L 348 av 20.12.2013, s. 1).

[6] Europaparlaments- og rådsforordning (EF) nr. 549/2004 av 10. mars 2004 om fastsettelse av rammeregler for opprettelse av et felles europeisk luftrom (rammeforordningen) (EUT L 96 av 31.3.2004, s. 1).

[7] Europaparlaments- og rådsdirektiv 2012/34/EF av 21. november 2012 om opprettelse av et felles europeisk jernbaneområde (EUT L 343 av 14.3.2009, s. 32).

[8] Europaparlaments- og rådsforordning (EF) nr. 725/2004 av 31. mars 2004 om forbedret sikkerhet for fartøyer og havneanlegg (EUT L 129 av 29.4.2004, s. 6).

[9] Europaparlaments- og rådsdirektiv 2005/65/EF av 26. oktober 2005 om forbedret sikkerhet for havner (EUT L 310 av 25.11.2005, s. 28).

[10] Europaparlaments- og rådsdirektiv 2002/59/EF av 27. juni 2002 om opprettelse av et overvåkings- og informasjonssystem for sjøtrafikk i Fellesskapet og om oppheving av rådsdirektiv 93/75/EØF (EFT L 208 av 5.8.2002, s. 10).

[11] Delegert kommisjonsforordning (EU) nr. 2015/962 av 18. desember 2014 om utfylling av europaparlaments- og rådsdirektiv 2010/40/EU med hensyn til sanntids trafikkinformasjonstjenester på EU-plan (EUT L 157 av 23.6.2015, s 21).

[12] Europaparlaments- og rådsdirektiv 2010/40/EU av 7. juli 2010 om en ramme for innføring av intelligente transportsystemer innen veitransport og for grensesnitt mot andre transportsystemer (EUT L 207 av 6.8.2010, s. 1).

[13] Europaparlaments- og rådsforordning (EU) nr. 575/2013 av 26. juni 2013 om tilsynskrav for kredittinstitusjoner og verdipapirforetak og om endring av forordning (EU) nr. 648/2012 (EUT L 176 av 27.6.2013, s. 1).

[14] Europaparlaments- og rådsdirektiv 2014/65/EU av 15. mai 2014 om markeder for finansielle instrumenter og om endring av direktiv 2002/92/EF og direktiv 2011/61/EU (EUT L 173 av 12.6.2014, s. 349).

[15] Europaparlaments- og rådsforordning (EU) nr. 648/2012 av 4. juli 2012 om OTC-derivater, sentrale motparter og transaksjonsregistre (EUT L 201 av 27.7.2012, s. 1).

[16] Europaparlaments- og rådsdirektiv 2011/24/EU av 9. mars 2011 om anvendelse av pasientrettigheter ved helsetjenester over landegrensene (EUT L 88 av 4.4.2011, s. 45).

[17] Rådsdirektiv 98/83/EF av 3. november 1998 om drikkevannets kvalitet (EFT L 330 av 5.12.1998, s. 32).

Vedlegg III

Typer av digitale tjenester med henblikk på artikkel 4 nr. 5

1. Nettbasert markedsplass.
2. Nettbasert søkemotor.
3. Skytjeneste.

Vedlegg 4

Kommisjonens gjennomføringsforordning (EU) 2018/151 av 30. januar 2018 om fastsettelse av regler for anvendelse av europaparlaments- og rådsdirektiv (EU) 2016/1148 med hensyn til ytterligere spesifisering av de elementene som tilbydere av digitale tjenester skal ta hensyn til for å håndtere risikoene knyttet til sikkerheten i nettverks- og informasjonssystemer, og av parametrene for å avgjøre om en hendelse har en betydelig innvirkning

EUROPAKOMMISJONEN HAR

under henvisning til traktaten om Den europeiske unions virkemåte,

under henvisning til europaparlaments- og rådsdirektiv (EU) 2016/1148 av 6. juli 2016 om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i hele Unionen[1], særlig artikkel 16 nr. 8, og

ut fra følgende betraktninger:

