Høringsnotat

Forslag til forskrift om cybersikkerhetssertifisering

Innhold

1 Høringsnotatets hovedinnhold

Nasjonal sikkerhetsmyndighet (NSM) sender med dette på høring forslag til forskrift om cybersikkerhetssertifisering. Forskriften gjennomfører den såkalte Cybersikkerhetsforordningen i norsk rett. Høringen gjennomføres på oppdrag fra Justis- og beredskapsdepartementet.

Forordning (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 vedtatt 17. april 2019 og trådte i kraft i EU 27. juni 2019. Forordningen ble vedtatt i EØS-komiteen 3. februar 2023 med artikkel 103-forbehold, og har vært gjeldende i EØS-området fra 1. august 2024.

Cybersikkerhetsforordningen er et ledd i EUs strategi for å etablere en felles ramme for å håndtere cybersikkerhetsutfordringer i EU/EØS. Målet med forordningen er å heve det generelle cybersikkerhetsnivået i medlemslandene.

Cybersikkerhetsforordningen del I og II om ENISA er allerede gjennomført i norsk rett, og høringsnotatet omhandler derfor implementering av forordningens del III om cybersikkerhetssertifisering.

Cybersikkerhetsforordningen del III etablerer et felles europeisk rammeverk for frivillig cybersikkerhetssertifisering av IKT-produkter, IKT-tjenester og IKT-prosesser.

Den 19. desember 2024 ble endringsforordning (EU) 2025/37 vedtatt, som innebærer at rammeverket for cybersikkerhetssertifisering utvides til å inkludere sertifiseringsordninger for administrerte sikkerhetstjenester. Endringsforordningen trådte i kraft i EU 4. februar 2025, og er ikke tatt inn i EØS-avtalen.

De konkrete sertifiseringsordningene vil bli vedtatt på et senere tidspunkt som gjennomføringsrettsakter til forordningen. Sertifiseringsordningene skal bidra til å dokumentere at IKT-produkter, IKT-tjenester, IKT-prosesser og administrerte sikkerhetstjenester oppfyller fastsatte sikkerhetskrav. På nåværende tidspunkt er det for tidlig å si noe om innholdet i og konsekvensene av de fremtidige sertifiseringsordningene. Det understrekes i denne forbindelse at sertifiseringsordningene vil være gjenstand for en alminnelig utrednings- og høringsprosess.

Cybersikkerhetsforordningen krever at medlemsstatene utpeker én eller flere nasjonale cybersikkerhetssertifiseringsmyndigheter.

Et sentralt punkt i høringsnotatet er derfor hvilken forvaltningsstruktur som er mest hensiktsmessig, både for å sikre tilstrekkelig gjennomføring av rammeverket som følger av cybersikkerhetsforordningen, og samtidig legge til rette for en fleksibel ordning for fremtidige sertifiseringsordninger.

I høringsnotatet foreslår NSM at det utpekes én nasjonal cybersikkerhetssertifiseringsmyndighet når forskriften fastsettes. Dette for å sikre at gjennomføringen blir korrekt. Den nasjonale cybersikkerhetssertifiseringsmyndighet vil ha et overordnet ansvar for å forvalte forordningen. I høringsnotatet kapittel 5

beskrives flere departementer og underliggende virksomheter som aktuelle, og vi ber derfor om høringsinstansenes innspill og synspunkter på dette.

I høringsnotatet foreslås også en fleksibel forvaltningsstruktur som beskrevet i kapittel 5. En fleksibel forvaltningsstruktur innebærer at det for fremtidige sertifiseringsordninger, vil utpekes flere nasjonale cybersikkerhetssertifiseringsmyndigheter. Dette avhenger av hvem som vurderes som mest hensiktsmessig til å ha myndighetsoppgaver knyttet til den konkrete ordningen.

Etter NSMs vurdering vil en fleksibel forvaltningsstruktur sikre at regelverkets formål oppnås, i tillegg til å gi en tilstrekkelig fleksibilitet med hensyn til kommende sertifiseringsordninger. En fleksibel forvaltningsstruktur vil også løse utfordringen ved at det i dag ikke er ett organ som innehar fagekspertise på alle kommende sertifiseringsordninger.

I høringsnotatets kapittel 6.5 beskrives administrative sanksjoner som kan ilegges ved manglende overholdelse av forordningen og sertifiseringsordningene, herunder pålegg, tvangsmulkt og overtredelsesgebyr.

Cybersikkerhetsforordningen foreslås gjennomført ved inkorporering i ny forskrift om cybersikkerhetssertifisering, med hjemmel i lov om digital sikkerhet § 19.

Ettersom endringsforordningen åpner for sertifisering av administrerte sikkerhetstjenester under rammeverket for sertifisering av IKT-produkter, IKT-tjenester og IKT-prosesser, er det behov for å endre digitalsikkerhetsloven §§ 1 og 19 for å sikre tilstrekkelig hjemmelsgrunnlag til å gjennomføre endringsforordningen som forskrift. Det foreslås derfor endringer i digitalsikkerhetsloven §§ 1 og 19, samtidig som det foreslås at endringsforordningen inkorporeres i norsk rett ved forskrift. Dette vil bli fulgt opp i et eget spor og følge en alminnelig lovprosess.

Avslutningsvis foreslås det at ekom-forskriften § 2-11 oppheves, slik at cybersikkerhetsforordningen gjennomføres samlet i ny forskrift om cybersikkerhetssertifisering.

2 Bakgrunn

2.1 Cybersikkerhetsforordningen

Cybersikkerhetsforordningen etablerer et nytt rammeverk for sikkerhetssertifisering av IKT-produkter, IKT-tjenester og IKT-prosesser, jf. Art. 1 nr.1 bokstav b.

Cybersikkerhetsforordningen er en del av Kommisjonens «Cyber Security package» som ble lansert i 2017. Kommisjonen har slått fast at EU står overfor betydelige digitale sikkerhetsutfordringer. Kommisjonen viste til at antallet utpressingssaker økte med 300 % mellom 2015 og 2017. Det ble også vist til at de økonomiske konsekvensene av IKT-kriminalitet ble femdoblet fra 2013 til 2017, og at de kan ytterligere firedobles innen 2019.

Cybersikkerhetsforordningen har som formål å sikre et velfungerende indre marked med et høyt nivå av cybersikkerhet, cyberrobusthet og tillit innad i EU/EØS, jf.

forordningen artikkel 1. Etablering av et nytt rammeverk for opprettelse av europeiske cybersikkerhetssertifiseringsordninger skal bidra til å oppnå dette formålet.

Cybersikkerhetsforordningen skal bedre vilkårene for det indre markedets virkemåte og muliggjøre en harmonisert tilnærming på unionsplan til europeiske cybersikkerhetssertifiseringsordninger, jf. artikkel 46 nr. 1. Forordningen inngår som et element i EUs digitaliseringsstrategi, som har som formål å stimulere til økonomisk vekst og øke EUs konkurransekraft. I fortalen punkt 65 fremkommer det at det digitale indre markedet bare kan ha framgang hvis allmennheten har tillit til at slike produkter, tjenester og prosesser har et visst nivå av cybersikkerhet.

Det følger av fortalen punkt 69 at forordningen har et dobbelt formål. For det første skal den øke tilliten til IKT-produkter, IKT-tjenester og IKT-prosesser som er blitt sertifisert i samsvar med sertifiseringsordninger under rammeverket. Bruk av sertifiseringsordninger skal bidra til å styrke privatpersoners, organisasjoners og virksomheters tillit til IKT-produktene/tjenestene/prosessene, ved at de får tilstrekkelig informasjon om cybersikkerheten og også øke bevisstheten om cybersikkerhetsspørsmål.

Det andre formålet er å redusere kostnadene for foretak som har virksomhet i det digitale indre markedet. Cybersikkerhetsforordningen skal bidra til å forhindre at det oppstår motstridende eller overlappende nasjonale cybersikkerhetssertifiseringsordninger, som ikke samspiller effektivt med det indre marked. Uten felles sertifiseringsordninger i det indre markedet, er sertifikater utstedt av en nasjonal cybersikkerhetssertifiseringsmyndighet i én stat i prinsippet ikke anerkjent i andre medlemsstater. For å delta i nasjonale anskaffelsesprosesser der det har vært krav om sertifisering har foretak vært nødt til å sertifisere sine IKT-produkter, IKT-tjenester og IKT-prosesser i hver enkelt medlemsstat der de har virksomhet, noe som øker virksomhetenes kostnader. En felles sertifiseringsordning kan bidra til å styrke det indre markedet ved at det kun er nødvendig med én sertifisering, og det vil gjøre det mulig for virksomheter å konkurrere i alle anskaffelser der det stilles krav til IKT-sertifisering.

I EU er det gjort en viss innsats for å sikre gjensidig anerkjennelse av sertifikater i Unionen, men i fortalen til cybersikkerhetsforordningen omtales dette som bare delvis vellykket. Det følger av fortalen punkt 68 at «[d]et viktigste eksempelet i denne forbindelse er avtalen om gjensidig anerkjennelse (MRA) fra gruppen av høyere tjenestemenn for informasjonssystemers sikkerhet (SOG-IS). SOG-IS er den viktigste modellen for samarbeid og gjensidig anerkjennelse på området sikkerhetssertifisering, men omfatter bare noen av medlemsstatene. Dette har begrenset SOG-IS-avtalens effektivitet med hensyn til det indre markedet». Videre følger det av fortalen punkt 69 at det derfor er «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.» Norge har tilsluttet seg sertifiseringsordningene Common Criteria Recognition Arrangement (CCRA) og SOG-IS Mutual Recognition Arrangement (SOG-IS MRA).

Sertifiseringsordningene vil bygge på eksisterende nasjonale og internasjonale sertifiseringsordninger.

2.2 Endringer i cybersikkerhetsforordningen - administrerte sikkerhetstjenester

I desember 2024 vedtok EU endringer i cybersikkerhetsforordningen ved å utvide forordningens virkeområde til å inkludere «administrerte sikkerhetstjenester».

Endringen innebærer at rammeverket for cybersikkerhetssertifisering utvides til å inkludere sertifiseringsordninger for administrerte sikkerhetstjenester. Som følge av dette vil også ENISAs mandat og oppgaver utvides til å omfatte sertifiseringsordninger for administrerte sikkerhetstjenester. Arbeidet med utvikling av en sertifiseringsordning for administrerte sikkerhetstjenester (EUMSS) er allerede i gang, og NSM følger dette arbeidet.

Administrerte sikkerhetstjenester består i å utføre, eller yte bistand til, aktiviteter knyttet til håndtering av cybersikkerhetsrisiko. Slike tjenester har fått økende betydning ved forebygging og håndtering av hendelser.

I fremleggelsen av forslaget til forordning viste EU-kommisjonen til konklusjoner fra Europarådet av 23. mai 2023 hvor EU og medlemsstatene ble oppfordret til å styrke innsatsen for å øke det generelle nivået av cybersikkerhet, for eksempel ved å legge til rette for fremveksten av pålitelige cybersikkerhetstjenesteleverandører.

Kommisjonen uttaler at sertifisering av administrerte sikkerhetstjenester er et effektivt virkemiddel for å sikre tillit til kvaliteten på disse tjenestene og dermed lette etableringen av en pålitelig europeisk cybersikkerhetsindustri. Leverandører av administrerte sikkerhetstjenester kommer bl.a. til å spille en viktig rolle i EUs cybersikkerhetsreserve, hvis gradvise oppbygging understøttes av forordning (EU) 2025/38 (cybersolidaritetsforordningen). De relevante cybersikkerhetstjenestene som leveres av såkalte «pålitelige leverandører» etter cybersolidaritetsforordningen tilsvarer de «administrerte sikkerhetstjenestene» i dette forslaget.

2.3 Aktuelle sertifiseringsordninger under rammeverket

Det er i dag etablert én sertifiseringsordning under rammeverket, mens omfanget av kommende sertifiseringsordninger ellers er ukjent.

Den første sertifiseringsordningen som er etablert i EU under rammeverket for cybersikkerhetssertifisering er European Common Criteria certification scheme (forkortet EUCC). Den er gjennomført i EU ved forordning (EU) 2024/482, og etablerer et rammeverk for cybersikkerhetssertifisering av IKT-produkter. EUCC bygger på avtalen om gjensidig anerkjennelse av sertifikater (SOG-IS MRA). Forordningen er under vurdering og er ikke tatt inn EØS-avtalen ennå, og vil derfor bli sendt på høring på et senere tidspunkt.

Det er flere EU-regelverk som henviser til at det vil bli etablert sertifiseringsordninger under cybersikkerhetsforordningen, for at virksomheter som underlegges annet EU-regelverk på forskjellig vis skal eller kan benytte sertifiseringsordninger under cybersikkerhetsforordningen.

Cyber Resilience Act (CRA) fastsetter krav til cybersikkerhet i produkter, og det skal frem mot 2027 utvikles 48 harmoniserte standarder for samsvarsvurdering av kravene til cybersikkerhet. Regelverket viser til samspill med sertifiseringsordninger under cybersikkerhetsforordningen og det pågår konkret arbeid med å tilrettelegge for samspill mellom EUCC og CRA. Annet regelverk som forutsetter at det etableres sertifiseringsordninger under cybersikkerhetsforordningen er KI-forordningen, eIDAS-forordningen 2.0 og Cyber Solidarity Act. I norsk forvaltning har Nasjonal kommunikasjonsmyndighet (Nkom) ansvar for å følge utviklingen av CRA, i tillegg til å ha fått det overordnede ansvaret for å følge opp og koordinere arbeidet med KI-forordningen i Norge. Nkom fører også tilsyn etter lov om elektroniske tillitstjenester som gjennomfører eIDAS-forordningen.

SERTIT er organisert under Nasjonal sikkerhetsmyndighet (NSM) og innehar rollen som samsvarsvurderingsorgan og er ansvarlig for drift av den norske sertifiseringsordningen for IT-sikkerhet. SERTIT representerer Norge i SOG-IS og CCRA og utsteder CC-sertifikater under SOG-IS og CCRA. Gjensidig anerkjennelse innen CCRA er basert på en avtale mellom myndighetene i de deltagende nasjonene. Avtalen fastsetter at partene har tillit til sertifikater som er utstedt under kontroll av myndighetsorganet som er med i arrangementet. En ren privat sertifikatutstedelse er ikke tillatt under CCRA.

Sertifiseringsordninger som er under utvikling under rammeverket er en sertifiseringsordning for 5G-nettverk og relaterte teknologier (EU5G), en sertifiseringsordning for sky-tjenester (EUCS), en sertifiseringsordning for digital lommebok (EUDI Wallets) og en sertifiseringsordning for administrerte sikkerhetstjenester (EUMSS).

3 Gjeldende rett

Cybersikkerhetsforordningen del I og II er gjennomført i forskrift om elektroniske kommunikasjonsnett og elektroniske kommunikasjonstjenester (ekomforskriften) § 2-11. Del I inneholder generelle bestemmelser om formål, virkeområde og definisjoner av begreper, mens del II omhandler ENISA. Cybersikkerhetsforordningens del III om rammeverk for cybersikkerhetssertifisering av IKT-produkter, IKT-tjenester, IKT-prosesser og administrerte sikkerhetstjenester er ikke gjennomført i norsk rett.

Digitalsikkerhetsloven skal etter § 1 første punktum 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.

Digitalsikkerhetslovens formål er blant annet å legge til rette for sikkerhet i IKT-produkter, IKT-tjenester og IKT-prosesser, jf. lovens § 1. I følge forarbeidene skal loven legge til rette for å gjennomføre cybersikkerhetsforordningen, jf. Prop. 109 LS (2022-2023) s. 55.

Etter digitalsikkerhetsloven § 18 bokstav f kan Kongen gi forskrift om gjennomføring av forpliktelser som følger av EØS-avtalen og andre internasjonale avtaler, og som understøtter lovens regler eller formål.

Digitalsikkerhetsloven § 19 gir Kongen hjemmel til å gi forskrift om sikkerhetssertifisering av IKT-produkter, -tjenester og -prosesser for å gjennomføre forpliktelser etter EØS-avtalen. Med «sikkerhetssertifisering» menes cybersikkerhetssertifisering slik det er angitt i cybersikkerhetsforordningen, jf. særmerknaden til Prop. 109 LS (2022-2023).

Digitalsikkerhetsloven § 19 kan benyttes til å fastsette supplerende og utfyllende regler til cybersikkerhetsforordningen når det er aktuelt. Den vil også kunne benyttes til å gjennomføre delegerte rettsakter fra Kommisjonen innen sikkerhetssertifisering.

Det finnes på enkelte samfunnsområder krav om godkjenning av IKT-produkter, men det er ikke identifisert generelle nasjonale sertifiseringsordninger for IKT-produkter, -tjenester og -prosesser i Norge, som dekker cybersikkerhetsforordningens virkeområde.

Forordning (EU) 2016/679 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (personvernforordningen) artikkel 42 og 43 regulerer personvernsertifisering. Dette kan være en måte for virksomheter å demonstrere etterlevelse av personvernregelverket på. Personvernforordningen artikkel 32 setter blant annet krav til IKT-sikkerhet ved systemer som behandler personopplysninger. Datatilsynet har etablert mekanismer for at virksomheter kan søke om å bli et akkreditert sertifiseringsorgan og at virksomheter kan søke om å få godkjent kriterier i en personvernsertifiseringsordning. Per i dag er det ingen norske virksomheter som har benyttet seg av disse mulighetene.

