EU-rettsakter som etter en foreløpig oversikt vil kunne behandles i EØS-komiteen 3. februar 2023

I det nedenstående følger oversikt inndelt som følger:

Under pkt. I følger rettsakter som krever lov- eller budsjettendring, samt rettsakter som krever forskriftsendring som vurderes å gripe vesentlig inn i norsk handlefrihet.

Under pkt. II følger rettsakter som krever forskriftsendring som ikke griper vesentlig inn i norsk handlefrihet, samt rettsakter som ikke har konsekvenser for norsk lovgivning.

Innhold

I. Rettsakter som krever lov- eller budsjettendring samt rettsakter som krever forskriftsendring som vurderes å gripe vesentlig inn i norsk handlefrihet

JUSTIS OG BEREDSKAPSDEPARTEMENTET

32016L1148 Europaparlaments- og rådsdirektiv (EU) 2016/1148 av 6. juli 2016 om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i hele Unionen

Status

Direktivet ble vedtatt i EU 6. juli 2016. Standardskjema ble levert til EFTA-sekretariatet 20. desember 2016.

Justis- og beredskapsdepartementet deltar på vegne av Norge i en ad-hoc NIS ekspertgruppe nedsatt av kommisjonen.

Rettsakten er under vurdering i EØS/EFTA-statene.

EØS-komiteen forventes 3.februar 2023 å treffe beslutning om innlemmelse av NIS-direktivet i EØS-avtalen. Beslutningen gjør tilføyelser til EØS-avtalens vedlegg XI og protokoll 37.

Sammendrag av innhold

Direktivet pålegger medlemsstatene å sørge for et visst nivå for landets IKT-sikkerhet ved å lage en strategi for sikkerhetsarbeidet, etablere en IKT-sikkerhetsberedskapsenhet (CSIRT) og pålegge operatører og leverandører av samfunnsviktige tjenester IKT-sikkerhetskrav og varslingsplikt ved alvorlige IKT-sikkerhetshendelser. Direktivet etablerer to internasjonale samarbeidsgrupper, en på strategisk nivå og en på CSIRT-nivå.

Grunnet behovet for lovendring tas det forbehold om Stortingets samtykke til å innlemme rettsakten i EØS-avtalen, jf. EØS-avtalen art. 103.

Bakgrunn og formål

Den 7. februar 2013 lanserte EU-kommisjonen EUs strategi for cybersikkerhet, *An Open, Safe and Secure Cyberspace*. Som ett av flere tiltak for å nå målene i strategien lanserte Kommisjonen samtidig et forslag til direktiv om tiltak for et høyt felles sikkerhetsnivå i nettverks- og informasjonssystemer i EU (NIS-direktivet). Direktivet ble vedtatt i EU 6. juli 2016.

Bakgrunnen for forslaget til direktivet er at det i dag, innen EU, ikke er implementert tilstrekkelige og helhetlige beskyttelsestiltak for å oppnå god nok sikkerhet i nettverk og informasjonssystemer som er særlig viktige for det indre markeds funksjon. Utfordringene er ikke bare grenseoverskridende, men globale. Medlemslandene har ulik kvalitet på de

beskyttelsestiltak som er implementert, hvilket medfører en fragmentert tilnærming på EU-nivå. Det er behov for felleseuropeiske regler om IKT-sikkerhet også for annen type infrastruktur.

Formålet med direktivet er å forbedre det indre markeds funksjon gjennom etableringen av et høyt felles sikkerhetsnivå i viktige nettverks- og informasjonssystemer. Direktivet setter krav til medlemslandenes arbeid med IKT-sikkerhet, til virksomheter som leverer tjenester som er essensielle for det indre markeds samfunnsmessige og økonomiske aktiviteter og til tilbydere av enkelte digitale tjenester. Det er særlig fokus på å sikre kontinuitet i leveransen av de aktuelle tjenestene. Et høyt felles IKT-sikkerhetsnivå skal gjøre EU mer konkurransedyktig i en globalisert verden, skape tillit til digitale tjenester og bidra til økonomisk vekst i Europa.

Innhold

1. Nasjonale rammeverk for sikkerhet i nettverks- og informasjonssystemer (NIS), jf. kap. II (art. 7 til 10)

Medlemsstatene skal sørge for at de har et minimum av nasjonal kapasitet for å møte IKT-sikkerhetsutfordringer ved å:

- utarbeide en nasjonal NIS-strategi
- opprette en nasjonal kompetent myndighet for nettverks- og informasjonssikkerhet
- opprette ett nasjonalt kontaktpunkt
- opprette minst en IKT-beredskapsenhet (Computer Security Incident Response Team - CSIRT).

Dersom oppgavene til den nasjonale kompetente myndigheten, CSIRTen og det nasjonale kontaktpunktet nasjonalt er fordelt på flere virksomheter, skal disse samarbeide om gjennomføringen av direktivet.

2. Samarbeid mellom medlemslandene og mellom CSIRTene, jf. kap. III (art. 11 til 13)

For å legge til rette for strategisk samarbeid og utvikling av tillit mellom medlemsstatene etablerer direktivet en samarbeidsgruppe med representanter fra medlemslandene, Kommisjonen og det europeiske byrået for nettverks- og informasjonssikkerhet (ENISA). Kommisjonen ivaretar sekretariatsfunksjonen. Samarbeidsgruppa skal blant annet utarbeide en handlingsplan for implementering av direktivet, utarbeide strategiske råd til CSIRT-nettverket, utveksle best-practice om informasjonsdeling relatert til hendelseshåndtering og utveksling av best-practice om kapasitetsbygging. Se videre art. 11.