1) I henhold til direktiv (EU) 2016/1148 står tilbydere av digitale tjenester fritt til å treffe tekniske og organisatoriske tiltak som de anser som hensiktsmessige og forholdsmessige for å håndtere risikoer for sikkerheten i sine nettverks- og informasjonssystemer, så lenge disse tiltakene sikrer et passende sikkerhetsnivå og tar hensyn til elementene som er omhandlet i det nevnte direktivet.
2) Når tilbydere av digitale tjenester skal identifisere hensiktsmessige og forholdsmessige tekniske og organisatoriske tiltak, bør de gripe an informasjonssikkerhet på en systematisk måte gjennom en risikobasert tilnærming.
3) For å ivareta sikkerheten i systemer og anlegg bør tilbydere av digitale tjenester gjennomføre vurderings- og analyseprosedyrer. Disse aktivitetene bør omfatte systematisk forvaltning av nettverks- og informasjonssystemer, fysisk og miljømessig sikkerhet, forsyningssikkerhet og adgangskontroll.
4) Når tilbydere av digitale tjenester foretar en risikoanalyse som ledd i den systematiske forvaltningen av nettverks- og informasjonssystemer, bør de oppmuntres til å identifisere spesifikke risikoer og kvantifisere deres betydning, for eksempel ved å identifisere trusler mot kritiske ressurser og hvordan disse kan påvirke driften, og til å avgjøre hvordan disse truslene best kan avhjelpes på grunnlag av gjeldende kapasitet og ressursbehov.
5) Personalpolitikken kan omfatte kompetansestyring, herunder aspekter knyttet til utviklingen av sikkerhetsrelaterte ferdigheter og bevisstgjøring. Når tilbydere av digitale tjenester skal fastsette hensiktsmessige retningslinjer for driftssikkerhet, bør de oppmuntres til å ta hensyn til aspekter ved endringsstyring, håndtering av sårbarhet, formalisering av drifts- og forvaltningspraksis og systemkartlegging.
6) Retningslinjer for sikkerhetsarkitektur kan spesifikt omfatte atskillelse av nettverk og systemer samt særlige sikkerhetstiltak for kritiske funksjoner, for eksempel administrative operasjoner. Atskillelsen av nettverk og systemer kan gjøre det mulig for en tilbyder av digitale tjenester å skille mellom elementer som datastrømmer og databehandlingsressurser som tilhører en kunde, en gruppe av kunder, tilbyderen av digitale tjenester eller en tredjepart.
7) Tiltakene som treffes med hensyn til fysisk og miljømessig sikkerhet, bør sikre en organisasjons nettverks- og informasjonssystemer mot skader forårsaket av hendelser som tyveri, brann, flom eller andre værfenomener, telekommunikasjonsfeil eller strømbrudd.
8) Forsyningssikkerheten, for eksempel elektrisk kraft, brensel eller kjøling, kan omfatte forsyningskjedens sikkerhet, som særlig

[1] EUT L 194 av 19.7.2016, s. 1.

omfatter tredjepartsleverandørers og underleverandørers sikkerhet og hvordan de forvalter den. Sporbarhet av kritiske forsyninger viser til evnen tilbyderen av digitale tjenester har til å identifisere og registrere kildene til disse forsyningene.

9) Brukere av digitale tjenester bør omfatte fysiske og juridiske personer som er kunder av eller abonnenter på en nettbasert markedsplass eller nettskytjeneste, eller som besøker et søkemotornettsted for å foreta nøkkelordsøking.
10) Når det skal fastsettes om en hendelse har en betydelig innvirkning, bør tilfellene fastsatt i denne forordningen anses som en ikke-uttømmende liste over betydelige hendelser. Det bør trekkes erfaringer fra gjennomføringen av denne forordningen og fra samarbeidsgruppens arbeid med å innhente opplysninger om beste praksis i forbindelse med risikoer og hendelser og drøftingene av metodene for rapportering av hendelser som nevnt i artikkel 11 nr. 3 bokstav i) og m) i direktiv (EU) 2016/1148. Resultatet kan bli detaljerte retningslinjer for kvantitative terskler for meldingsparametrer som kan utløse meldingsplikten for tilbydere av digitale tjenester i henhold til artikkel 16 nr. 3 i direktiv (EU) 2016/1148. Kommisjonen kan eventuelt også vurdere å revidere de gjeldende tersklene som er fastsatt i denne forordningen.
11) For at vedkommende myndigheter skal kunne bli underrettet om potensielle nye risikoer, bør tilbyderne av digitale tjenester oppmuntres til frivillig å rapportere enhver hendelse med kjennetegn som tidligere har vært ukjent for dem, for eksempel nye metoder for å utnytte sikkerhetshull («exploits»), angrepsvektorer eller trusselaktører, sårbarheter og farer.
12) Denne forordningen bør få anvendelse dagen etter utløpet av fristen for innarbeiding av direktiv (EU) 2016/1148.
13) Tiltakene fastsatt i denne forordningen er i samsvar med uttalelse fra komiteen for sikkerhet i nettverks- og informasjonssystemer nevnt i artikkel 22 i direktiv (EU) 2016/1148.