Forordning (EF) nr. 765/2008 om akkreditering og markedstilsyn gjelder hovedsakelig det harmoniserte vareområdet. Det harmoniserte vareområdet er varer der EU har utarbeidet rettsakter med vesentlige krav som berører helse-, miljø- og/eller sikkerhetsaspekter. De tekniske kravene spesifiseres i det som kalles harmoniserte standarder som utarbeides av standardiseringsorganer på bakgrunn av rettsaktene. En vare som er produsert i samsvar med en harmonisert standard, vil i praksis anses for å oppfylle kravene i rettsakten, men det er som hovedregel ikke obligatorisk å følge en standard.

For noen varegrupper er det tilstrekkelig med en intern kontroll av varens samsvar med kravene i harmonisert EØS-regelverk. For andre varegrupper stilles det krav om at en uavhengig tredjepart foretar en vurdering av varens samsvar med kravene. Denne samsvarsvurderingen utføres da av et teknisk kontrollorgan.

Forordningen om akkreditering og markedstilsyn gir regler om akkreditering, markedstilsyn, kontroll av varer fra tredjeland og CE-merking. Felles regler for akkreditering skal bidra til økt tillit til akkrediterte samsvarsvurderingsorganers kompetanse, og dermed økt tillit til attester og testrapporter de utsteder. Forordningen fastsetter minimumskrav til EØS-statenes organisering av det nasjonale arbeidet med markedstilsyn.

EØS-vareloven gjennomfører forordning 765/2008 om akkreditering og markedstilsyn. Forordning 765/2008 er en del av «EUs varepakke» som er et regelverk for handel med varer. Varepakkens formål er at varer i markedet oppfyller krav som sikrer et høyt nivå av vern av offentlige interesser som helse, sikkerhet og

miljø, samtidig som det frie varebytte ikke blir begrenset i større grad enn det som er tillatt etter EØS-lovgivningen.

I henhold til EØS-vareloven § 3 er Norsk Akkreditering nasjonalt akkrediteringsorgan i Norge.

Lov om tekniske kontrollorgan som har til oppgåve å gjennomføre samsvarsvurderingar (heretter TKO-loven) gjelder etter § 1 «utpeiking av og verksemda til tekniske kontrollorgan som driv samsvarsvurderingar etter reglar som er gitt til gjennomføring av EØS-avtalen». Ved gjennomføring av cybersikkerhetsforordningen vil TKO-loven komme til anvendelse. Loven gir regler for utpeking av samsvarsvurderingsorganer, og reglene for organene. TKO-loven forvaltes av Nærings- og fiskeridepartementet.

4 Cybersikkerhetsforordningen del III

4.1 Europeisk rammeverk for cybersikkerhetssertifisering

Etter cybersikkerhetsforordningen artikkel 1 nr. 1 bokstav b etablerer forordningen et europeisk rammeverk for cybersikkerhetssertifisering av IKT-produkter, IKT-tjenester, IKT-prosesser og administrerte sikkerhetstjenester, kalt «European cybersecurity certification framework» (forkortet ECCF).

Forordningen innfører ikke operasjonelle sertifiseringsordninger. Sertifiseringsordningene vil bli utarbeidet og vedtatt i etterkant som gjennomføringsrettsakter til forordningen på senere tidspunkt. Når en sertifiseringsordning under rammeverket gjennomføres i nasjonal rett skal nasjonale sertifiseringsordninger som omfattes av den europeiske sertifiseringsordningen opphøre, jf. artikkel 57 nr. 1. Medlemsstatene kan heller ikke innføre nye nasjonale sertifiseringsordninger for noe som allerede omfattes av en etablert sertifiseringsordning under rammeverket for cybersikkerhetssertifisering, jf. artikkel 57 nr. 2. Eksisterende nasjonale sertifikater som allerede var utstedt før en ny sertifiseringsordning under rammeverket er etablert, vil forbli gyldige fram til sertifiseringens utløpsdato, jf. artikkel 57 nr. 4.

Det er i utgangspunktet frivillig for virksomheter å benytte sertifiseringsordningene, med mindre noe annet fastsettes i EØS-retten eller nasjonal rett, jf. artikkel 56 nr. 2 og fortalen punkt 91. På enkelte områder kan det i framtiden bli obligatorisk med sertifisering for visse IKT-produkter, IKT-tjenester, IKT-prosesser og administrerte sikkerhetstjenester, jf. fortalen punkt 92. Slike påbud kan fastsettes i de enkelte sertifiseringsordningene under forordningen, i annet EØS-regelverk eller i nasjonal rett.

Tilbydere av sertifiserte IKT-produkter, -tjenester eller -prosesser skal i henhold til artikkel 55 offentliggjøre enkelte opplysninger om cybersikkerheten, 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.

Ved å ha felles sertifiseringsordninger på tvers av alle EØS-stater, vil det være lettere for virksomheter å informere forbrukere, næringsliv og offentlig sektor om cybersikkerheten til deres IKT-produkter, -tjenester, og -prosesser på tvers av medlemsstatene. Virksomhetene kan også lettere delta i offentlige anbudsprosesser i hele EØS-området, siden det ikke lenger kan stilles krav om nasjonale sertifiseringer. Begge deler vil kunne styrke virksomhetenes markedsposisjon om de har sertifiserte IKT-produkter, -tjenester, -prosesser og fremme virksomhetens salg i hele EØS-området. Dette kan være et insitament for virksomhetene til å få sertifisert sine IKT-produkter. -tjenester, -prosesser. Når flere virksomheter sørger for å oppfylle krav til digital sikkerhet for å bli sertifisert, kan dette bidra til styrket digital sikkerhet.

4.2 Saklig virkeområde

Forordningen etablerer et rammeverk for sertifiseringsordninger for «IKT-produkter», «IKT-tjenester», «IKT-prosesser» og «administrerte sikkerhetstjenester».

Forordningens artikkel 2 definerer begrepene. Et *IKT-produkt* er «et element eller en gruppe av elementer i et nett- eller informasjonssystem». En *IKT-tjeneste* er «en tjeneste som helt eller hovedsakelig består av overføring, lagring, innhenting eller behandling av informasjon ved hjelp av nett- og informasjonssystemer». En *IKT-prosess* er «et sett av aktiviteter som utføres for å utforme, utvikle, levere eller vedlikeholde et IKT-produkt eller en IKT-tjeneste». Videre er «*administrert sikkerhetstjeneste*» definert som en tjeneste levert til en tredjepart som består i å utføre eller yte bistand til aktiviteter knyttet til håndtering av cybersikkerhetsrisiko, for eksempel knyttet til hendelseshåndtering, rådgivning, revisjon, inkludert ekspertrådgivning knyttet til teknisk støtte. Det vises til forordningen og endringsforordningen for en fullstendig oversikt over hva som ligger i begrepene.

Det er innenfor disse fire områdene at forordningen legger opp til at Kommisjonen senere skal utgi sertifiseringsordninger.

Det følger av artikkel 1 nr. 2 at rammeverket for cybersikkerhetssertifisering får anvendelse uten at det berører bestemmelser om sertifisering som følger av annet EU-regelverk. Det kan også leses ut av fortalens punkt 74 at bestemmelsene i forordningen ikke bør berøre den EU-retten som inneholder særlige regler om sertifisering av IKT-produkter, IKT-tjenester, IKT-prosesser og administrerte sikkerhetstjenester. Forordningen viser særlig til at bestemmelser om sertifiseringsmekanismer for oppfyllelse av personvernforordningen faller utenfor virkeområdet.

Videre følger det av art. 1 nr. 3 at forordningen ikke berører medlemsstatenes myndighetsområder med hensyn til aktiviteter som gjelder offentlig sikkerhet, forsvar, nasjonal sikkerhet og statens aktiviteter på det strafferettslige området. Forordningen er derfor ikke til hinder for at Norge vedtar eller opprettholder nasjonale cybersikkerhetssertifiseringsordninger for formål knyttet til nasjonal sikkerhet.

Sertifiseringsordninger som drives av privat næringsliv og andre aktører enn staten omfattes heller ikke av forordningen, jf. fortalens punkt 73.

4.3 Etablering av sertifiseringsordninger

Det følger av artikkel 46 nr. 2 at «[d]en europeiske rammen for cybersikkerhetssertifisering skal fastsette en mekanisme for opprettelse av europeiske cybersikkerhetssertifiseringsordninger og for å sikre at IKT-produkter, IKT-tjenester og IKT-prosesser som er vurdert i samsvar med slike ordninger, oppfyller særlige sikkerhetskrav som har som mål å beskytte tilgjengeligheten, autentisiteten, integriteten eller fortroligheten til lagrede, overførte eller behandlede data eller til funksjoner eller tjenester som tilbys i eller er tilgjengelige via disse produktene, tjenestene og prosessene gjennom hele deres livssyklus.» Sertifiseringsordningene skal utformes slik at de vil bidra til å oppnå de relevante sikkerhetsmålene som er opplistet i artikkel 51.

Rammeverket gir Kommisjonen myndighet til å fastsette rettsakter som vil implementere de konkrete sertifiseringsordningene med utfyllende bestemmelser innenfor ulike produkter, tjenester og prosesser, jf. artikkel 49 nr. 7.

Forordningen legger opp til at kandidater til de europeiske sertifiseringsordningene skal utarbeides av den europeiske unions cybersikkerhetsbyrå (ENISA) primært etter anmodning fra Kommisjonen basert på Kommisjonens arbeidsprogram, jf. artikkel 48. Kommisjonen skal ha et løpende arbeidsprogram for europeisk cybersikkerhetssertifisering som skal angi de strategiske prioriteringene for framtidige europeiske cybersikkerhetssertifiseringsordninger, jf. artikkel 47.

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.

4.4 Samsvarsvurdering

Begrepet «samsvarsvurdering» er definert i artikkel 2 nr. 17, der bestemmelsen viser til definisjonen i forordning 765/2008 om akkreditering og markedstilsyn, som i Norge er gjennomført i EØS-vareloven. Det følger av forordningens artikkel 2 nr. 12 at samsvarsvurdering er «en prosess for å fastslå om nærmere angitte krav til et produkt, en prosess, en tjeneste, et system, en person eller et organ er oppfylt». En samsvarsvurdering og sertifisering etter denne forordningen utgjør derfor 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, jf. fortalen punkt 77. Det utgjør følgelig ikke en garanti for at sertifiserte IKT-produkter, IKT-tjenester og IKT-prosesser er cybersikre.

Samsvarsvurdering etter rammeverket kan gjennomføres enten ved en egenvurdering av samsvar eller av samsvarsvurderingsorganer. Det er den enkelte sertifiseringsordning som spesifiserer om egenvurdering tillates eller ikke, men det er kun sertifiseringsordninger for tillitsnivået «grunnleggende» som kan tillate egenvurdering av samsvar. Se mer om tillitsnivåer i punkt **Error! Reference source not found.**.

Egenvurdering av samsvar er regulert i artikkel 53. Dette innebærer at produsenter og leverandører har mulighet til å utføre en vurdering av om deres eget/egen produkt/tjeneste/prosess oppfyller kravene i en sertifiseringsordning. Det vil si at det er tilstrekkelig at produsenten eller leverandøren selv utfører alle kontrollene for å sikre at produktene/tjenestene/prosessene er i samsvar med sertifiseringsordningen, jf. fortalen nr. 79. Ved egenvurdering må produsent eller leverandør utstede en erklæring om at de oppfyller kravene i en sertifiseringsordning, og gjøre all relevant dokumentasjon tilgjengelig for den nasjonale cybersikkerhetssertifiseringsmyndigheten. En kopi av EU-samsvarserklæringen skal fremlegges for den nasjonale cybersikkerhetssertifiseringsmyndigheten og ENISA. En egenerklæring om samsvar skal anerkjennes i alle medlemsstater i EØS.

Ved utstedelse og undertegning av en EU-samsvarserklæring påtar produsenten eller leverandøren av IKT-produktet, IKT-tjenesten eller IKT-prosessen seg ansvaret for at IKT-produktene, IKT-tjenestene eller IKT-prosessene oppfyller de lovfestede kravene fastsatt av den europeiske cybersikkerhetssertifiseringsordningen.

Dersom egenvurdering ikke tillates må sertifisering gjennomføres av samsvarsvurderingsorganer. For sertifikater som viser til tillitsnivåene «grunnleggende» og «betydelig» er hovedregelen at sertifisering kan gjøres av alle akkrediterte samsvarsvurderingsorganer iht. artikkel 60, jf. artikkel 56 nr. 4.

Unntaksvis kan enkelte sertifiseringsordninger kreve at sertifisering må utføres av et offentlig organ som enten er en nasjonal cybersikkerhetssertifiseringsmyndighet eller et annet offentlig organ som er akkreditert som et samsvarsvurderingsorgan i samsvar med artikkel 60 nr. 1, jf. artikkel 56 nr. 5.

For sertifiseringsordninger på tillitsnivå «høyt», krever artikkel 56 nr. 6 at sertifikatet bare kan utstedes av enten en nasjonal cybersikkerhetssertifiseringsmyndighet, eller av et annet samsvarsvurderingsorgan etter forhåndsgodkjenning for hvert enkelt sertifikat eller en generell delegering av oppgaven fra den nasjonale cybersikkerhetssertifiseringsmyndigheten til det andre organet, jf. artikkel 56 nr. 6 bokstav a og b.

For produsenter og leverandører av IKT-produkter, IKT-tjenester eller IKT-prosesser er det valgfritt hvilket samsvarsvurderingsorgan de kan sende søknad om sertifisering til, jf. fortalen punkt 97. Dersom det ikke finnes samsvarsvurderingsorganer i det landet leverandøren eller produsenten holder til i, kan de derfor sende søknad om sertifisering til samsvarsvurderingsorganer etablert i andre land i EØS-området. Dette gjelder også dersom det stilles krav om at sertifisering må utøves av offentlig myndighet eller en nasjonal cybersikkerhetssertifiseringsmyndighet, slik at disse myndighetene skal sertifisere IKT-produkter, IKT-tjenester eller IKT-prosesser fra produsenter og leverandører i andre land.

Ved søknad om sertifisering skal søkeren gjøre all informasjon som er nødvendig for å utføre sertifiseringen, tilgjengelig for samsvarsvurderingsorganet, jf. artikkel 56 nr. 7. Innehaveren av et europeisk cybersikkerhetssertifikat er også pålagt å informere samsvarsvurderingsorganet 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, jf. artikkel 56 nr. 8.

Når en leverandør/produsent er blitt sertifisert eller har utstedt en egenerklæring om samsvar, får de en plikt til å offentliggjøre tilleggsinformasjon som beskrevet i artikkel 55, for å ivareta sluttbrukere av deres produkter/tjenester/systemer. Begrepet «offentliggjøre» betyr at informasjonen må gjøres tilgjengelig for allmennheten. Det er for eksempel ikke tilstrekkelig at informasjonen som beskrevet i artikkel 55 kun blir tilgjengelig gjennom individuelle kontrakter mellom virksomhet og kunde. Det kan følge av den enkelte sertifiseringsordning hvilket format eller hvilke prosedyrer virksomheten må følge når de offentliggjør informasjon etter artikkel 55, jf. artikkel 54 nr. 1 bokstav v.

4.5 Samsvarsvurderingsorganer

Begrepet «samsvarsvurderingsorgan» er definert i artikkel 2 nr. 18, der bestemmelsen viser til definisjonen i forordning EF nr. 765/2008 om akkreditering og markedstilsyn artikkel 2 nr. 13. Et samsvarsvurderingsorgan er «et organ som utøver samsvarsvurderingsvirksomhet, herunder kalibrering, prøving, sertifisering og inspeksjon». Organet kan være både private og offentlige virksomheter. Artikkel 60 nr. 1 bestemmer at samsvarsvurderingsorganene skal akkrediteres av de nasjonale akkrediteringsorganer som er utpekt etter forordningen om akkreditering og markedstilsyn. For at en virksomhet kan bli akkreditert må organet oppfylle kravene som følger av vedlegget til forordningen. En akkreditering kan ha en varighet på høyst fem år, men kan fornyes på samme vilkår om organet fortsatt oppfyller kravene, jf. artikkel 60 nr. 4.

Etter forordningen om akkreditering og markedstilsyn artikkel 5 nr. 3 skal akkrediteringsorganet føre tilsyn med de organer de har akkreditert. Dette er for å sikre at samsvarsvurderingsorganene oppfyller vilkårene for en akkreditering.

Det følger av forordningen artikkel 60 nr. 4 at nasjonale akkrediteringsorganer «skal treffe alle egnede tiltak innenfor en rimelig frist for å 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».

Nasjonale cybersikkerhetssertifiseringsmyndigheter må akkrediteres på samme vilkår som samsvarsvurderingsorganer dersom de skal utstede sertifikater iht. artikkel 56 nr. 5 bokstav a eller nr. 6.

En sertifiseringsordning kan fastsette særlige eller ytterligere krav til samsvarsvurderingsorganer, jf. artikkel 54 nr. 1 bokstav f. Dersom det stilles slike krav, kreves det at samsvarsvurderingsorganet blir godkjent av den nasjonale cybersikkerhetssertifiseringsmyndigheten for å kunne utføre oppgavene innenfor disse ordningene, jf. artikkel 60 nr. 3. En slik godkjenning kan begrenses, midlertidig oppheves eller trekkes tilbake dersom samsvarsvurderingsorganet overtrer kravene i forordningen, jf. artikkel 58 nr. 7 bokstav e.