VEDTATT DENNE FORORDNINGEN:

Artikkel 1

Formål

Denne forordningen spesifiserer nærmere hvilke elementer tilbydere av digitale tjenester skal ta hensyn til når de identifiserer og treffer tiltak for å garantere et nivå av sikkerhet i nettverks- og informasjonssystemer som de bruker i forbindelse med tilbud av tjenester nevnt i vedlegg III til direktiv (EU) 2016/1148, og spesifiserer nærmere hvilke parametrer som skal tas i betraktning for å avgjøre om en hendelse har en betydelig innvirkning på leveringen av disse tjenestene.

Artikkel 2

Sikkerhetselementer

1. Med sikkerhet i systemer og anlegg nevnt i artikkel 16 nr. 1 bokstav a) i direktiv (EU) 2016/1148 menes sikkerheten i nettverks- og informasjonssystemer og i deres fysiske miljø, som skal omfatte følgende elementer:
   a) Systematisk forvaltning av nettverks- og informasjonssystemer, som innebærer en kartlegging av informasjonssystemer og utarbeiding av egnede retningslinjer for informasjonssikkerhetsstyring, herunder risikoanalyse, menneskelige ressurser, driftssikkerhet, sikkerhetsarkitektur, sikker livssyklusstyring for data og systemer og eventuelt kryptering og håndtering av slik kryptering.
   b) Fysisk og miljømessig sikkerhet, som innebærer at det finnes et sett av tiltak for å ivareta sikkerheten i nettverks- og informasjonssystemene til tilbydere av digitale tjenester mot skader gjennom en risikobasert tilnærming som dekker alle farer, for eksempel systemfeil, menneskelige feil, skadelige handlinger eller naturfenomener.
   c) Forsyningssikkerhet, som innebærer at det utarbeides og ajourføres egnede retningslinjer for å sikre tilgjengeligheten av og, dersom det er relevant, sporbarheten for kritiske forsyninger som brukes ved levering av tjenestene.
   d) Adgangskontroll for nettverks- og informasjonssystemer, som innebærer at det finnes et sett av tiltak for å sikre at fysisk og logisk adgang til nettverks- og informasjonssystemer, herunder den administrative sikkerheten i nettverks- og informasjonssystemer, gis og begrenses på grunnlag av forretnings- og sikkerhetsmessige krav.
2. Når det gjelder hendelseshåndtering nevnt i artikkel 16 nr. 1 bokstav b) i direktiv (EU) 2016/1148, skal tiltakene som treffes av tilbyderen av digitale tjenester, omfatte følgende:
   a) Opprettholdelse og testing av påvisningsprosesser og -prosedyrer for å sikre at avvik oppdages til rett tid og i tilstrekkelig grad.

b) Prosesser og retningslinjer for rapportering av hendelser og kartlegging av svakheter og sårbarheter i informasjonssystemene deres.
c) Respons i samsvar med fastsatte prosedyrer og rapportering av resultatene av tiltaket som er truffet.
d) En vurdering av hendelsens alvorlighetsgrad med dokumentasjon av kunnskapen fra hendelsesanalysen og innsamling av relevant informasjon som kan tjene som bevis og støtte en kontinuerlig forbedringsprosess.

3. Med styring av driftskontinuitet nevnt i artikkel 16 nr. 1 bokstav c) i direktiv (EU) 2016/1148 menes en organisasjons evne til å opprettholde eller eventuelt gjenopprette leveringen av tjenester på akseptable forhåndsdefinerte nivåer etter en forstyrrende hendelse og skal omfatte
   a) utarbeiding og bruk av beredskapsplaner basert på en driftskonsekvensanalyse for å sikre kontinuitet i tjenestene som leveres av tilbydere av digitale tjenester, som skal vurderes og testes regelmessig, for eksempel gjennom øvelser,
   b) katastrofeberedskap, som skal vurderes og testes regelmessig, for eksempel gjennom øvelser.
4. Overvåkingen, revisjonen og testingen nevnt i artikkel 16 nr. 1 bokstav d) i direktiv (EU) 2016/1148 skal omfatte utarbeiding og ajourføring av retningslinjer for
   a) gjennomføring av en planlagt rekke observasjoner eller målinger for å vurdere om nettverks- og informasjonssystemene fungerer etter hensikten,
   b) inspeksjon og verifisering for å kontrollere om en standard eller et sett med retningslinjer blir fulgt, om registreringene er nøyaktige og om målene for effektivitet og virkning nås,
   c) en prosess som er beregnet på å avdekke mangler i sikkerhetsmekanismene i et nettverks- og informasjonssystem som beskytter data og opprettholder den tilsiktede funksjonaliteten. En slik prosess skal omfatte tekniske prosesser og personell som er involvert i driftsflyten.
5. Med internasjonale standarder nevnt i artikkel 16 nr. 1 bokstav e) i direktiv (EU) 2016/1148 menes standarder som er vedtatt av et internasjonalt standardiseringsorgan som nevnt i artikkel 2 nr. 1 bokstav a) i europaparlaments- og rådsforordning (EU) nr. 1025/2012[2]. I henhold til artikkel 19 i direktiv (EU) 2016/1148 kan europeisk eller internasjonalt anerkjente standarder og spesifikasjoner som er relevante for sikkerheten i nettverks- og informasjonssystemer, herunder eksisterende nasjonale standarder, også brukes.
6. Tilbydere av digitale tjenester skal sikre at de har tilstrekkelig dokumentasjon tilgjengelig til at vedkommende myndighet kan kontrollere samsvar med sikkerhetselementene angitt i nr. 1, 2, 3, 4 og 5.

Artikkel 3

Parametrer som skal tas i betraktning for å avgjøre om virkningen av en hendelse er betydelig

1. Med hensyn til antallet brukere som er berørt av en hendelse, særlig brukere som er avhengige av tjenesten for å yte egne tjenester som nevnt i artikkel 16 nr. 4 bokstav a) i direktiv (EU) 2016/1148, skal tilbyderen av digitale tjenester kunne anslå enten
   a) antallet berørte fysiske og juridiske personer som det er inngått en avtale om levering av tjenesten med, eller
   b) antallet berørte brukere som har brukt tjenesten, særlig basert på tidligere trafikkdata.
2. Med varigheten av en hendelse som nevnt i artikkel 16 nr. 4 bokstav b) menes tidsrommet fra avbruddet i normal levering av tjenesten med hensyn til tilgjengelighet, autentisitet, integritet eller fortrolighet til tidspunktet for gjenoppretting.
3. Når det gjelder størrelsen på det geografiske området som er berørt av hendelsen, nevnt i artikkel 16 nr. 4 bokstav c) i direktiv (EU) 2016/1148, skal tilbyderen av digitale tjenester kunne fastslå om hendelsen påvirker leveringen av tjenestene i bestemte medlemsstater.
4. Omfanget av driftsforstyrrelser i tjenesten nevnt i artikkel 16 nr. 4 bokstav d) i direktiv (EU) 2016/1148 skal måles med hensyn til én eller flere av følgende egenskaper som påvirkes negativt av en hendelse: dataenes eller de

[2] 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).

tilknyttede tjenestenes tilgjengelighet, autentisitet, integritet eller fortrolighet.

5. Når det gjelder omfanget av virkningen på økonomisk og samfunnsmessig virksomhet nevnt i artikkel 16 nr. 4 bokstav e) i direktiv (EU) 2016/1148, skal tilbyderen av digitale tjenester kunne konkludere, basert på indikasjoner som for eksempel arten av sitt kontraktsforhold med kunden eller, der det er relevant, det potensielle antallet berørte brukere, om hendelsen har forårsaket betydelige materielle eller ikke-materielle tap for brukerne, for eksempel med hensyn til helse, sikkerhet eller skade på eiendom.
6. Ved anvendelse av nr. 1, 2, 3, 4 og 5 skal tilbydere av digitale tjenester ikke være pålagt å innhente tilleggsopplysninger som de ikke har tilgang til.