Alle akkrediterte, og eventuelt godkjente samsvarsvurderingsorganer i henhold til artikkel 60 nr. 3 skal meldes til Kommisjonen, jf. artikkel 61 nr. 1. I

gjennomføringsforordning av 18. desember 2024 vedtok Kommisjonen at meldingen skal gjøres gjennom det elektroniske verktøyet som benyttes under EUs varepakke, som er «NANDO». En slik melding har likevel ikke betydning for gyldigheten av sertifikatene et akkreditert og eventuelt godkjent samsvarsvurderingsorgan utsteder. NSM forstår det som at det avgjørende for gyldigheten av utstedte sertifikater er kun at organet var akkreditert og evt. godkjent av en cybersikkerhetssertifiseringsmyndigheter iht. artikkel 60 nr. 3. Dersom en cybersikkerhetssertifiseringsmyndigheter for eksempel bruker lang tid på å melde inn et samsvarsvurderingsorgan til Kommisjonen, skal ikke det ha betydning for organets muligheter til å utstede sertifikater. Dette betyr også at EØS-medlemsstatene plikter å anerkjenne sertifikater utstedt fra samsvarsvurderingsorganer som ikke enda er meldt til Kommisjonen. Akkrediterte samsvarsvurderingsorganer kan sertifisere alle produsenter eller leverandører av IKT-produkter, IKT-tjenester eller IKT-prosesser fra alle stater i EØS.

Cybersikkerhetsforordningens vedlegg opplister krav til samsvarsvurderingsorganer som ønsker å bli akkreditert. Et samsvarsvurderingsorgan skal blant annet oppfylle kravene til den relevante standarden for samsvarsvurderingsorganer under forordningen om akkreditering og markedstilsyn, jf. vedlegget punkt 19. Den relevante standarden er ISO/IEC 17065, som sier at organet skal iverksette passende tiltak dersom krav ikke etterleves. Et slikt tiltak kan være å trekke tilbake sertifikatet de har utstedt.

4.6 Tillitsnivåer

Cybersikkerhetssertifiseringsordninger kan angi ett eller flere tillitsnivåer, jf. artikkel 52 nr. 1. Et «tillitsnivå» er definert som et grunnlag for tillit til at et IKT-produkt, en IKT-tjeneste eller en IKT-prosess oppfyller sikkerhetskravene i en bestemt europeisk cybersikkerhetssertifiseringsordning, som angir på hvilket nivå et IKT-produkt, en IKT-tjeneste eller en IKT-prosess er blitt vurdert, men måler ikke i seg selv det aktuelle IKT-produktets, IKT-tjenestens eller IKT-prosessens sikkerhet, jf. artikkel 2 nr. 21.

Det følger av fortalen punkt 86 at «[t]illitsnivået 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 ordningen. Hvert europeisk cybersikkerhetssertifikat kan vise til ett av tillitsnivåene «grunnleggende», «betydelig» eller «høyt» […] 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».

Den enkelte sertifiseringsordningen vil fastsette sikkerhetskravene som svarer til tillitsnivået, inkludert de tilsvarende sikkerhetsfunksjonene og den tilsvarende

nøyaktigheten og grundigheten i vurderingen som IKT-produktet, IKT-tjenesten eller IKT-prosessen skal gjennomgå, jf. artikkel 52 nr. 3.

«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* (egen utheving). 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,» jf. art. 52 nr. 5.

For tillitsnivået «betydelig» må de samme kravene som gjelder for «grunnleggende» oppfylles, i tillegg til ytterligere krav, jf. fortalen punkt 89. For «betydelig» må det vurderes 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*» (egen utheving), jf. art. 52 nr. 6. Videre følger det av bestemmelsen at 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».

For tillitsnivået «høyt» må de samme kravene som gjelder for «betydelig» oppfylles, og det må i tillegg gjøres en vurdering på et nivå «*som har som formål å minimere risikoen for avanserte cyberangrep utført av aktører med betydelige ferdigheter og ressurser*» (egen utheving), jf. art. 52 nr. 7. Det følger vider av bestemmelsen at «[v]urderingene 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».

«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», jf. art. 52 nr. 8.

4.7 Cybersikkerhetssertifiseringsmyndigheter

4.7.1 Innledning

Det følger av artikkel 58 nr. 1 at det skal utpekes én eller flere nasjonale cybersikkerhetssertifiseringsmyndigheter (forkortet NCCA) på hver stats territorium. Oppgavene cybersikkerhetssertifiseringsmyndigheten skal utføre fremkommer av artikkel 58 nr. 7. Artikkel 58 nr. 8 fastsetter hvilke fullmakter myndigheten som minimum skal ha for å kunne utføre de oppgavene den er pålagt. Oppgavene kan

deles inn i tre hovedkategorier av oppgaver; markedstilsyn, notifisering og samsvarsvurdering.

Etter forordningen artikkel 58 nr. 3 skal hver cybersikkerhetssertifiseringsmyndighet være uavhengig av de enhetene den fører tilsyn med når det gjelder organisering, beslutninger om finansiering, juridisk struktur og beslutningstaking. Det følger videre av artikkel 58 nr. 4 at NCCAs aktiviteter i forbindelse med utstedelse av sertifikater skal være «strengt atskilt fra deres tilsynsaktiviteter […] og at disse aktivitetene utføres uavhengig av hverandre». Uavhengig av om det opprettes én eller flere NCCA må følgelig samsvarsvurderingsorganet være adskilt og uavhengig av tilsynsfunksjonene til markedstilsynet og den notifiserende myndigheten.

4.7.2 Markedstilsynsmyndighet

Cybersikkerhetssertifiseringsmyndigheten (NCCA) skal utføre markedstilsyn i samarbeid med andre vedkommende markedstilsynsmyndigheter. Det skal føres tilsyn og kontroll med at sertifiserte IKT-produkter, IKT-tjenester og IKT-prosesser, oppfyller kravene i de aktuelle sertifiseringsordningene, der sertifikater er utstedt på statens territorium, jf. bokstav a.

At et sertifikat er utstedt på statens territorium innebærer at der et sertifikat er utstedt av enten norsk NCCA eller et samsvarsvurderingsorgan etablert i Norge, vil den norske NCCA ha ansvar for å føre tilsyn med IKT-produktet, -tjenesten eller -prosessen. Dette gjelder også dersom virksomheten som innehar sertifikatet er etablert i et annet land. For å kunne utføre tilsyn og håndheve bestemmelsene overfor virksomheter etablert i en annen stat, må statene samarbeide med andre relevante myndigheter. Det kan for eksempel inngås bilaterale avtaler mellom medlemsstatene, eller det kan inngås avtaler mellom de aktuelle myndigheter. Samarbeidet mellom statene kan for eksempel innebære at NCCA i staten der et sertifikat er utstedt forespør NCCA i staten der virksomheten holder til, om å utføre tilsynsoppgaver som å be om informasjon eller få adgang til virksomhetens lokaler i henhold til den andre statens lovgivning.

Cybersikkerhetssertifiseringsmyndigheten skal også kontrollere at produsenter/leverandører etablert i deres territorium, som har utstedt en EU-samsvarserklæring etter en sertifiseringsordning, oppfyller og håndhever forpliktelsene etter denne, jf. bokstav b. Det avgjørende for denne bestemmelsen er om virksomheten er «etablert» i staten. Begrepet «etablert» er ikke definert i forordningen. NSM forstår innholdet i begrepet i samsvar med de overordnede reglene for fri etableringsrett som følger av EØS-avtalen del 3 kapittel 2. Der en virksomhet er etablert i flere medlemsstater, vil alle statene ha ansvar og myndighet til å føre tilsyn.

Den enkelte sertifiseringsordning vil inneholde nærmere bestemmelser om markedstilsyn og kontroll av IKT-produkter, -tjenester og -prosesser for den spesifikke sertifiseringsordning, jf. artikkel 54 nr. 1 bokstav j.

Markedstilsynet skal ha myndighet til å kreve at innehavere av sertifikater og virksomheter med utstedt egenerklæring om samsvar fremlegger all informasjon myndigheten trenger for å utføre sine oppgaver, jf. artikkel 58 nr. 8 bokstav a. Markedstilsynet kan undersøke og revidere virksomhetene for å kontrollere at de

overholder kravene i cybersikkerhetsforordningen eller til en sertifiseringsordning, jf. artikkel 58 nr. 8 bokstav b. For å gjennomføre undersøkelser skal markedstilsynet kunne få adgang til lokalene til innehavere av sertifikater etter artikkel 58 nr. 8 bokstav d. For å sikre overholdelse av bestemmelsene i cybersikkerhetsforordningen eller en sertifiseringsordning skal markedstilsynet ha myndighet til å treffe tiltak og ilegge sanksjoner i samsvar med nasjonal rett, samt kreve at overtredelser av forordningen opphører jf. bokstav c og f.

NCCAs myndighet iht. artikkel 58 nr. 8 bokstav c kan også omfatte og pålegge virksomheter å trekke tilbake en EU-samsvarserklæring som virksomheten har utstedt. Det kan være grunn til å pålegge tilbaketrekning av en utstedt erklæring dersom en virksomhet ikke samarbeider med markedstilsynet, og for eksempel ikke gir den informasjonen tilsynet trenger.

Oppgavene som ligger til markedstilsynet er:

- motta kopi av EU-samsvarserklæringer fra produsenter og leverandører som har utført egenvurdering av samsvar og som utstedes i henhold til artikkel 53 nr. 3.
- kontrollere at IKT-produkter, -tjenester og -prosesser som er sertifisert på statens territorium oppfyller kravene i den respektive sertifiseringsordningen, jf. artikkel 58 nr. 7 bokstav a.
- kontrollere at produsenter og leverandører av IKT-produkter, -tjenester og prosesser som har utstedt egenerklæring om samsvar oppfyller og håndhever sine forpliktelser, jf. artikkel 58 nr. 7 bokstav b.
- treffe egnede tiltak overfor innehavere av sertifikater eller utstedere av EU-samsvarserklæringer for å sikre overholdelse av bestemmelser i cybersikkerhetsforordningen eller sertifiseringsordninger, jf. artikkel 58 nr. 8 bokstav c.
- ilegge innehavere av sertifikater eller utstedere av EU-samsvarserklæringer sanksjoner ved overtredelse av cybersikkerhetsforordningen eller sertifiseringsordninger, jf. artikkel 58 nr. 8 bokstav f.
- behandle klager fra produsenter og leverandører som har utstedt EU-samsvarserklæring, jf. artikkel 58 nr. 7 bokstav f.
- overvåke den relevante utviklingen på cybersikkerhetssertifiseringsområdet, jf. artikkel 58 nr. 7 bokstav i.

4.7.3 Notifiserende myndighet

Cybersikkerhetssertifiseringsmyndigheten (NCCA) skal utføre oppgaver som notifiserende myndighet (meldermyndighet og utpekende myndighet er synonymer). Begrepet «notifiserende myndighet» må leses i lys av referansebestemmelsene for EUs harmoniseringsregelverk, Europaparlaments- og rådsbeslutning nr. 768/2008/EF Vedlegg 1, for produkter kapittel R4, som beskriver oppgaver som ligger til en «notifying authority». I den norske offisielle oversettelsen av referansebestemmelsene er begrepet «meldermyndigheter» benyttet.

Artikkel 61 nr. 1 tillegger cybersikkerhetssertifiseringsmyndigheten (NCCA) ansvaret for å informere Kommisjonen om hvilke samsvarsvurderingsorganer som er akkreditert, og, dersom det er relevant, godkjent til å utstede sertifikater på angitte

tillitsnivåer iht. artikkel 52 og 60. nr. 3. Oppgavene som ligger i tilknytning til notifikasjonen til Kommisjonen anses å være en del av den notifiserende myndighet.

Det følger av artikkel 58 nr. 7 bokstav e at cybersikkerhetssertifiseringsmyndigheten (NCCA) skal «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». En slik godkjenning kreves dersom en cybersikkerhetsordning fastsetter særlige eller ytterligere krav til samsvarsvurderingsorganer enn det som kreves for å bli akkreditert, jf. artikkel 54 nr. 1 bokstav f.

Dersom det kreves en godkjenning av samsvarsvurderingsorganet etter artikkel 60 nr. 3 får cybersikkerhetssertifiseringsmyndigheten (NCCA) ansvar for godkjenningen og oppfølgingen av denne. Kun virksomheter som oppfyller tilleggskravene og er akkreditert kan bli godkjente virksomheter. Disse skal meldes til Kommisjonen etter artikkel 61 nr. 1, og godkjente virksomheter blir offentliggjort i Den europeiske unions tidende, jf. artikkel 61 nr. 2. Dersom en NCCA trekker tilbake en godkjenning av et samsvarsvurderingsorgan, har myndigheten også ansvar for å melde dette til Kommisjonen, jf. artikkel 61 nr. 1 siste punktum og nr. 4. Denne endringen vil også bli publisert i Den europeiske unions tidende.

Det er cybersikkerhetssertifiseringsmyndighetens ansvar at kun de samsvarsvurderingsorganene som oppfyller tilleggskravene iht. sertifiseringsordningene og som innehar akkreditering, er godkjent til å uføre sertifisering. Samsvarsvurderingsorganer skal underlegges tilsyn av myndigheten for å sikre at de overholder bestemmelsene i forordningen og aktuelle sertifiseringsordninger, jf. artikkel 58 nr. 7 bokstav b. For å gjennomføre tilsyn og undersøkelser skal NCCA ha myndighet til å få adgang til lokalene hos samsvarsvurderingsorganene og få fremlagt all informasjon myndigheten trenger for å utføre sine oppgaver, jf. artikkel 58 nr. 8 bokstav a og d.

Akkrediteringsorganet har ansvar for å føre tilsyn med de samsvarsvurderingsorganer de har akkreditert. Dersom et organ mister akkrediteringen, må det også miste godkjenningen til å utføre sertifisering. Disse oppgavene er derfor knyttet til hverandre, og det forutsetter et samarbeid mellom akkrediteringsorganet og NCCA. Artikkel 58 nr. 7 bokstav c beskriver forholdet slik: Nasjonale cybersikkerhetssertifiseringsmyndigheter skal «aktivt bistå og støtte de nasjonale akkrediteringsorganene med å kontrollere og føre tilsyn med samsvarsvurderingsorganenes aktiviteter for denne forordningens formål». Slik støtte kan for eksempel være i form av teknisk ekspertise knyttet til den enkelte sertifiseringsordning.

Til slutt ligger det også til den notifiserende myndigheten å kontrollere og føre tilsyn med de offentlige organene nevnt i artikkel 56 nr. 5, jf. artikkel 58 nr. 7 bokstav d. Dette er offentlige organer som utfører sertifisering dersom en sertifiseringsordning fastsetter at sertifikater kun skal utstedes av et offentlig organ.

For å sikre at samsvarsvurderingsorganene overholder bestemmelsene i forordningen eller en sertifiseringsordning skal den notifiserende myndigheten ha

hjemmel til å treffe tiltak og ilegge sanksjoner i samsvar med nasjonal rett, samt kreve at overtredelser av forordningen opphører jf. bokstav c og f.

Oppgavene som ligger til den notifiserende myndigheten er:

- der det er relevant, godkjenne samsvarsvurderingsorganer i samsvar med artikkel 60 nr. 3 og begrense, midlertidig oppheve eller trekke tilbake eksisterende godkjenning dersom samsvarsvurderingsorganene overtrer kravene i denne forordningen, jf. artikkel 58 nr. 7 bokstav e.
- utføre revisjoner av samsvarsvurderingsorganer for å kontrollere at de overholder kravene fastsatt i det europeiske rammeverket for cybersikkerhetssertifisering og gjeldende sertifiseringsordning.
- informere Kommisjonen om hvilke samsvarsvurderingsorganer som er akkreditert og eventuelt godkjent, jf. artikkel 61 nr. 1.
- be Kommisjonen om å fjerne samsvarsvurderingsorganer som tidligere er meldt dersom samsvarsvurderingsorganene ikke lenger er akkreditert eller en godkjenning oppheves, jf. artikkel 61 nr. 4.
- kontrollere og føre tilsyn med aktivitetene til de offentlige organene nevnt i artikkel 56 nr. 5, jf. artikkel 58 nr. 7 bokstav d.
- bistå og støtte akkrediteringsorganet med å kontrollere og føre tilsyn med samsvarsvurderingsorganer jf. artikkel 58 nr. 7 bokstav c.

4.7.4 Samsvarsvurderingsorgan

Det at NCCA opptrer som samsvarsvurderingsorgan er aktuelt i to tilfeller. Det ene tilfellet er der en sertifiseringsordning krever tillitsnivået «høyt» ettersom slike sertifikater som utgangspunkt bare utstedes av en nasjonal cybersikkerhetssertifiseringsmyndighet, jf. artikkel 56 nr. 6. Det andre tilfellet er der en sertifiseringsordning fastsetter at et sertifikat bare kan utstedes av et offentlig organ, som enten er en NCCA eller et annet offentlig organ som er akkreditert som samsvarsvurderingsorgan. Det følger av artikkel 60 nr. 2 at «[d]ersom et europeisk cybersikkerhetssertifikat utstedes av en nasjonal cybersikkerhetssertifiseringsmyndighet i samsvar med artikkel 56 nr. 5 bokstav a) og artikkel 56 nr. 6, skal samsvarsvurderingsorganet til den nasjonale cybersikkerhetssertifiseringsmyndigheten akkrediteres som et samsvarsvurderingsorgan».

Artikkel 56 nr. 6 fastsetter at en sertifisering med tillitsnivå «høyt», også kan utføres av andre samsvarsvurderingsorganer i to alternative tilfeller. Etter bokstav a kan et samsvarsvurderingsorgan utføre sertifisering på tillitnivå *høyt* «etter forhåndsgodkjenning fra den nasjonale cybersikkerhetssertifiseringsmyndigheten for hvert enkelt europeisk cybersikkerhetssertifikat. Alternativt kan NCCA delegere oppgaven generelt til et samsvarsvurderingsorgan etter bokstav b. Etter en slik forhåndsgodkjenning eller delegering av oppgaven vil det være samsvardsvurderingsorganet som blir ansvarlig for utstedelsen av sertifikatet. Cybersikkerhetsforordningen oppstiller ingen spesielle kriterier for å delegere sertifisering til et samsvarsvurderingsorgan etter artikkel 56 nr. 6, bortsett fra de generelle reglene for samsvarsvurderingsorganer, som at det må være akkreditert og

oppfylle eventuelle tilleggskrav som kan følge av den enkelte sertifiseringsordning. Ytterligere krav kan bli fastsatt senere i den enkelte sertifiseringsordning. Det er heller ingen begrensning i antall samsvarsvurderingsorganer som en NCCA kan godkjenne eller delegere oppgaven til.

Dersom utstedelsen av et sertifikat utføres av et samsvarsvurderingsorgan i henhold til artikkel 56 nr. 6 bokstav a eller b, forstår NSM artikkel 60 nr. 2 det slik at det da ikke er krav om at NCCA skal være akkreditert som samsvarsvurderingsorgan, siden NCCA ikke er den som utsteder sertifikatet.

Der det i sertifiseringsordninger stilles krav om at det er NCCA eller et offentlig akkreditert organ som utsteder sertifikat etter artikkel 56 nr. 5, er det dette organet som skal fatte avgjørelse om sertifisering skal gis eller ikke. I motsetning til artikkel 56 nr. 6 der sertifiseringen kan delegeres til et samsvarsvurderingsorgan etter en forhåndsgodkjenning eller generell delegering, kan ikke en avgjørelse om sertifisering etter artikkel 56 nr. 5 delegeres til private samsvarsvurderingsorganer. Dette utelukker derimot ikke at det benyttes underleverandører til å utføre enkelte oppgaver på vegne av myndigheten, jf. forordningens vedlegg punkt 9. For eksempel kan private laboratorier utføre tester av samsvar på vegne av det offentlige organet. Det kreves ikke at laboratoriet i et slikt tilfelle er akkreditert.

Selv om det er et krav i en sertifiseringsordning at sertifikatet kun kan utstedes av en NCCA, innebærer det ikke en forpliktelse for staten til å utføre sertifiseringen. Samsvarsvurderingsorganet er derfor en valgfri myndighetsoppgave. Ved vedtakelsen av nye sertifiseringsordninger, der det kreves at sertifisering utføres av en NCCA, vil det derfor være opp til statene om de ønsker å utføre denne sertifiseringen. Dersom staten for eksempel ikke har kapasitet eller kompetanse til å opprette et samsvarsvurderingsorgan til å utføre sertifisering etter sertifiseringsordningen, er ikke dette et krav etter forordningen.

Virksomheter som ønsker en type sertifisering som ikke utføres i egen stat, kan søke om dette i andre EØS-stater som utfører den aktuelle sertifiseringen. Dette betyr at en NCCA som utfører sertifisering etter en sertifiseringsordning skal sertifisere også virksomheter som er etablert i andre stater som søker sertifisering.

Samsvarsvurderingsorganet i NCCA skal som andre samsvarsvurderingsorganer behandle klager relatert til de sertifikatene den utsteder. Artikkel 58 nr. 7 bokstav f jf. artikkel 63 nr. 1 fastsetter at myndigheten skal «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. Dette innebærer at selv om NCCA ikke selv utfører sertifisering, og har forhåndsgodkjent eller delegert oppgaven til andre etter artikkel 56 nr. 6, må NCCA likevel behandle klager relatert til disse sertifiseringene, og dette er en del av NCCAs samsvarsvurderingsorgans oppgave.

NCCA har myndighet til å trekke tilbake sertifikater den selv har utstedt eller av samsvarsvurderingsorganer som har sertifisert i samsvar med artikkel 56 nr. 6 dersom kravene ikke overholdes, jf. artikkel 58 nr. 8 bokstav e.

For å gjennomføre tilsyn og undersøkelser skal den notifiserende myndigheten ha adgang til lokalene hos NCCAs samsvarsvurderingsorganener og få fremlagt all informasjon myndigheten trenger for å utføre sine oppgaver, jf. artikkel 58 nr. 8 bokstav a og d.

Oppgavene som ligger til cybersikkerhetssertifiseringsmyndighetens samsvarsvurderingsorgan er:

- utstede sertifikater etter artikkel 56 nr. 5 og artikkel 56 nr. 6.
- etter eget valg forhåndsgodkjenne andre samsvarsvurderingsorganer i hvert enkelt tilfelle for utstedelse av sertifikater på tillitsnivå «høyt», jf. artikkel 56 nr. 6 bokstav a.
- etter eget valg delegere sertifisering på tillitsnivå «høyt» generelt til andre samsvarsvurderingsorganer, jf. artikkel 56 nr. 6 bokstav b.
- oppfylle krav som gjelder generelt for alle samsvarsvurderingsorganer, fastsatt i vedlegget til cybersikkerhetsforordningen.
- trekke tilbake sertifikater organet selv har utstedt eller sertifikater utstedt av samsvarsvurderingsorganer i samsvar med artikkel 56 nr. 6 bokstav a og b, jf. artikkel 58 nr. 8 bokstav e.
- behandle klager i forbindelse med sertifikater organet selv har utstedt eller sertifikater utstedt av samsvarsvurderingsorganer i samsvar med artikkel 56 nr. 6 bokstav a og b, jf. artikkel 58 nr. 7 bokstav f.

4.7.5 Andre myndighetsoppgaver

Artikkel 58 nr. 7 pålegger den nasjonale cybersikkerhetssertifiseringsmyndigheten (NCCA) å fremlegge en årlig sammendragsrapport om de aktivitetene som er utført ifølge artikkel 58 nr. 7 bokstav b, c og d eller myndighet som er utøvet i henhold til artikkel 58 nr. 8.

NCCA skal også samarbeide med andre nasjonale cybersikkerhetssertifiseringsmyndigheter eller andre offentlige myndigheter blant annet ved informasjonsutveksling om mulig manglende samsvar med kravene i sertifiseringsordninger ved IKT-produkter/tjenester/prosesser, jf. bokstav h. Etter artikkel 58 nr. 9 skal de også samarbeide med andre staters nasjonale cybersikkerhetssertifiseringsmyndigheter og med Kommisjonen. Det er naturlig at alle de tre myndighetsrollene; markedstilsyn, notifiserende myndighet og samsvarsvurderingsorganet samarbeider med deres tilsvarende motparter i EØS.

Etter bokstav i skal myndigheten overvåke den relevante utviklingen på cybersikkerhetssertifiseringsområdet.

Det er opprettet en europeisk cybersikkerhetssertifiseringsgruppe («ECCG») under det europeiske rammeverket for cybersikkerhetssertifisering. Oppgavene til ECCG fremkommer av artikkel 62 nr. 4. Det europeiske rammeverket for cybersikkerhetssertifisering legger opp til at det i utgangspunktet er representanter for NCCA som deltar i gruppen jf. artikkel 58 nr. 6. Det åpnes likevel for at andre enn representanter for nasjonale myndigheter deltar i gruppen, jf. artikkel 62 nr. 2.

For å oppnå likeverdige standarder i hele EØS-området skal NCCA fagfellevurderes jf. artikkel 59 nr. 1. En fagfellevurdering skal utføres av minst to nasjonale

cybersikkerhetssertifiseringsmyndigheter fra andre EØS-medlemsstater og Kommisjonen, jf. artikkel 59 nr. 4. Det kan derfor være aktuelt at NCCA deltar i fagfellevurderinger i andre stater.

4.8 Klage og sanksjoner

Fysiske og juridiske personer har rett til å klage til utstederen av cybersikkerhetssertifikatet eller den relevante nasjonale cybersikkerhetssertifiseringsmyndighet etter artikkel 63. Klageorganet skal informere klageren om saksforløpet, beslutningen som er truffet og retten til effektive rettsmidler etter artikkel 64. Det følger av artikkel 64 nr. 1 at «[u]ten hensyn til eventuelle administrative rettsmidler eller annen ikke-rettslig prøving skal fysiske og juridiske personer ha rett til effektive rettsmidler ved 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, en manglende reaksjon på en klage inngitt til myndigheten eller organet nevnt i artikkel 63 nr. 1.»

Videre følger det av artikkel 64 nr. 2 at saker i medhold av denne artikkelen skal bringes inn for domstolene i medlemsstaten der myndigheten eller organet som rettsmidlet søkes brukt mot, befinner seg.

Etter artikkel 65 nr. 8 skal medlemsstatene fastsette effektive, forholdsmessige og avskrekkende sanksjoner ved brudd på regelverket.

5 Forslag til forvaltningsstruktur

5.1 Innledning

Cybersikkerhetsforordningen åpner for at de ulike oppgavene som ligger til cybersikkerhetssertifiseringsmyndigheten (NCCA) kan fordeles på én eller flere offentlige etater. Forordningen legger ingen føringer for antall myndigheter i én stat eller hvordan oppgavene fordeles, med unntak av at det skal opprettholdes et klart skille mellom tilsynsoppgaver og sertifiseringsoppgaver.

Det er flere alternative måter å organisere myndighetsoppgavene etter cybersikkerhetsforordningen på: en fastsatt forvaltningsstruktur og en fleksibel forvaltningsstruktur. En fastsatt forvaltningsstruktur er konkret fastsatt og gjelder for alle kommende sertifiseringsordninger. En fleksibel forvaltningsstruktur innebærer at det gjøres konkrete vurderinger av hvem som skal utpekes for hver sertifiseringsordning som blir etablert.

Vurderingen av om det skal etableres en fastsatt eller fleksibel forvaltningsstruktur er basert på følgende momenter:

Formålseffekt: I hvilken grad ivaretas formålet med forordningen? I hvilken grad legger alternativet til rette for at norske virksomheter kan oppnå sertifisering, og dermed ha tilgang til det europeiske markedet?

Fleksibilitet: Vil alternativet inneha nødvendig fleksibilitet? Det forventes at rammeverket vil utvikles over tid, og at flere sertifiseringsordninger vil bli etablert i fremtiden. Hvordan vil alternativet kunne håndtere denne utviklingen?

Gjennomførbarhet: Hvor realistisk vil alternativet være? Kan alternativet etableres?

Kompetanse: I hvilken grad kan alternativet benytte eksisterende kompetanse, og i hvor stor grad er det nødvendig å bygge ny kompetanse?

Kostnadseffektivitet: Hvilket alternativ vil medføre lavest kostnader for staten?

For å undersøke hvilke etater som best egner seg til å bli utpekt som NCCA er momentene rolleklarhet, fagkompetanse og økonomiske virkninger vurdert.

I vurderingen av ulike alternativ ses det på de obligatoriske myndighetsoppgavene under forordningen, samt etablering av samsvarsvurderingsorgan. NSM legger til grunn at staten ivaretar de obligatoriske myndighetsoppgavene, og at kommersielle samsvarsvurderingsorganer i størst mulig grad vil stå for sertifiseringer. Cybersikkerhetsforordningen pålegger som nevnt ikke staten å utføre sertifisering. Sertifisering på tillitsnivå høyt kan overlates til kommersielle aktører eller andre offentlige samsvarsvurderingsorganer etter artikkel 56 nr. 6 bokstav a og b. Evnen til å løse de obligatoriske rollene som markedstilsyn og notifisering vektlegges derfor tyngre enn evnen til å etablere og operere et offentlig samsvarsvurderingsorgan.

5.2 Forvaltningsstruktur for EUs varepakke i Norge

EUs varepakke har en struktur som i stor grad samsvarer med rammeverket for cybersikkerhetssertifisering. De samme myndighetsrollene skal etableres under begge regelverkene og begge regelverkene forsøker å harmonisere krav til produkter som settes på markedet og håndhevingen av kravene, og forhindre at stater etablerer særnasjonale krav. Begge regelverkene er utformet som rammeverk som hjemler senere vedtagelse av produktspesifikke regelverk ut i fra behovet.

Varepakkens forvaltningsstruktur i Norge er utformet som en fleksibel løsning, der det for hvert produktregelverk forsøkes å utnytte eksisterende kompetanse på området i samfunnet. Nærings- og fiskeridepartementet er ansvarlig for lov om tekniske kontrollorgan og EØS-vareloven, men ansvaret for regelverk om produkter er fordelt på ulike myndigheter. Ansvarlig myndighet for et produktregelverk bestemmes av ansvarsområdet til den enkelte etat, eventuelt i samråd dersom det er flere aktuelle etater.

5.3 Forvaltningsstruktur i andre land

I Sverige, Finland og Danmark er alle myndighetsoppgavene etter forordningen lagt til én etat. Det samme har andre land som Tyskland, Frankrike, Nederland og Belgia. Det kan synes som at EU-land har utpekt etater som har ansvar for beslektede reguleringer, som for eksempel Cyber Resilience Act (CRA), til rollen som nasjonale cybersikkerhetssertifiseringsmyndigheter (NCCA).

I de årene det ikke har vært noen sertifiseringsordning under forordningenen har myndighetsoppgavene vært helt minimale. Det ville derfor trolig vært lite hensiktsmessig for EU-statene å dele opp myndighetsrollene på et så tidlig tidspunkt.

Sverige

Sverige har lagt NCCA til Försvarets materialverk (FMV) som ligger under det svenske forsvarsdepartementet. Oppgaven knyttet til NCCA er lagt til avdelingen Cybersäkerhet och certifiering. Avdelingen består av Sveriges certifieringsorgan för IT-säkerhet (CSEC) og Inspektionen för cybersäkerhetscertifiering (ICC). CSEC vil ha ansvar for sertifisering, mens ICC har ansvar for tilsynsoppgavene. CSEC tilhører SOG-IS og CCRA, og har utført sertifisering i 20 år. FMV hadde før utpekingen som NCCA ingen tilsynsoppgaver og ICC ble opprettet etter at FMV ble utpekt som NCCA. CSEC kan sammenlignes med SERTIT i Norge, mens FMV som helhet tilsvarer Forsvarsmateriell.

Det kan se ut til at Sverige har lagt vekt på sertifiseringskompetansen ved utpeking av NCCA, og har valgt å bygge opp ny kompetanse i etaten på tilsyn.

Finland

Finland har utpekt Transport and Communications Agency (Traficom) som ligger under det finske samferdselsdepartementet til NCCA. Traficom har ansvar innenfor transport, kommunikasjon og cyber. NCCA er plassert i National Cyber Security Centre Finland (NCSC-FI). NCSC-FI utvikler og overvåker driften og sikkerheten til kommunikasjonsnettverk og tjenester og overvåker situasjonsbildet innen cybersikkerhet. NCSC-FI har også en bred portefølje av andre oppgaver innen cyberdomenet. Traficom har ansvar for myndighetsoppgavene innen EU-regelverkene NIS 2 og eIDAS, og har ansvar for lovarbeidet ifm. CRA i Finland. Traficom deltar i SOG-IS på vegne av Finland.

Det virker til at Finland i stor grad legger opp til at det skal være kommersielle aktører som utfører sertifisering på tillitsnivået høyt, og at Traficom skal utføre tilsyn og notifisering av samsvarsorganer.

Traficom har et stort spekter av oppgaver innen ulike samfunnsområder. Det er derfor vanskelig å finne en direkte sammenlignbar etat i Norge. Traficom dekker store deler av ansvarsområdet til Nkom, samt enkelte ansvarsområder som ligger til NSM og Datatilsynet.

Danmark

Danmark har utpekt Sikkerhedsstyrelsen til NCAA. Sikkerhetsstyrelsen er en etat under det danske næringsdepartementet, og har som oppgave å utføre markedsovervåkning, kontroll og tilsyn på området for forbrukerprodukter, energiområdet og helseområdet.

Danmark legger opp til at Sikkerhedsstyrelsen vil benytte etaten Center for Cybersikkerhed (CFCS), som er det nasjonale kompetansemiljøet for cybersikkerhet, for sparring og rådgivning ved behov.

Sikkerhedsstyrelsen vil utføre markedstilsyn og oppgaver som notifiserende myndighet. Det er uklart hvem som vil utføre sertifiseringer på tillitsnivå høyt, noe som kan tyde på at dette blir delegert til kommersielle aktører.

Oppgavene til Sikkerhedsstyrelsen innen markedstilsyn og notifisering kan sammenfalle noe med oppgavene under Direktoratet for samfunnssikkerhet og beredskaps (DSB) oppgaver innen dette i Norge.