Artikkel 4

En hendelses betydelige innvirkning

1. En hendelse skal anses å ha en betydelig innvirkning dersom den har ført til minst én av følgende situasjoner:
   a) Tjenesten som leveres av en tilbyder av digitale tjenester, var utilgjengelig i mer enn 5 000 000 brukertimer, der uttrykket brukertimer viser til antallet berørte brukere i Unionen i et tidsrom på 60 minutter.
   b) Hendelsen har ført til tap av integritet, autentisitet eller fortrolighet for lagrede, overførte eller behandlede data eller tilknyttede tjenester som tilbys av eller er tilgjengelige via et nettverks- og informasjonssystem hos tilbyderen av digitale tjenester, og tapet berører flere enn 100 000 brukere i Unionen.
   c) Hendelsen har medført risiko for offentlig orden, offentlig sikkerhet eller tap av menneskeliv.
   d) Hendelsen har forårsaket materiell skade for minst én bruker i Unionen og skaden for denne brukeren overstiger 1 000 000 euro.
2. På grunnlag av opplysninger om beste praksis som er innhentet av samarbeidsgruppen ved utførelsen av sine oppgaver i henhold til artikkel 11 nr. 3 i direktiv (EU) 2016/1148, og drøftingene i henhold til direktivets artikkel 11 nr. 3 bokstav m), kan Kommisjonen revidere tersklene fastsatt i nr. 1.

Artikkel 5

Ikrafttredelse

1. Denne forordningen trer i kraft den 20. dagen etter at den er kunngjort i *Den europeiske unions tidende*.
2. Den får anvendelse fra 10. mai 2018.

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

Utferdiget i Brussel 30. januar 2018.

For Kommisjonen

Jean-Claude Juncker
President

Vedlegg 5

Europaparlaments- og rådsforordning (EU) 2019/881 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 bidrar særlig 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 motstandsdyktighet i deres utforming, 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 oppnå 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.
4) Ved å gjøre relevant informasjon tilgjengelig for offentligheten bidrar Den europeiske

---

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).

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 imidlertid cybersikkerhetsmyndighetenes og de rettshåndhevende myndighetenes kompetanse og politiske innsats 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 cyberresiliens 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 større 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, idet 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 avhengig 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

---

[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).

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.

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 hvert enkelt tilfelle 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. Med det mål å bedre beskytte borgere 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 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

---

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 Byråets 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).

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.

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 cybersikkerhetsutfordringer 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 cybersikkerhetsområdet, 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 det 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

---

[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).

[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).

ENISA skal nå sine mål og samtidig gi ENISA 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.
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 cyberresiliensen. 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 cyberresiliens.
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 «opplære opplæringspersonale» 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 stille ekspertise og rådgivning til rådighet, 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 de 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 direktivet.

32) ENISA bør bidra til innsats på unionsplan i forbindelse med større 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 større cybersikkerhetshendelser og -kriser i Unionen. Denne oppgaven kan omfatte innsamling av relevant informasjon og tilrettelegge 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.

---

14 EUT C 12 av 13.1.2018, s. 1.

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

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 større 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.
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 motstandsdyktighet 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 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 motstandsdyktighet 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 motstandsdyktighet. 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 informasjon- 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, botnet, 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 det 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 luftfartssikkerhetsbyrå (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 myndigheter med ansvar for håndheving av loven og personvernmyndigheter på nasjonalt plan og unionsplan bør kunne være representert i ENISAs rådgivende gruppe. Når ENISA samarbeider med myndigheter som har ansvar for håndheving av loven, om nett- og informasjonssikkerhetsspørsmål som kan påvirke deres arbeid, bør det 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 øke 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 oppmuntres 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 og, der det er relevant, medlemsstatene 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 et samarbeid med Det europeiske forskningsråd, Det europeiske institutt for innovasjon og teknologi og Den europeiske unions institutt for sikkerhetsstudier.

53) ENISA bør regelmessig rådføre seg med standardiseringsorganisasjoner, særlig europeiske standardiseringsorganisasjoner, når

de utarbeider de europeiske cybersikkerhetssertifiseringsordningene.

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 det 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 årlig 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 de tilskuddene 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.

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 marked 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

---

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).

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 vurderingen midtveis 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. Den 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). Selv om den er den viktigste modellen for samarbeid og gjensidig anerkjennelse på området sikkerhetssertifisering, omfatter SOG-IS 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

[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).

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.

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 cybersikkerhetssertifiseringsordningene 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 inndragning 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 cybersikkerhetssertifiseringsordning kunne fastsette tillitsnivåer for europeiske cybersikkerhetssertifikater og EU-samsvarserklæringer utstedt innenfor rammen av den 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 beskyttelse av full stakk- 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 cybersikkerhetssertifisering 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

---

[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).

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.