5.4 Vurdering av fast forvaltningsstruktur

Det er hovedsakelig to alternative måter å etablere en fastsatt forvaltningsstruktur på. Den ene er å utpeke én etat med ansvar for alle oppgaver. Den andre er at det fordeles faste oppgaver mellom ulike offentlige myndigheter som gjelder generelt for alle sertifiseringsordningene.

5.3.1. Utpeking av én etat

Utpeking av én etat vil medføre at alle myndighetsoppgaver legges til én etat for alle fremtidige sertifiseringsordninger.

Artikkel 58 nr. 3 krever at tilsynsorganene er uavhengige av de den fører tilsyn med. Dette vil si at notifiserende myndighet må være uavhengig av samsvarsvurderingsorganet.

På nåværende tidspunkt har NSM vurdert tre hovedalternativer dersom det skal utpekes én etat, herunder utpeking av NSM, Nkom eller å opprette en ny etat. Alternativet med opprettelsen av en ny etat er ikke utredet nærmere fordi det vil være kostnadsdrivende, duplisere allerede eksisterende kompetanse, skape ressursutfordringer ved å flytte eller bygge opp fagmiljøer på nytt, i tillegg til å kreve ekstra forvaltning og oppfølging uten å utnytte eksisterte nettverk og ordninger.

5.3.1.1. Nasjonal sikkerhetsmyndighet

Ved utpeking av NSM som NCCA kan NSM benytte erfaringen og kompetansen med sertifisering av IKT-produkter fra forvaltningen av SERTIT, se punkt 2.3. SERTIT mangler imidlertid den akkrediteringen som artikkel 60 krever, og må i så fall oppnå akkreditering hos Norsk akkreditering. NSM har også erfaring med å godkjenne selskaper som leverer tjenester for hendelseshåndtering av IKT-sikkerhetshendelser via den såkalte Kvalitetsordningen. Samtidig vurderes det å være flere utfordringer med å utpeke NSM. For å ivareta uavhengighetskravene etter forordningen bør sertifisering delegeres, hvilket begrenser nytten av NSMs egen sertifiseringskompetanse. NSM har ikke etablert kompetanse på markedstilsyn eller notifisering og må bygge nye funksjoner.

For å utføre alle oppgavene til NCCA for et så bredt spekter av områder, vil det kreve at det bygges opp ny kompetanse i virksomheten. ECCF er først og fremst et regelverk med betydning for konkurransen i EØS, offentlige anskaffelser og konsumenter av varer og tjenester, og ikke nasjonal sikkerhet. Oppgavene som NCCA er et godt stykke unna NSMs resterende oppgaveportefølje.

NSM må utvikle nye funksjoner for å utføre markedstilsyn og notifisering av samsvarsorganer, noe som vil kreve ekstra ressurser. I tillegg må det for hver ny sertifiseringsordning vurderes om NSM har den nødvendige kompetansen for å utføre oppgavene som NCCA. Dersom NSM ikke har relevant kompetanse innenfor en sertifiseringsordning og kompetansen finnes i andre etater, vil dette innebære duplisert kompetanse og være ressursdrivende.

Tilsyn etter det europeiske rammeverket for cybersikkerhetssertifisering har dessuten et helt annet formål enn NSMs tilsynsvirksomhet etter lov om nasjonal sikkerhet sikkerhetsloven). Fremtidige ordninger (EUCC, EUCS, EU5G, samt ordninger som kan følge av CRA, KI-forordningen og eIDAS 2.0) favner også bredere enn NSMs kjerneområder og samfunnsoppdrag som er å beskytte nasjonale sikkerhetsinteresser. Det vil derfor også kreve en betydelig ny oppbygging av tilsynskompetanse i etaten dersom NSM utpekes.

5.3.1.2. Nasjonal kommunikasjonsmyndighet

Nasjonal kommunikasjonsmyndighet (Nkom) har solid erfaring med markedstilsyn (bl.a. under Varepakken) og fører i dag tilsyn etter flere relevante forskrifter.

Hva gjelder markedstilsyn spesifikt fører Nkom markedstilsyn etter forskrift til EØS-krav til elektromagnetisk kompatibilitet (EMC) for utstyr til elektronisk kommunikasjon, forskrift om EØS-krav til radioutstyr og forskrift om EØS-krav til maritimt radioutstyr. Nkom er også tilsynsmyndighet etter lov om elektroniske tillitstjenester som gjennomfører eIDAS-forordningen. Nkom har ansvar for å føre tilsyn med at kravene i Radioutstyrsdirektivet (RED) til cybersikkerhet i radioutstyr er oppfylt, og har ansvar for å forberede regelverk og tilsyn med forordning (EU) 2024/2847 om cybersikkerhet (Cyber Resilience Act (CRA)). CRA har betydelig overlapp mot rammeverket for cybersikkerhetssertifisering, og etter NSMs vurdering vil Nkoms tilsynserfaring ha overføringsverdi til oppgaven som markedstilsyn.

Nkom har derimot ingen egne oppgaver som samsvarsvurderingsorgan i dag, og vil derfor måtte bygge opp sertifiseringskompetanse. En kostnadseffektiv løsning kan være at Nkom overfører sertifisering til eksisterende offentlige eller kommersielle organer fremfor å bygge opp egen sertifiseringskompetanse. Dette vil også ivareta skillet mellom sertifisering og tilsyn. Dersom Nkom utpekes som NCCA, vil de i likhet med NSM, måtte vurdere for hver ny sertifiseringsordning om Nkom innehar tilstrekkelig kompetanse til å kunne utføre oppgavene som NCCA, eller om det må bygges opp ny kompetanse, noe som kan være kostnadsdrivende.

5.3.2 Fordeling av oppgaver

Et alternativ er å fordele myndighetsoppgavene mellom flere etater, herunder at tilsynsoppgavene plasseres hos én etat, samtidig som sertifiseringsoppgavene plasseres til en annen. Dette vil skape det nødvendige skillet mellom tilsynsoppgaver og sertifiseringsoppgaver. Det vil samtidig sikre at allerede etablerte funksjoner og kompetansemiljøer videreføres og bygges videre på, noe som vil redusere kostnader til kompetansebygging og etablering av nye prosesser og funksjoner.

Et alternativ er for eksempel at markedstilsyn og notifisering tildeles Nkom, samtidig som oppgavene knyttet til sertifisering tildeles NSM. I tillegg må de andre myndighetsrollene plasseres mellom de to etatene.

Etter NSMs vurdering kan en slik fordeling skape uklare ansvarsforhold, og over tid vil det kunne skape lite eierskap til forordningen. Tydelig rollefordeling og aktivt samarbeid mellom etatene vil være en forutsetning, i tillegg til samarbeid mellom ansvarlige departementer. Etter NSMs vurdering kan dette føre til noe merarbeid i staten.

Fordeling av oppgaver vil derimot ivareta et klart skille mellom tilsynsoppgaver i Nkom og sertifiseringsoppgaver i NSM. Fordelingen vil videre sikre at allerede etablerte funksjoner og kompetansemiljøer videreføres og bygges videre på, noe som vil redusere kostander til kompetansebygging og etablering av nye prosesser og funksjoner.

5.3.3 Samlet vurdering av fast forvaltningsstruktur

I en fast forvaltningsstruktur vektlegges at obligatoriske myndighetsoppgaver (markedstilsyn, notifisering m.m.) må utføres av en utpekt myndighet, mens sertifisering kan overlates til private eller andre offentlige organer. Etter NSMs vurdering taler dette for at én etat med allerede etablert markedstilsynskompetanse utpekes som myndighet, herunder Nkom.

Nkom kan være cybersikkerhetsmyndighet alene, eller dele ansvaret med NSM som samsvarsvurderingsorgan. NSM vurderer at begge løsninger kan fungere, men at det vil skape et klarere ansvarsforhold og at eierskapet til myndighetsoppgavene vil styrkes om det kun er én etat som utpekes. Nkom kan også delegere sertifisering til andre offentlige eller private organer. Det legges til grunn at det mest kostnadsbesparende er om private virksomheter utfører sertifisering i størst mulig grad. Under en fastsatt struktur vurderer NSM det som mest hensiktsmessig at Nkom utpekes alene til å være cybersikkerhetsmyndighet. NSM ber om høringsinstansenes innspill.

Effekt- og kriterievurderinger under en fast struktur:

- Formålseffekt: Norsk næringsliv får tilgang til sertifisering på tvers av fremtidige ordninger. Sertifiseringsmyndigheten er den samme, selv om utførende organer kan variere gjennom delegering.
- Fleksibilitet: Ingen enkelt etat har i dag full breddekompetanse for alle foreslåtte ordninger (EUCC, EUCS, EU5G m.fl.). Én fast forvaltningsstruktur for alle ordninger kan bli rigid og kan føre til at nesten identiske markedstilsynsoppgaver havner i ulike etater når annet EØS-regelverk berører samme fagområde. Dette kan føre til at nesten samme oppgave utføres i flere myndigheter.
- Gjennomførbarhet: En etat med allerede etablert markedstilsynskompetanse kan utpekes umiddelbart og bygge kompetanse over tid.
- Kompetanse: Sertifiseringsordningene spenner over ulike domener som i dag eies av ulike myndigheter. Selv om kravene er cybersikkerhetsorienterte, kan forvaltningsansvaret kreve domeneinnsikt
- Kostnadseffektivitet: Etaten må tilføres midler for kompetansebygging der nye ordninger kommer. Hvis andre etater allerede fører tilsyn på nærliggende områder, kan en enkelt-etat-modell føre til to parallelle tilsynsløp og høyere samlede kostnader, sammenlignet med om én etat har flere, beslektede tilsynsroller.

5.5 Vurdering av fleksibel forvaltningsstruktur

En fleksibel forvaltningsstruktur innebærer at det for hver enkelt sertifiseringsordning som gjennomføres under rammeverket for cybersikkerhetssertifisering, utpekes én eller flere NCCA. Utpekingen vil baseres på konkrete vurderinger av hva som anses

hensiktsmessig for den spesifikke sertifiseringsordningen med hensyn til hvilke etater som har erfaring og kompetanse på fagområdet. Ved innføringen av en ny sertifiseringsordning, kan det både pekes på myndigheter som allerede er NCCA for andre sertifiseringsordninger eller det kan utpekes etater som ikke har noen slik rolle fra før.

Det vurderes å være to alternative måter å etablere dette på:

- Én etat per sertifiseringsordning
- En helt fleksibel forvaltningsstruktur

I første alternativ utpekes det én etat per sertifiseringsordning. Dette innebærer at det kun er én etat som får samlet ansvar for tilsyn, notifisering og sertifisering. Løsningen kan gi klare linjer og enkel styring, men krever tydelige interne tiltak for å sikre det nødvendige organisatoriske skillet mellom tilsynsorgan og samsvarsvurderingsorgan.

En helt fleksibel forvaltningsstruktur åpner for at det kan gjøres frie og konkrete vurderinger av hva som er mest hensiktsmessig forvaltning av den enkelte sertifiseringsordning.

En fleksibel forvaltningsstruktur åpner for at det både kan utpekes én NCCA for en sertifiseringsordning med ansvar for alle myndighetsoppgavene, men også åpnes for utpeking av flere NCCA, slik at oppgavene under en sertifiseringsordning fordeles på flere ulike etater.

En fleksibel forvaltningsordning speiler varepakken, der hvert underliggende regelverk fordeles til den etaten som har dette som sitt ansvarsområde.

Under en fleksibel forvaltningsstruktur utpekes i utgangspunktet kun én nasjonal cybersikkerhetssertifiseringsmyndighet etter forordningens artikkel 58 inntil hver enkelt sertifiseringsordning gjennomføres i norsk rett. Øvrige myndighetsroller fordeles først når en konkret sertifiseringsordning innføres i norsk rett. Den nasjonale myndighet bør ha handlingsrom til å anbefale myndighetsroller som vurderes som mest hensiktsmessige. NSM vurderer at den helt fleksible forvaltningsstrukturen, der markedstilsyn, notifisering og sertifisering kan fordeles helt fritt, er det mest hensiktsmessige alternativet for å oppnå forordningens formål, og sikre en faglig og effektiv forvaltning av fremtidige sertifiseringsordninger.

Ved å gjøre vurderinger for hver sertifiseringsordning av hvilken etat som innehar mest relevant kompetanse for å kunne utføre oppgavene som NCCA, legges det til grunn at man i størst mulig grad vil kunne gjenbruke eksisterende fagkompetanse i forvaltningen. Alternativet vurderes å ha mindre økonomiske konsekvenser når det i mindre grad trengs å bygges opp ny fagkompetanse i forvaltningen. Rolleklarhet må sikres ved utpeking av NCCA for hver enkelt sertifiseringsordning.

Fordelingslogikken bygger på gjenbruk av eksisterende fagmiljøer for å redusere behovet for opplæring og parallelle strukturer:

- Formålseffekt: Modellen sikrer tilgang til sertifisering på norsk territorium og øker sannsynligheten for at “riktig etat” med relevant kompetanse blir utpekt

for hver ordning. En mulig ulempe er at saks- og beslutningsløp ved hver innføring kan forsinke nasjonal gjennomføring noe.

- Fleksibilitet: Svært høy. Både tempo og volum av nye EU-regler er usikre, og fleksibel utpeking gjør det mulig å matche fagansvar med riktig etat i hvert enkelt tilfelle og utnytte best tilgjengelige synergier.

- Gjennomførbarhet: En nasjonal cybersikkerhetssertifiseringsmyndighet har begrenset oppgaveomfang, og modellen er gjennomførbar (erfaringsstøtte fra Varepakken). Samtidig kan praktisk oppfølging variere mellom ulike sertifiseringsordninger, og antallet involverte virksomheter blir høyere totalt – men kan bli lavere innen enkelte produktområder dersom man samler tilsyn med beslektede regelverk hos samme etat.

- Kompetanse: Modellen adresserer at ingen enkelt etat i dag dekker alle kommende ordninger (f.eks. EUCC, EUCS, EU5G). Ved å legge ordninger til etater som allerede fører relevant markedstilsyn (som under Radioutstyrsdirektivet) eller har nær beslektet kompetanse, oppnås reell faglig synergi og gjenbruk.

- Kostnadseffektivitet: Ved å legge myndighetsroller der kompetansen allerede finnes, reduseres behovet for å bygge opp nye, dupliserte fagmiljøer. Det gir lavere etablerings- og driftskostnader totalt og vurderes som den mest kostnadseffektive tilnærmingen—forutsatt tydelig rolleklarhet og koordinering ved hver utpeking.

5.6 Anbefalt forvaltningsstruktur

Det er gjort en vurdering av de to alternativene fastsatt og fleksibel forvaltningsstruktur opp mot hverandre. Hva gjelder formålseffekt og gjennomførbarhet vurderes både en fastsatt og en fleksibel forvaltningsstruktur til å oppfylle kriteriene i like stor grad. Det er på områdene fleksibilitet, kompetanse og kostnadseffektivitet de store forskjellene ligger. En fleksibel struktur vil i vesentlig bedre grad klare å ivareta kriteriene fleksibilitet, kompetanse og kostnadseffektivitet.

En fleksibel forvaltningsstruktur vurderes på nåværende tidspunkt som den mest hensiktsmessige organiseringen av NCCA i Norge. Dette vil innebære å avvente utpeking av myndigheter basert på en vurdering av hver enkelt sertifiseringsordning, men at det utpekes én nasjonal cybersikkerhetssertifiseringsmyndighet med ansvar for å forvalte cybersikkerhetsforordningen på et overordnet nivå.

5.7 Utpeking av nasjonal cybersikkerhetssertifiseringsmyndighet

5.7.1 Oppgaver

Dersom det utpekes én cybersikkerhetssertifiseringsmyndighet til å ha en nasjonal overordnet rolle, vil den ha ansvar for:

- å delta i den Europeiske cybersikkerhetssertifiseringsgruppen (ECCG) eller delegere deltagelse til andre etater, jf. artikkel 58 nr. 6.
- sørge for at Norge deltar i relevante undergrupper i ECCG, enten ved egen deltagelse eller ved å sikre at andre nasjonale cybersikkerhetssertifiseringsmyndigheter eller andre offentlige etater får muligheten til å delta i undergrupper.
- sammenstille en årlig sammendragsrapport om aktivitetene som nevnt i artikkel 58 nr. 7 bokstav g.
- være kontaktpunkt og eventuelt koordinere en fagfellevurdering av cybersikkerhetssertifiseringsmyndigheter i Norge etter artikkel 59.
- følge relevant utvikling på cybersikkerhetssertifiseringsområdet jf. artikkel 58 nr. 7 bokstav i.
  Informere Kommisjonen om identiteten til utpekte nasjonale cybersikkerhetssertifiseringsmyndigheter og hvilke oppgaver de ulike myndighetene har fått tildelt, jf. artikkel 58 nr. 2.

5.7.2 Én nasjonal cybersikkerhetssertifiseringsmyndighet

I en fleksibel forvaltningsstruktur vurderer NSM det som mest hensiktsmessig at det utpekes én nasjonal cybersikkerhetssertifiseringsmyndighet som får et overordnet ansvar for å forvalte forordningen.

NSM har vurdert to departementer som aktuelle:

Justis- og beredskapsdepartementet (JD) har ansvar for å samordne IKT-sikkerhet på sivil side og er ansvarlig departement for digitalsikkerhetsloven og digitalsikkerhetsforskriften. Det kan derfor være naturlig at de også har en nasjonal rolle etter cybersikkerhetssertifiseringsforskriften som er forankret i samme lov. JD er ansvarlig for å gjennomføre cybersikkerhetsforordningen i norsk rett, selv om arbeidet med cybersikkerhetssertifiseringsforskriften er delegert til NSM.

Et annet departement som vurderes som aktuell for den nasjonale rollen er Digitaliserings- og forvaltningsdepartementet (DFD). Departementet skal bidra til å styrke statens og samfunnets evne til å utnytte potensialet og håndtere utfordringene som digital teknologi skaper, og har en pådriverrolle og en samordningsrolle i dette arbeidet. Det legges derfor til grunn at DFD har en god oversikt over bredden av ulik teknologi og statlige virksomheter med kompetanse på dette området. I lys av dette fremstår DFD å ha gode forutsetninger for å ha en overordnet og nasjonal rolle for forvaltning av forordningen. DFD har også ansvar for CRA, KI-forordningen og eIDAs 2.0 som har grenseflater mot rammeverket for cybersikkerhetssertifisering.

Det kan også gjøres en vurdering av om den nasjonale rollen bør legges til NSM eller Nkom. NSM har fått delegert ansvar for å utarbeide forskrift og høringsnotat som gjennomfører cybersikkerhetsforordningen i norsk rett.

Nkom har ansvar for flere av fagområdene der det kan komme europeiske sertifiseringsordninger fremover, som f.eks. 5G, CRA, KI-forordningen og eIDAS. Nkom har også erfaring med å følge utviklingen av produktrammeverk under varepakken.

Ved innføring av nye sertifiseringsordninger må relevante departementer involveres. Om NSM eller Nkom utpekes til en nasjonal rolle, kan de i samråd med relevante departementer og etater kartlegge hvilke etater som har kompetanse på området, og vurdere og anbefale plassering av NCCA for ulike sertifiseringsordninger.

Etter NSMs vurdering ligger oppgaven som nasjonal cybersikkerhetssertifiseringsmyndighet utenfor NSMs samfunnsoppdrag. Etter NSMs vurdering fremstår Nkom som bedre egnet til å utføre oppgavene til en nasjonal myndighet når det ses hen til deres erfaring med varepakken og markedstilsyn, og deres kompetanse på flere av områdene det vil kunne komme sertifiseringsordninger for.

5.7.3 Anbefaling

NSM har gjennomført en helhetlig vurdering av hvordan den nasjonale rollen etter forordningen kan organiseres. I vurderingen er det lagt vekt på at utpekingen av nasjonale cybersikkerhetsmyndigheter for fremtidige sertifiseringsordninger vil kreve involvering av flere departementer med ansvar for ulike sektorer og underliggende etater. En løsning der den nasjonale cybersertifiseringsmyndigheten legges til et departement kan derfor bidra til en mer effektiv beslutningsprosess enn dersom rollen plasseres hos en underliggende etat, men dette må vurderes nærmere i lys av helhetlige behov og ansvarligfordeling på tvers av sektorer. Andre aktuelle kandidater kan være virksomheter under Digitaliserings- og forvaltningsdepartementet eller Justis- og beredskapsdepartementet, herunder Digitaliseringsdirektoratet, NSM, Nkom m.fl.

Gjedrem II-utvalget overleverte sin rapport 9. april 2025. Utvalget har gjennomført en ekstern gjennomgang av NSMs oppgaveportefølje med formål å vurdere om NSM er hensiktsmessig organisert for å svare på fremtidens utfordringer. Rapporten er under oppfølging og inkluderer en bredere vurdering av ansvar og oppgaver innenfor digital sikkerhet på departements- og etatsnivå. Resultatet av dette arbeidet vil kunne få betydning for hvordan myndighetsoppgavene etter forskriften skal plasseres.

Endelig beslutning vil bli tatt før forskriften fastsettes. Vi ber høringsinstansene om innspill og synspunkter på dette.

6 Gjennomføring av cybersikkerhetsforordningen i norsk rett

6.1 Inkorporering i ny forskrift

Det foreslås at cybersikkerhetsforordningen gjennomføres i norsk rett som ny forskrift til digitalsikkerhetsloven i tråd med forutsetningene i Prop 109 LS (2022-2023), se side 6. Forskriftsutkastet § 1 inkorporerer cybersikkerhetsforordningen fullt ut. Som nevnt er del I og II allerede gjennomført i ekomforskriften. Del III av forordningen bør leses i lys av del I som inneholder generelle bestemmelser om formål, virkeområde og definisjoner av begreper. Etter NSMs vurdering bør forordningen uansett ikke gjennomføres i ulike regelverk, og det foreslås derfor at forordningens del I og II som

er gjennomført i ekomforskriften overføres til forskriften om cybersikkerhetssertifisering, og at ekomforskriften § 2-11 oppheves.

I og med at forordningen skal gjennomføres som sådan, jf. EØS-avtalen artikkel 7 bokstav a, foreslås det at forordningen inkorporeres i forskriften ved en henvisningsbestemmelse. Det forutsettes i forordningen artikkel 65 at det nasjonalt fastsettes sanksjoner ved overtredelser av bestemmelsene i forordningen og sertifiseringsordningene. I tillegg overlates det til statene å gi regler som skal sikre overholdelse av bestemmelsene i forordningen, jf. artikkel 58 nr. 8 bokstav c, samt tilbakekalle sertifikater ved overtredelser av bestemmelsene i forordningen eller sertifiseringsordning, jf. artikkel 58 nr. 8 bokstav e.

Forskriften fastsettes med hjemmel i digitalsikkerhetsloven § 18 bokstav f og § 19.

TKO-loven vil gjelde for autorisering av samsvarsvurderingsorganer og disse organenes virksomhet. Det foreslås derfor at forskriften også hjemles i TKO-loven § 7.

Se forslag til inkorporering av cybersikkerhetsforordningen i forslag til ny forskrift § 1.

6.2 Geografisk virkeområde

Forordningen gjelder innenfor EØS-avtalens geografiske virkeområde. EØS-avtalen er ikke gjort gjeldende for Svalbard, og Norge er derfor ikke forpliktet til å gjennomføre EØS-rettsakter i Svalbardregelverket. På Svalbard er utgangspunktet at norsk privatrett og strafferett gjelder, mens andre lovbestemmelser ikke gjelder, med mindre det er særskilt fastsatt, jf. lov av 17. juli 1925 nr. 11 om Svalbard § 2. Det følger av forslaget til digitalsikkerhetsforskriften § 3 at digitalsikkerhetsloven med forskrifter gjelder for Svalbard. Det må likevel gjøres en særskilt vurdering av om cybersikkerhetsforordningen skal implementeres i lovverk som gjelder for Svalbard, og eventuelt tilpasses å gjelde på Svalbard.

Dagens reguleringer for virksomheter som ønsker å bli samsvarsvurderingsorganer, oppstiller hindre for å gjøre cybersikkerhetsforordningen gjeldende på Svalbard. TKO-loven gjelder ikke på Svalbard. Det gjør heller ikke EØS-vareloven, som utpeker Norsk akkreditering til nasjonalt akkrediteringsorgan. NSM vurderer at det vil kreve lovendringer i EØS-vareloven og TKO-loven om cybersikkerhetsforordningen del III helt eller delvis gjennomføres på Svalbard. Cybersikkerhetssertifiseringsforskriften gjøres derfor ikke gjeldende på Svalbard.

Slik NSM forstår forordningen forhindrer ikke dette virksomheter etablert på Svalbard fra å søke om sertifisering av samsvarsvurderingsorganer etablert på fastlands-Norge.

6.3 Nasjonalt akkrediteringsorgan

Artikkel 60 nr. 1 fastsetter at samsvarsvurderingsorganene skal akkrediteres av de nasjonale akkrediteringsorganene som er utpekt i samsvar med forordning (EF) nr. 765/2008. Norsk Akkreditering er utpekt som nasjonalt akkrediteringsorgan etter EØS-vareloven § 3, og vil være akkrediteringsorgan også etter cybersikkerhetsforordningen.

Se forslag til bestemmelse i § 2.

6.4 Nasjonale cybersikkerhetssertifiseringsmyndigheter

Det foreslås at det utpekes flere nasjonale cybersikkerhetssertifiseringsmyndigheter med myndighetsroller under cybersikkerhetsforordningen jf. artikkel 58 nr. 1. Det utpekes én nasjonal cybersikkerhetssertifiseringsmyndighet med ansvar for å forvalte cybersikkerhetsforordningen på et overordnet nivå.

For hver sertifiseringsordning som etableres under rammeverket, skal det utpekes minst en markedstilsynsmyndighet og en notifiserende myndighet. For de sertifiseringsordningene der det er relevant, kan det utpekes en nasjonal cybersikkerhetssertifiseringsmyndighet som samsvarsvurderingsorgan. Markedstilsynsmyndigheten, den notifiserende myndigheten og samsvarsvurderingsorganet kan tilhøre samme virksomhet, men slik at kravene i artikkel 58 nr. 3 og 4 overholdes.

6.5 Sanksjoner

6.5.1 Pålegg om retting eller tilbaketrekning av samsvarsvurdering

Artikkel 58 nr. 8 bokstav c fastsetter at tilsynsmyndigheten skal kunne treffe egnede tiltak i samsvar med nasjonal rett for å sikre overholdelse av bestemmelsene i forordningen eller sertifiseringsordninger. Den enkelte sertifiseringsordning kan også fastsette konsekvenser for IKT-produkter, -tjenester, -prosesser og administrerte sikkerhetstjenester som er sertifisert eller som det er utstedt egenerklæring om samsvar for, men som ikke oppfyller kravene i sertifiseringsordningen, jf. artikkel 54 nr. 1 bokstav l.

Et pålegg om retting slik at kravene til en sertifiseringsordning blir oppfylt, kan være et utgangspunkt for ytterligere tiltak dersom pålegget ikke etterleves. Muligheten til å gi pålegg er ikke begrenset til kun å overholde krav fastsatt i en sertifiseringsordning, men gjelder alle krav som også kan følge av det overordnede rammeverket. Pålegg om retting kan være et relevant tiltak ved for eksempel overtredelse av:

- bestemmelsene om offentliggjøring av tilleggsinformasjon jf. artikkel 55,
- plikten til å gi informasjon til samsvarsvurderingsorganet ved påviste sårbarheter eller uregelmessigheter jf. artikkel 56 nr. 8,
- manglende medvirkning til NCCAs undersøkelser som for eksempel fremleggelse av informasjon eller adgang til lokaler jf. artikkel 58 nr. 8 bokstav a og d.

Når det gis pålegg om retting, bør det også fastsettes en frist for når forholdet må bringes i orden.

Så lenge det er valgfritt for virksomheter hvorvidt de vil sertifisere administrerte sikkerhetstjenester, IKT-produkter, -tjenester og -prosesser, og sertifisering ikke er et rettslig krav for å gjøre noe tilgjengelig på markedet, har NSM vurdert det som mindre aktuelt å innføre regler om å forby salg av IKT-produktet, -tjenesten eller -prosessen generelt.

Der en produsent eller leverandør har utstedt EU-samsvarserklæring uten å oppfylle kravene som følger av sertifiseringsordningen kan et aktuelt tiltak være å pålegge produsenter og leverandører som har utstedt EU-samsvarserklæringen å trekke denne tilbake, og forby markedsføring som gir uttrykk for at administrerte sikkerhetstjenester, IKT-produktet, -tjenesten eller -prosessen oppfyller kravene til sertifiseringsordningen.

Se forslag til bestemmelse i § 4 andre ledd om tilsynsmyndighetens kompetanse og om pålegg i § 9.

6.5.2 Tvangsmulkt

Dersom pålegg om retting ikke blir brakt i orden innen fastsatt frist, kan tvangsmulkt etter forvaltningsloven § 51 være et aktuelt tiltak. Etter NSMs vurdering bør det være opp til markedstilsynets skjønn om tvangsmulkt er et egnet tiltak.

Etter NSMs vurdering er det relevant å se hen til momentene for utmåling av tvangsmulkt etter markedsføringsloven. Forskrift om utmåling av tvangsmulkt og overtredelsesgebyr av 14. februar 2023 gir regler om utmåling av tvangsmulkt og overtredelsesgebyr etter markedsføringsloven og flere andre lover som skal ivareta forbrukerinteresser. Forskriftens § 4 angir følgende momenter det særlig skal legges vekt på ved utmåling av tvangsmulkt:

- hvilken type pålegg som ikke er etterkommet,
- hvor alvorlig unnlatelsen av å etterkomme pålegget er i forhold til de hensyn som pålegget skal ivareta,
- hvor byrdefullt det vil være for den næringsdrivende å etterkomme pålegget,
- den næringsdrivendes økonomiske evne, eventuelle fordeler ved ikke å etterkomme pålegget.

NSM mener de samme momentene bør vektlegges ved utmåling av tvangsmulkt etter cybersikkerhetssertifiseringsforskriften. NSM foreslår ikke et generelt maksimalt tak på tvangsmulktens størrelse i cybersikkerhetssertifiseringsforskriften, og mener at størrelsen kan variere for ulike sertifiseringsordninger. NSM mener utmålingen bør være opp til markedstilsynets skjønn, med mindre det ved gjennomføringen av en sertifiseringsordning fastsettes noe annet.

Se forslag til bestemmelse i § 10.

6.5.3 Overtredelsesgebyr

6.5.3.1 Bør det innføres generelle regler om overtredelsesgebyr?

Artikkel 58 nr. 8 bokstav f fastsetter at NCCA skal ha myndighet til å ilegge sanksjoner i samsvar med nasjonal rett, jf. artikkel 65. Det må fastsettes nasjonale regler for sanksjoner ved overtredelse av forordningen og sertifiseringsordninger, jf. artikkel 65. Sanksjonene skal være «virkningsfulle, stå i forhold til overtredelsen og virke avskrekkende». Digitalsikkerhetsloven § 19 bokstav c gir hjemmel til å ilegge overtredelsesgebyr ved overtredelse av krav til sikkerhetssertifisering. I likhet med pålegg og tvangsmulkt etter samme bestemmelse, må bestemmelsen forstås slik at det er anledning til å gi overtredelsesgebyr ved overtredelser av cybersikkerhetsforordningen generelt, og ikke utelukkende ved manglende etterlevelse av krav fastsatt i en sertifiseringsordning.

Det vises til Prop. 109 LS (2022–2023) punkt 9.5/side 45, hvor det uttales at «[o]vertredelsesgebyr 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».

I forarbeidene til EØS-vareloven, Prop. 17 L (2012-2013) s. 62, drøfter Nærings- og fiskeridepartementet sanksjoner ved uriktig bruk av CE-merking. Det vises til at de enkelte regelverkene som gjennomfører direktivene som omhandler CE-merking gir grunn til å reagere med overtredelser, men at reaksjonsform varierer for ulike varesektorer. Det innføres ikke generelle sanksjonsregler i EØS-vareloven. Sanksjonene for overtredelser av reglene for CE-merking varierer for ulike varesektorer, og inkluderer overtredelsesgebyr, bøter og fengsel.

I de nordiske landene varierer det hva slags sanksjoner overtredelser kan medføre. I lovforslaget til den danske loven som fastsetter supplerende bestemmelser til forordningen, Lovforslag nr. L 174 Folketinget 2020-21, drøftes behovet for økonomiske sanksjoner ved overtredelse av forordningen. Det vises til at omkostningene ved sertifisering generelt er en stor utgift for virksomhetene som søker sertifisering og at sertifisering er frivillig. Videre vurderes det at det mest effektive og rimelige rettsmiddel ved overtredelser av forordningen eller en sertifiseringsordning vil være å trekke tilbake sertifiseringen. I lovforslaget argumenteres det med at hensynet til en balansert løsning som både ivaretar sikkerhetshensyn, men også virksomhetenes konkurranse og vekstvilkår tilsier at en økonomisk straff ikke er rimelig. Det åpnes for at dette revurderes dersom noen sertifiseringsordninger senere gjøres obligatoriske.

Den svenske lovgivningen har gått i motsatt retning. I den svenske lovgivingen er det gjort obligatorisk for NCCA å utstede sanksjonsavgift dersom lovens vilkår for slik avgift er oppfylt. Sanksjonsavgiften skal være på minst 10 000 svenske kroner og maksimalt 15 millioner svenske kroner. I de svenske forarbeidene, Prop. 2020/21:186 s. 31-32, vises det til at sanksjonsavgifter vil medføre økt etterlevelse og mindre overtredelser av regelverket, samt at forbrukernes tillit til bransjen vil øke. Hva gjelder størrelsen på avgiften vises det til at regelverket vil gjelde svært forskjellige virksomheter, og for at det skal ha en tilstrekkelig avskrekkende effekt på de store virksomhetene er maksimumsbeløpet satt høyt. Tilsynsmyndighetene gis mulighet til en skjønnsmessig vurdering ved utmålingen.

NSM mener, slik de danske lovforarbeidene uttaler, at muligheten til å tilbaketrekke utstedte sertifikater kan være et vel så effektivt tiltak, som å ilegge økonomiske sanksjoner. Tilbaketrekking av sertifikater kan oppleves som en like alvorlig, eller verre konsekvens enn et overtredelsesgebyr, selv om en slik tilbaketrekning ikke kan anses som en sanksjon. Det må derfor vurderes konkret om hvilket behov det er for å reagere med overtredelsesgebyr opp mot muligheten til å tilbaketrekke sertifikater.