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 cybersikkerhetssertifiseringsordningene 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-samsvarserklæ-

ringer 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 cybersikkerhetssertifiseringsmyndigheter 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 cybersikkerhetssertifiseringsordninger. 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 cybersikkerhetssertifiseringsordning 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 cybersikkerhetssertifiseringsordninger 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.

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, cyberresiliens og tillit i Unionen, fastsetter denne forordningen

[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).

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, og 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 de rådene og den 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 cyberresiliens 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 cyber-

sikkerhetsområdet 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.

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

[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).

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 å
   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 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) 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, 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 større 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 ordninger for europeisk cybersikkerhetssertifisering («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 når 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

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

med hjemmel i artikkel 2 nr. 1 i vedtektene for tjenestemenn og artikkel 6 i tjenestevilkårene for andre ansatte, som delegerer ansettelsesmyndighetens relevante myndighet til daglig leder og fastsetter vilkårene for når denne delegeringen av myndighet kan avbrytes. Daglig leder kan videredelegere denne myndigheten.

3. Styret kan, dersom særlige omstendigheter krever det, treffe en beslutning om å midlertidig avbryte delegeringen av ansettelsesmyndighetens myndighet til den daglige lederen og den myndigheten som er delegert videre av denne, 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. Styreledereren 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 framdriftsrapport 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 ekspertsammensetninger.
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.
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

[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).

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

[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).

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.
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.
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

[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).

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.

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 Byrået 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.

---

[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).

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 fra det på 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.

[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).

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.

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, over-

førte 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. Når ENISA utarbeider et forslag til ordning, skal det 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 den oversender det forslaget til ordning som er utarbeidet i samsvar med nr. 3, 4 og 5, 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 av 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 cybersikkerhetssertifiseringsordninger 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 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 cybersikkerhetssertifiseringsordningen, inkludert de tilsvarende sikkerhetsfunksjonene og den tilsvarende nøyaktigheten og grundigheten i den vurderingen som IKT-produktet, IKT-tjenesten eller IKT-prosessen skal gjennomgå.
4. Sertifikatet eller EU-samsvarserklæringen skal vise til tekniske spesifikasjoner, standar-

der 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. De 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. De 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. De 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 cybersikkerhets-sertifiseringsordninger

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 de 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 cybersikkerhetskravene 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) Det tidsrommet når 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-proses-

ser 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 rettsakten.
4. I fravær av harmonisert unionsrett kan medlemsstatenes nasjonale rett også fastsette at en europeisk cybersikkerhetssertifiseringsordning 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) Det tidsrommet når sluttbrukerne vil bli tilbudt sikkerhetsstøtte, særlig når det gjelder tilgjengeligheten av cybersikkerhetsrelaterte 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 cybersikkerhetssertifiseringsordning 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 cybersikkerhetssertifiseringsordningene 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 cybersikkerhetssertifiseringsmyndighet 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 cybersikkerhetssertifiseringsmyndigheten 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 cybersikkerhetssertifiseringsordningen, 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 cybersikkerhetssertifiseringsordning, 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 marked bør medlemsstatene informere Kommisjonen og ECCG om eventuelle hensikter om å utarbeide nye nasjonale cybersikkerhetssertifiseringsordninger.

Artikkel 58

Nasjonale cybersikkerhetssertifiserings-myndigheter

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 cybersikkerhetssertifiseringsmyndighetene. 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 cybersikkerhetssertifiseringsmyndighet 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 cybersikkerhetssertifiseringsmyndigheter 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) eventuelt 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 de 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 den 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 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 cybersikkerhetssertifi-

sering, 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 cybersikkerhetssertifiseringsordninger,

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 cybersikkerhetssertifiseringsordning 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 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 overholder 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 deres mandatperiode.

Artikkel 69

Ikrafttredelse

1. Denne forordningen trer i kraft den 20. dagen etter at den er kunngjort i D*en 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 et offentlig foretak eller en offentlig institusjon, skal det sikres og dokumenteres at det er uavhengig og at det ikke foreligger interessekonflikter mellom den nasjonale cybersikkerhetssertifiseringsmyndigheten 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. Det 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, i 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 de 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 personene 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 de 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.

Bestilling av publikasjoner

Departementenes sikkerhets- og serviceorganisasjon
publikasjoner.dep.no
Telefon: 22 24 00 00

Publikasjonene er også tilgjengelige på
www.regjeringen.no

Trykk: Departementenes sikkerhets- og serviceorganisasjon – 05/2023