Pr. dags dato er det valgfritt for virksomheter å bli sertifisert eller utstede en egenerklæring om samsvar. Fordelen virksomheter kan oppnå ved sertifisering eller å utstede egenerklæring er av økonomisk art, da det kan fremme salg og bidra til godt omdømme. Virksomhetens potensielle vinning er at de kan vinne markedsandeler og anbud i konkurranse med andre virksomheter ved å tilby

sertifiserte IKT-produkter/tjenester/prosesser. Reaksjon med overtredelsesgebyr ved manglende oppfyllelse av krav i en sertifiseringsordning eller krav fastsatt i rammeverket for cybersikkerhetssertifisering, kan bidra til å sikre like konkurransevilkår og hindre urettmessig vinning.

Samtidig vil det innebære en økonomisk kostnad for virksomheter å bli sertifisert. Dersom tilsynsmyndigheten gis for vide fullmakter til å ilegge overtredelsesgebyr ved enhver forsømmelse, og gebyrets størrelse fastsettes for høyt, antar NSM at dette kan avskrekke virksomheter fra å søke om sertifisering. For samfunnet er det gunstig at flere virksomheter blir sertifisert, dersom dette innebærer at virksomhetene strekker seg for å oppfylle krav til digital sikkerhet som de ikke ville gjort om ikke sertifiseringsordningene krevde det.

Når det gjelder bestemmelsene i de ulike sertifiseringsordningene kan disse potensielt være svært ulike, slik at det på nåværende tidspunkt er usikkert om det finnes generelle bestemmelser i sertifiseringsordningene som bør utløse overtredelsesgebyr. Det foreslås derfor at det ved gjennomføringen av hver sertifiseringsordning i norsk rett, tas stilling til hvilke bestemmelser i gjennomføringsforordningen som kan utløse overtredelsesgebyr. Dette vil innebære at sanksjonene for overtredelse av de ulike sertifiseringsordningene kan variere fra sertifiseringsordning til sertifiseringsordning, på samme måte som overtredelser av regler om CE-merking er regulert.

Enkelte overtredelser av rammeverket for cybersikkerhetssertifisering kan det likevel være grunn til å regulere generelt i forskriften.

6.5.3.2 Når overtredelsesgebyr kan være aktuelt

Hensynet til forutberegnelighet tilsier at det fastsettes hvilke bestemmelser i forordningen som kan utløse overtredelsesgebyr. Det er markedstilsynet som vil kontrollere overholdelse av forskriften og hindre urettmessig bruk av sikkerhetssertifiseringer. Ved manglende medvirkning til markedstilsynets undersøkelser, som feilaktige eller uriktige opplysninger til tilsynsmyndigheten etter artikkel 58 nr. 8 bokstav a kan det være behov for å reagere. Det kan også være aktuelt dersom virksomheter ikke gir tilsynsmyndigheten tilgang til lokaler for å utføre tilsyn etter artikkel 58 nr. 8 bokstav d. I disse tilfelle mener NSM det er hensiktsmessig å kunne reagere med overtredelsesgebyr.

Der markedstilsynet har gitt en virksomhet pålegg om retting, og pålegget ikke blir etterlevd må det også kunne reageres. Avhengig av hvilket pålegg som er gitt, kan det både være aktuelt å trekke tilbake sertifikater, eller å ilegge overtredelsesgebyr.

Sertifiserte virksomheter har en plikt til å informere samsvarsvurderingsorganet om senere påviste sårbarheter eller uregelmessigheter, jf. artikkel 56 nr. 8. Selv om det er mulighet for å gi pålegg om at virksomheten skal oppfylle plikten, kan det også være et behov for å sanksjonere virksomheter for å forhindre fremtidige overtredelser. Dersom en virksomhet har unnlatt å opplyse om sårbarheter som ville ha gjort at et sertifikat blir trukket tilbake, vil virksomheten være feilaktig sertifisert i en periode de ikke oppfyller kravene. Dette tilsier at det kan reageres med overtredelsesgebyr for dette forhold.

Det følger allerede av forskrift om urimelig handelspraksis § 1 andre ledd nr. 2 at å fremvise et sertifikat, kvalitetsmerke eller tilsvarende uten å ha oppnådd nødvendig tillatelse er villedende handelspraksis, som under alle omstendigheter anses urimelig. Dette er forbudt etter markedsføringsloven § 6, og håndheves iht. denne loven. NSM forstår loven slik at den som utsteder en egenerklæring om samsvar i henhold til en sertifiseringsordning under rammeverket for cybersikkerhetssertifisering, uten å oppfylle vilkårene kan rammes av forbudet i markedsføringsloven § 6. Likevel mener NSM det kan være grunn til å regulere dette konkret i cybersikkerhetssertifiseringsforskriften for å tydeliggjøre dette.

De som utsteder egenerklæringer om samsvar vil ikke underlegges noen kontroll av et samsvarsvurderingsorgan, noe som kan gjøre terskelen for å utstede egenerklæring lavere. Det følger av cybersikkerhetsforordningens artikkel 53 nr. 2 at produsenten eller leverandøren påtar seg ansvaret for å oppfylle kravene i forordningen. Når terskelen for å utstede samsvarserklæring kan oppfattes som lavere, mener NSM det er enda viktigere at virksomhetene følges opp og at det kan ilegges overtredelsesgebyr til de som ikke oppfyller vilkårene.

6.5.3.3 Utmåling av overtredelsesgebyr

I forvaltningsloven § 44 andre ledd første punktum fremgår det at overtredelsesgebyr kan ilegges etter faste satser eller utmåles i det enkelte tilfelle (individuell utmåling) innenfor en øvre ramme som må fastsettes i eller i medhold av lov. Bakgrunnen for bestemmelsen er blant annet at handlingsrommet for skjønnsutøvelse ikke skal være videre enn nødvendig, jf. Prop. 62 L (2015–2016) side 86-87.

I norsk lovgivning varierer bestemmelsene for utmåling av overtredelsesgebyr.

Under Varepakken er det ikke fastsatt noen generell regel om utmåling av overtredelsesgebyr, slik at dette varierer fra produktregelverk til produktregelverk. I flere av regelverkene som gjennomfører varepakken er det fastsatt et overtredelsesgebyr på inntil 15 ganger folketrygdens grunnbeløp. Dette gjelder blant annet overtredelser av skipsutstyrsforskriften, REACH-forskriften og produktforskriften.

I andre regelverk er det knyttet til et prosentbeløp av virksomhetens omsetning. Dette gjelder for eksempel overtredelse av forskrift om EØS-krav til radioutstyr der grensen er fem prosent av foretakets omsetning. Ved overtredelser av markedsføringsloven mfl. er den maksimale rammen for gebyrets størrelse inntil fire prosent av den næringsdrivendes årsomsetning eller inntil 25 millioner kroner, der det høyeste beløpet anvendes. I konkurranseloven skilles det mellom overtredelser som utløser et gebyr på maksimalt 1 prosent, og overtredelser med maksimalt gebyr på 10 % av foretakets omsetning, jf. forskrift om utmåling og lempning av overtredelsesgebyr § 2 fastsatt med hjemmel i konkurranseloven.

NSM vurderer at bestemmelsene om manglende medvirkning til markedstilsyn, som manglende etterlevelse av opplysningsplikt overfor tilsynet, feilaktige eller ufullstendige opplysninger eller forhindring av adgang til lokaler, har likehetstrekk med de overtredelser i konkurranseloven som utløser et overtredelsesgebyr på inntil 1 prosent av virksomhetens omsetning.

Når det gjelder overtredelser der en virksomhet har utstedt egenerklæring om samsvar uten å oppfylle kravene eller en virksomhet har unnlatt å opplyse samsvarsvurderingsorganet om senere påviste sårbarheter, vil disse overtredelsene kunne ha ført til virksomhetens har fått en urettmessig økonomisk vinning. Det er derfor grunn til å reagere strengere på dette. Når det gjelder å utstede overtredelsesgebyr til virksomheter som ikke etterlever pålegg om retting, vil alvorlighetsgraden kunne variere stort. Maksimalt gebyr for overtredelser av digitalsikkerhetsloven er satt til 4 prosent. Slike overtredelser kan potensielt få stor negativ betydning for samfunnsviktige tjenester. Overtredelser av rammeverket for cybersikkerhetssertifisering anses som noe mindre alvorlig. For overtredelse av disse bestemmelsene foreslås et maksimalt gebyr på 3 prosent av virksomhetens omsetning.

Ved innføringen av de ulike sertifiseringsordningene må det tas stilling til om det er noen bestemmelser i disse ordningene som skal gi hjemmel til å utstede overtredelsesgebyr, og gebyrets størrelse.

Se forslag til bestemmelse i § 11.

6.6 Tilsyn med samsvarsvurderingsorganer

Digitalsikkerhetsloven § 19 bokstav b uttaler at Kongen kan gi forskrift om «tilsyn med sertifiseringsorganer som tilbyr sikkerhetssertifisering av IKT-produkter, IKT-tjenester og IKT-prosesser». Begrepet sertifiseringsorgan må forstås som det samme som et samsvarsvurderingsorgan.

Notifisering av samsvarsvurderingsorganer etter cybersikkerhetsforordningen skal gjøres i medhold av bestemmelsene i TKO-loven. Dette innebærer at den NCCA som tildeles en notifiserende myndighet, må notifisere samsvarsvurderingsorganer i medhold av både TKO-loven og bestemmelsene som kan følge av en sertifiseringsordning. TKO-loven gir «departementet» myndighet til å utpeke tekniske kontrollorgan. Ved innføringen av sertifiseringsordninger som tildeler en offentlig etat en rolle som notifiserende myndighet må departementet samtidig delegere myndighet etter TKO-loven til den offentlige etaten.

Det følger av TKO-loven § 3 at samsvarsvurderingsorganer kan pålegges å utarbeide rapporter og annen nødvendig dokumentasjon for å kontrollere virksomheten. Det følger av lovens § 4 at dersom organer ikke lenger oppfyller kravene som er satt for å være samsvarsvurderingsorgan eller om de opptrer i strid med regelverket, kan departementet gi pålegg om retting innen en nærmere fastsatt frist eller trekke tilbake autoriseringen.

Utpekte samsvarsvurderingsorganer etter TKO-loven har plikt til å samarbeide med den notifiserende myndigheten når det gjennomføres tilsyn. Den skal oppgi alle opplysningene myndigheten trenger for å kontrollere og utføre sine oppgaver, de skal samarbeide med myndigheten under revisjoner og gi myndigheten adgang til deres lokaler. Dersom et samsvarsvurderingsorgan ikke oppfyller disse kravene, vil det innebære å opptre i strid med regelverket, og myndigheten kan gi pålegg om retting eller trekke tilbake autoriseringen.

NSM har ikke sett behov for å innføre ytterligere generelle regler om sanksjoner enn de som følger av TKO-loven for samsvarsvurderingsorganer. Regler om sanksjoner kan eventuelt innføres ved innføringen av de enkelte sertifiseringsordningene.

6.7 Informasjonsutveksling mellom myndigheter og organer

Det er samsvarsvurderingsorganer som har ansvar for å trekke tilbake sertifikater de selv har utstedt. Som nevnt krever forordningen at det er et klart organisatorisk skille mellom samsvarsvurderingsorganer og tilsynsvirksomheten.

Dersom markedstilsynet mener at samsvarsvurderingsorganer bør trekke tilbake enkelte virksomheters sertifiseringer, kan markedstilsynet varsle samsvarsvurderingsorganer om dette. Det gjelder uavhengig av om det er et offentlig organ som er samsvarsvurderingsorgan eller private virksomheter. Det er opp til samsvarsvurderingsorganets selvstendige vurdering hva organet gjør med saken, men samsvarsvurderingsorganer har generelt en forpliktelse til å følge opp virksomheter de har sertifisert.

NSM mener at markedstilsynet bør ha en forpliktelse til å informere samsvarsvurderingsorganet om eventuelle avvik det har avdekket, slik at samsvarsvurderingsorganet får forutsetninger til å vurdere å trekke tilbake sertifiseringer.

For at markedstilsynet skal kunne følge opp de virksomhetene som har fått sertifisert et IKT-produkt, -tjeneste eller -prosess, må det ha kunnskap om hvilke virksomheter dette er. Det foreslås derfor en plikt for samsvarsvurderingsorganer til å informere det utpekte markedstilsynet om de sertifiseringene de utsteder. Dersom et samsvarsvurderingsorgan trekker tilbake et sertifikat bør også samsvarsvurderingsorganet informere markedstilsynet om dette.

Hva gjelder oppfølging av samsvarsvurderingsorganene er den notifiserende myndigheten avhengig av å vite om samsvarsvurderingsorganer er akkreditert og om de mister akkrediteringen. Det foreslås derfor en bestemmelse om at akkrediteringsorganet har en plikt til å informere den utpekte notifiserende myndigheten om samsvarsvurderingsorganer som mister akkrediteringen.

Se forslag til bestemmelse i § 7.

6.8 Vederlag for samsvarsvurdering

Samsvarsvurderinger utført av et offentlig samsvarsvurderingsorgan vil påføre staten utgifter. Cybersikkerhetsforordningen legger i stor grad opp til at samsvarsvurderinger utføres av private virksomheter, slik at de som søker sertifisering må betale markedspris for dette. Enkelte ordninger kan kreve at sertifisering utføres av enten en NCCA eller andre offentlige virksomheter.

Å få en sertifisering er et gode for virksomhetene som staten kan velge å tilby. Det er verken obligatorisk for virksomheter å få sertifisering eller for myndighetene å utføre sertifisering. Det er derfor ikke en selvfølge at staten skal bruke offentlige midler på dette. Brukerbetaling ved sertifisering kan gi insentiver for virksomhetene til å vurdere egen mulighet for å oppnå sertifisering grundigere før de søker, og det kan føre til en

mer effektiv søknadsprosess. En økt bevissthet hos virksomhetene før de søker om sertifisering kan medføre en økt bevissthet om kravene sertifiseringsordningene stiller. NSM vurderer at brukerbetaling for samsvarsvurdering vil føre til mindre statlige utgifter.

TKO-loven § 5 andre punktum gir hjemmel for at samsvarsvurderingsorganer kan ta vanlig betaling for samsvarsvurderingene. I forarbeidene til TKO-loven, Ot.prp. nr. 47 (1993-1994) s. 12, fremgår det at samsvarsvurderingsorgan kan ta betaling på forretningsmessig grunnlag.

For offentlige samsvarsvurderingsorganer vil det ikke være naturlig å ta betaling på forretningsmessig grunnlag, og reglene for disse kan skille seg noe fra private samsvarsvurderingsorganer. Det er likevel grunn til at også offentlige samsvarsvurderingsorganer kan ta vederlag.

På bakgrunn av det ovenstående foreslås det at virksomhetene som søker sertifisering utført av offentlige virksomheter skal dekke statens kostnader ved sertifiseringen. Dersom en sertifiseringsordning blir gjort obligatorisk bør det vurderes særskilt om de offentlige samsvarsvurderingsorganene kan ta vederlag.

Se forslag til bestemmelse i § 8.

6.9 Klage

Forvaltningsloven gjelder for «virksomhet som drives av forvaltningsorganer», jf. fvl. § 1. Alle myndighetsoppgavene vil utføres av statlige organer eller på vegne av statlige organer, og forvaltningsloven vil komme til anvendelse.

Fysiske og juridiske personer har rett til å klage til samsvarsvurderingsorganet som utsteder det aktuelle sertifikatet, jf. artikkel 63. Dette kan typisk være der virksomheter vil klage på manglende utstedelse av sertifikat eller tilbaketrekning av et sertifikat. Dersom et sertifikat skal utstedes av et samsvarsvurderingsorgan etter forhåndsgodkjenning eller delegering iht. artikkel 56 nr. 6, skal klagen rettes til NCCAs utpekte samsvarsvurderingsorgan under sertifiseringsordningen. Etter artikkel 63 nr. 2 skal myndigheten eller organet som mottar klagen informere klageren om saksforløpet og om beslutningen som er truffet, og om retten til effektive rettsmidler etter artikkel 64.

Etter TKO-loven § 5 gjelder klagereglene i forvaltningsloven for samsvarsvurderinger utført av notifiserte samsvarsvurderingsorganer. Forvaltningsloven kapittel VI regulerer følgelig disse forhold. Det følger av forarbeidene til TKO-loven, Ot.prp.nr.47 (1993-1994) s. 12 at ansvarlig departement er klageorgan, med mindre det opprettes andre særskilte klageorgan.

Dersom samsvarsvurderingsorganet er en NCCA, vil kravet om at den notifiserende myndigheten og samsvarsvurderingsorganet skal være helt adskilt tale for at det er en annen virksomhet enn den som utfører sertifiseringen som er overordnet klageorgan. Det bør fastsettes særskilt hvem som er overordnet klageinstans dersom samsvarsvurderingsorganet og den notifiserende myndigheten tillegges samme etat, jf. forvaltningsloven § 28 fjerde ledd.

Sanksjoner og vedtak fattet av markedstilsynet vil være enkeltvedtak etter forvaltningsloven § 2 første ledd bokstav b. Forvaltningsloven kommer til anvendelse på saksbehandlingen, og forvaltningslovens kapittel VI om klage og omgjøring er gjeldende. Overordnet klageinstans er «det forvaltningsorgan (klageinstansen) som er nærmest overordnet», jf. fvl § 28 første ledd. Det er mulig å fastsette regler som avviker fra dette ved gjennomføringen av de enkelte sertifiseringsordningene, jf. forvaltningsloven § 28 fjerde ledd.

Det anses ikke påkrevd å fastsette i forskrift at forvaltningslovens klageregler kommer til anvendelse.

7 Sertifisering av administrerte sikkerhetstjenester

7.1 Gjeldende rett

Digitalsikkerhetsloven skal etter § 1 første punktum 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 etter andre punktum også legge til rette for sikkerhet i IKT-produkter, IKT-tjenester og IKT-prosesser.

Etter digitalsikkerhetsloven § 18 bokstav f kan Kongen gi forskrift om gjennomføring av forpliktelser som følger av EØS-avtalen og andre internasjonale avtaler, og som understøtter lovens regler eller formål.

Etter digitalsikkerhetsloven § 19 første punktum kan Kongen gi forskrift om sikkerhetssertifisering av IKT-produkter, IKT-tjenester og IKT-prosesser for å gjennomføre forpliktelser etter EØS-avtalen. Etter annet punktum omfatter dette blant annet utpeking av sertifiseringsmyndighet, tilsyn med sertifiseringsorganer som tilbyr sikkerhetssertifisering av IKT-produkter, IKT-tjenester og IKT-prosesser og pålegg om retting, tvangsmulkt og overtredelsesgebyr ved overtredelse av krav til sikkerhetssertifisering.

Hensikten med omtalte bestemmelser er å sikre at lovens formål reflekterte cybersikkerhetsforordningens formål knyttet til cybersikkerhetssertifisering og ga hjemmel til å gjennomføre cybersikkerhetsforordningen, med tilhørende gjennomføringsrettsakter, ved forskrift.

7.2 Behov for og forslag til endringer

Endringsforordning (EU) 2025/37 gjør endringer i cybersikkerhetsforordningen ved å inkludere administrerte sikkerhetstjenester i EUs rammeverk for cybersikkerhetssertifisering.

Digitalsikkerhetslovens bestemmelser som legger til rette for gjennomføring av cybersikkerhetsforordningen som forskrift har i sin ordlyd begrenset seg til sikkerhetssertifisering av IKT-produkter, -tjenester og -prosesser. Det kan imidlertid tenkes at digitalsikkerhetsloven § 18 bokstav f er tilstrekkelig for å hjemle

inkorporeringen, da denne har en videre ordlyd. Digitalsikkerhetsloven § 18 er avgrenset til å gi forskrift som understøtter lovens regler eller formål, hvilket innebærer at det også skal kunne gis forskrift som understøtter de øvrige bestemmelsene i loven, slik som f.eks. krav til sikkerhet. Det å tilrettelegge for sikkerhetssertifisering av tilbydere av administrerte sikkerhetstjenester er nettopp ment å bidra til at tilbydere av samfunnsviktige tjenester kan ta gode valg når de skal håndtere sikkerhetskrav.

Samtidig er loven innrettet slik at hjemmel til å regulere sertifiseringsordninger har særskilte bestemmelser, noe som taler for at det er disse som setter rammen for forskriftsregulering av cybersikkerhetssertifisering. For å fjerne usikkerhet og sikre at loven også hjemler gjennomføring av sertifiseringsordninger om administrerte sikkerhetstjenester, bør ordlyden i digitalsikkerhetsloven endres tilsvarende.

Endringsforordningen er ikke innlemmet i EØS-avtalen, men det vurderes likevel hensiktsmessig å sende på høring forslag til nødvendige endringer i digitalsikkerhetsloven i påvente av slik innlemmelse. Endringene er følgelig forutsatt av at endringsforordningen formelt innlemmes i EØS-avtalen.

Endringsforordningen endrer ikke forpliktelsene i cybersikkerhetsforordningen. Forordningen er knyttet til NIS2-direktivet gjennom at tilbydere av administrerte sikkerhetstjenester er en virksomhetskategori omfattet av vedlegg I til direktivet (under sektor/samfunnsområdet «Forvaltning av IKT-tjenester»). I tillegg er definisjonen av «administrerte sikkerhetstjenester» i forordningen avledet fra og nært knyttet til definisjonen av «leverandører av administrerte sikkerhetstjenester» i NIS2.

Som det fremgår i fortalepunkt 86 i NIS2-direktivet spiller tilbydere av administrerte sikkerhetstjenester en viktig rolle i å bistå virksomheter i deres arbeid med å forebygge, oppdage, reagere på eller gjenopprette etter hendelser. Disse tilbyderne er imidlertid også et mål for cyberangrep selv.

Endringsforordningen tar sikte på å forbedre kvaliteten og sammenlignbarheten av administrerte sikkerhetstjenester og åpner dermed for at virksomheter underlagt NIS2 kan utøve økt aktsomhet ved valg av leverandør av administrerte sikkerhetstjenester, slik det kreves i direktivet.

Det skal også nevnes at endringsforordningen også utfyller cybersolidaritetsforordningen (EU) 2025/38. Etter cybersolidaritetsforordningen skal det etableres en cybersikkerhetsreserve på EU-nivå, som blant annet bør ta hensyn til om relevante leverandører i reserven har en europeisk eller nasjonal cybersikkerhetssertifisering. Fremtidige sertifiseringsordninger for administrerte sikkerhetstjenester vil derfor spille en viktig rolle i gjennomføringen av cybersolidaritetsforordningen.

På bakgrunn av dette foreslås det at i opplistingen i § 1 andre punktum legges til «administrerte sikkerhetstjenester». Tilsvarende at det i § 19 legges til «administrerte sikkerhetstjenester» i opplistingen av hva Kongen kan gi forskrifter om sikkerhetssertifisering av.

Videre foreslås det at endringsforordningen inkorporeres i nasjonal rett som forskrift til digitalsikkerhetsforskriften. Se forslag til inkorporeringsbestemmelse i forslag til ny forskrift om cybersikkerhetssertifisering § 1.

8 Økonomiske og administrative konsekvenser

Etter NSMs vurdering vil gjennomføring av cybersikkerhetsforordningen i norsk rett ikke medfører store økonomiske konsekvenser for næringslivet, men ha positive konsekvenser for norsk næringsliv som er leverandører eller produsenter av IKT-produkter, IKT-tjenester, IKT-prosesser og administrerte sikkerhetstjenester.

Sertifisering i henhold til forordningen er inntil videre frivillig, og skal sikre et velfungerende indre marked ved å øke cybersikkerhetsnivået i EU/EØS, og etablere et harmonisert og felles rammeverk for cybersikkerhetssertifisering. Forordningen vil derfor virke positivt inn på deres konkurranseevne i EU/EØS.

Særnasjonale cybersikkerhetssertifiseringsordninger vil på sikt opphøre, etter hvert som Kommisjonen vedtar sertifiseringsordninger på ulike områder. I dag kan kostnadene knyttet til ulike særnasjonale sertifiseringsordninger i EU/EØS gjøre at terskelen for å søke om sertifisering er høy. Et felles europeisk rammeverk for cybersikkerhetssertifisering, vil sørge for at det holder med én sertifisering i EU/EØS for å kunne konkurrere i hele det indre markedet. Rammeverket for cybersikkerhetssertifisering kan lette markedsadgangen innen EU/EØS-området og redusere virksomheters kostander til sertifisering.

Konsekvensene for samsvarsvurderingsorganer som er etablert i Norge, er at det kan åpnes nye virksomhetsområder for disse, noe også norske teknologibedrifter kan nyte godt av.

Etter NSMs vurdering vil gjennomføring av cybersikkerhetsforordningen i utgangspunktet ikke medføre store konsekvenser for staten på nåværende tidspunkt. Cybersikkerhetsforordningen krever at staten utpeker minst én nasjonal cybersikkerhetssertifiseringsmyndighet. Som det fremgår av høringsnotatet foreslår NSM at det utpekes én myndighet som tildeles en nasjonal rolle. Oppgavene til den nasjonale myndigheten er beskrevet i kapittel 5.7. Den nasjonale myndigheten vil måtte sette av noen ressurser til å følge opp disse oppgavene.

Den fleksible forvaltningsstrukturen som foreslås, krever et fremtidig samarbeid mellom den nasjonale myndighet og andre etater. Den fleksible forvaltningsstrukturen legger også opp til et samarbeid på tvers av departementsområder. Når sertifiseringsordningene etter hvert vedtas, vil oppfølging av myndighetsoppgavene etter forordningen innebære økonomiske og administrative konsekvenser for forvaltningsorganene som får tildelt disse myndighetsoppgavene.

På grunn av stor fleksibilitet i hvordan myndighetene kan utføre sine oppgaver etter forordningen, er det ikke mulig å vurdere ressursbehovet på nåværende tidspunkt. Det understrekes imidlertid at hver sertifiseringsordning vil være gjenstand for en alminnelig utrednings- og høringsprosess, der økonomiske og administrative

konsekvenser for hver sertifiseringsordning og myndighet vil måtte utredes. Det pålegges således ikke myndighetsoppgaver etter sertifiseringsordningene på nåværende tidspunkt, men kan bli aktuelt ved fremtidig implementering av sertifiseringsordninger.

Kravet i artikkel 60 nr. 1 som fastsetter at samsvarsvurderingsorganene skal akkrediteres av det nasjonale akkrediteringsorganet vil ha økonomiske konsekvenser Norsk akkreditering, bl.a. som følge av etablering av nye akkrediteringsområder.

Avslutningsvis nevnes at gjennomføringen av cybersikkerhetsforordningen vil kunne gjøre det lettere for offentlige virksomheter å stille og evaluere krav til cybersikkerhet ved IKT-produkter, -tjenester, -prosesser og administrerte sikkerhetstjenester i offentlige anskaffelsesprosesser.

Forslag til forskrift om cybersikkerhetssertifisering

Hjemmel: Fastsatt av Kongen [dato] med hjemmel i lov 20. desember 2023 nr. 108 om digital sikkerhet (digitalsikkerhetsloven) § 18 og § 19 og lov 16. juni 1994 nr. 20 om tekniske kontrollorgan som har til oppgåve å gjennomføre samsvarsvurderingar § 7.

§ 1. Gjennomføring av EØS-regler om cybersikkerhetssertifisering

Forordning (EU) 2019/881 om ENISA (den europeiske unions byrå for nett- og informasjonssikkerhet), om cybersikkerhetssertifisering av informasjons- og kommunikasjonsteknologi og om opphevelse av forordning (EU) nr. 526/2013 (cybersikkerhetsforordningen), som inntatt i EØS-avtalens vedlegg XI nr. 5cp, gjelder som forskrift. Forordningen gjelder med de tilpasninger som følger av vedlegg XI, protokoll 1 til avtalen og avtalen for øvrig, og med de endringene som følger av forordning (EU) 2025/37.

§ 2. *Akkrediteringsorgan*

Nasjonalt akkrediteringsorgan etter lov av 12. april 2013 nr. 13 om det frie varebytte i EØS (EØS-vareloven) skal akkreditere samsvarsvurderingsorganer etter cybersikkerhetsforordningen artikkel 60.

§ 3. Nasjonale cybersikkerhetssertifiseringsmyndigheter

XX er nasjonal cybersikkerhetssertifiseringsmyndighet, jf. artikkel 58.

§ 4. Markedstilsynsmyndigheter

Markedstilsynsmyndighetene har de fullmakter som følger av cybersikkerhetsforordningen artikkel 58 nr. 8.

Markedstilsynsmyndighetene skal innenfor den enkelte sertifiseringsordning treffe egnede tiltak overfor innehavere av sertifikater eller utstedere av EU-samsvarserklæringer, for å sikre overholdelse av bestemmelser i cybersikkerhetsforordningen eller sertifiseringsordninger, jf. artikkel 58 nr. 8 bokstav c.

§ 5. Samsvarsvurderingsorganer

Samsvarsvurderingsorganet kan trekke tilbake sertifikater organet selv har utstedt eller sertifikater utstedt av samsvarsvurderingsorganer i samsvar med artikkel artikkel 58 nr. 8 bokstav e.

§ 6. Utpeking og tilsyn med samsvarsvurderingsorganer

Den notifiserende myndigheten peker ut og fører tilsyn med samsvarsvurderingsorganer etter lov 16. juni 1994 nr. 20 om tekniske kontrollorgan som har til oppgåve å gjennomføre samsvarsvurderingar og forordning (EU) 2019/881 (cybersikkerhetsforordningen).

§ 7. Informasjonsutveksling mellom myndigheter og organer

Markedstilsynsmyndigheten skal informere det aktuelle samsvarsvurderingsorganet om eventuelle avvik det avdekker hos produsenter og leverandører som har fått sertifisert IKT-produkter, IKT-tjenester eller IKT-prosesser.

Samsvarsvurderingsorganer skal informere markedstilsynsmyndigheten om sertifikatene den utsteder og sertifikater den trekker tilbake.

Akkrediteringsorganet skal informere den notifiserende myndigheten om samsvarsvurderingsorganer som mister akkrediteringen.

§ 8. Vederlag for samsvarsvurderinger

Offentlige samsvarsvurderingsorganer kan ta vederlag for å dekke organets kostnader ved samsvarsvurderinger. For andre samsvarsvurderingsorganer gjelder reglene i lov 16. juni 1994 nr. 20 om tekniske kontrollorgan som har til oppgåve å gjennomføre samsvarsvurderingar § 5.

Vederlaget er tvangsgrunnlag for utlegg.

§ 9. Pålegg

Markedstilsynsmyndigheten kan gi produsenter og leverandører av sertifiserte IKT-produkter, IKT-tjenester, IKT-prosesser og administrerte sikkerhetstjenester pålegg om retting ved brudd på forskriften.

Der en produsent eller leverandør har utstedt EU-samsvarserklæring, men ikke oppfyller kravene som følger av sertifiseringsordningen, kan markedstilsynsmyndigheten pålegge produsenten eller leverandøren å trekke EU-samsvarserklæringen tilbake, og forby markedsføring som gir uttrykk for at administrerte sikkerhetstjenester, IKT-produktet, -tjenesten eller -prosessen oppfyller kravene til sertifiseringsordningen.

§ 10. Tvangsmulkt

Markedstilsynsmyndigheten kan treffe vedtak om tvangsmulkt for å sikre at pålegg etter § 9 blir oppfylt.

Tvangsmulkten kan fastsettes som en løpende tvangsmulkt for hver dag/uke/måned som går etter utløpet av den frist som er satt for oppfylling av pålegget, inntil pålegget er oppfylt.

Markedstilsynsmyndigheten kan i særlige tilfeller frafalle påløpt tvangsmulkt.

§ 11. Overtredelsesgebyr

Markedstilsynsmyndigheten kan ilegge produsenter eller leverandører overtredelsesgebyr på inntil 1 prosent av foretakets omsetning dersom foretaket eller noen som handler på dennes vegne, forsettlig eller uaktsomt:

a) gir feilaktige eller ufullstendige opplysninger til markedstilsynsmyndigheten, når myndigheten trenger opplysningene for å utføre sine oppgaver jf. artikkel 58 nr. 8 bokstav a og b.
b) hindrer markedstilsynsmyndigheten tilgang til lokaler som når myndigheten skal utføre undersøkelser jf. artikkel 58 nr. 8 bokstav d.

Markedstilsynsmyndigheten kan ilegge produsenter eller leverandører overtredelsesgebyr på inntil 3 prosent av foretakets omsetning dersom foretaket eller noen som handler på dennes vegne, forsettlig eller uaktsomt:

a) ikke etterkommer pålegg etter § 9.
b) overtrer forpliktelsen til å informere om påviste sårbarheter eller uregelmessigheter etter artikkel 56 nr. 8.
c) utsteder en EU-samsvarserklæring etter artikkel 53 uten at kravene som følger av sertifiseringsordningen er oppfylt.

Omsetningen er foretakets samlede årsomsetning i det forutgående regnskapsåret.

§ 12. Ikrafttredelse

Forskriften trer i kraft fra den tid Kongen bestemmer.

Forslag til endring av ekomforskriften

I forskrift 20. desember 2024 nr. 3410 om elektroniske kommunikasjonsnett og elektroniske kommunikasjonstjenester gjøres følgende endringer:

Paragraf 2-11 oppheves.

Forslag til endring av lov om digital sikkerhet (digitalsikkerhetsloven)

I lov 20. desember 2023 nr. 108 om digital sikkerhet (digitalsikkerhetsloven) foreslås følgende endringer:

I kapittel 1. Innledende bestemmelser skal § 1 første ledd andre punktum skal lyde:

Loven skal også legge til rette for sikkerhet i IKT-produkter, IKT-tjenester, IKT-prosesser *og administrerte sikkerhetstjenester*.

I kapittel 6. Sikkerhetssertifisering skal § 19 første ledd første punktum lyde:

Kongen kan gi forskrift om sikkerhetssertifisering av IKT-produkter, IKT-tjenester, IKT-prosesser og *administrerte sikkerhetstjenester* 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, IKT-prosesser og *administrerte sikkerhetstjenester*
c. pålegg om retting, tvangsmulkt og overtredelsesgebyr ved overtredelse av krav til sikkerhetssertifisering.