For å fremme rask og effektiv operativt samarbeid samt utvikling av tillit mellom medlemslandene etablerer direktivet også et CSIRT-nettverk bestående av representanter fra de nasjonale CSIRTene og CERT-EU. Kommisjonen deltar som observatør og ENISA står for sekretariatet. Nettverkets arbeidsoppgaver vil blant annet bestå av informasjonsdeling om CSIRTenes tjenester, operasjoner og samarbeidskapasiteter, informasjonsdeling om hendelser og samarbeid om felles respons mot hendelser. Se videre art. 12.

3. Virksomheters nettverks- og informasjonssystemsikkerhet, jf. kap IV og V (art. 14 til 18)

Det følger av NIS-direktivet art. 1(3) at virksomheter som faller inn under virkeområdet til rammedirektivet 2002/21/EF og dermed må oppfylle sikkerhetskravene i art. 13a og 13b, er unntatt fra NIS-direktivet. Det samme gjelder tilbydere av tillitstjenester som faller inn under virkeområdet i Europaparlaments- og Rådsforordning (EU) nr. 910/2014 om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked og opphevelse av direktiv 1999/93/EF (EIDAS-forordningen), jf. NIS-direktivet art. 1(4). Det følger videre av art. 1(7) et lex specialis-unntak for virksomheter som er underlagt sektorspesifikt EU-regelverk, der dette regelverket stiller minst tilsvarende krav til sikkerhet og varsling. Dersom lex specialis-reglene fullt ut kommer til anvendelse, er det ikke nødvendig å identifisere virksomheter som er omfattet av det sektorspesifikke EU-regelverket.

3.1 Sikkerhet i nettverk og informasjonssystemer tilhørende tilbydere av samfunnsviktige tjenester (operators of essential services), se kap. IV.

Direktivet pålegger medlemsstatene å sørge for at tilbydere av samfunnsviktige tjenester, jf. vedlegg II til direktivet, iverksetter flere sikkerhetstiltak, herunder risikostyring og varslingsplikt om hendelser som har vesentlig virkning (significant impact). Dette er virksomheter som anses særlig viktige for opprettholdelsen av et funksjonsdyktig indre marked og hvis bortfall kan få alvorlige negative konsekvenser for samfunnssikkerheten og økonomiske og samfunnsmessige aktiviteter. Vedlegg II til direktivet inneholder følgende sektorer:

- Energi (*elektrisitet, olje og gass*)
- Transport (*luft, jernbane, sjø og vei*)
- Helse (*helsetjenester*)
- Bank
- Finansmarkedsinfrastruktur
- Drikkevannsforsyning og -distribusjon
- Digital infrastruktur (*IXP, DNS og TLD*)

3.1.1 Virkeområde - Tilbydere av samfunnsviktige tjenester

Det endelige virkeområdet for direktivet blir fastlagt gjennom en utpekingsprosess i regi av hver enkelt medlemsstat, jf. art. 5. Som et minimum skal virksomheter som faller inn under direktivets vedlegg II vurderes. Det skilles ikke mellom offentlige og private virksomheter.

En virksomhet defineres som tilbyder av en samfunnsviktig tjeneste dersom følgende kumulative kriterier er oppfylt, jf. art. 5(2) :
1. Virksomheten tilbyr en tjeneste som er viktig for opprettholdelsen av kritiske samfunnsmessige og/eller økonomiske aktiviteter,
2. tjenesteleveransen er avhengig av nettverk og informasjonssystemer, og

3. en hendelse i tjenestens nettverk og informasjonssystemer ville hatt *vesentlig forstyrrende virkning* på tjenesteleveransen

For å oppfylle punkt 1 synes det ut i fra direktivets premiss (20) tilstrekkelig å fastslå at virksomheten faktisk leverer en samfunnsviktig tjeneste som er opplistet i direktivets vedlegg II.

Ved vurderingen av om en sikkerhetshendelse kan få vesentlig forstyrrende virkning på tjenesteleveransen skal både tverrsektorielle og sektorspesifikke momenter tas i betraktning. Art. 6 oppstiller en ikke uttømmende liste med tverrsektorielle momenter som skal vurderes:

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

Medlemsstatene plikter å opprette en liste over alle tilbydere av samfunnsviktige tjenester. Listen skal oppdateres jevnlig og minst hvert andre år.

For å gjøre Kommisjonen i stand til å evaluere gjennomføringen av direktivet skal medlemslandene innen 9. november 2018 rapportere til kommisjonen blant annet:

- om hvilke tiltak som er iverksatt for utpeking
- liste over essensielle tjenester (ikke de konkrete operatørene)
- antall operatører i hver sektor

3.1.2 Sikkerhetstiltak

Direktivet stiller generelle og overordnede krav til sikkerheten i virksomhetene. Blant annet gjennom innføring av krav om risikostyring, skal medlemsstatene sørge for at tilbydere av samfunnsviktige tjenester iverksetter sikkerhetstiltak som står i et rimelig forhold til risikoen den enkelte virksomhet står overfor. Det skal også iverksettes tiltak for å forebygge og minimere virkningen av hendelser i nettverk og informasjonssystemer, med henblikk på opprettholdelse av tjenesteleveransen. Se nærmere art. 16(1) og (2).

For å legge til rette for harmonisert gjennomføring av art. 16(1) og (2), skal medlemsstatene fremme bruk av europeiske og internasjonale standarder. ENISA skal bistå med rådgivning og retningslinjer.

Medlemsstatene skal videre sørge for at tilbydere av samfunnsviktige tjenester uten ugrunnet opphold varsler om alvorlige hendelser. Vurderingskriteriene for hendelsens alvorlighet er:

- antallet brukere som er rammet av hendelsen
- hendelsens varighet
- det geografiske området som er rammet

Dette betyr altså at det kun skal varsles om hendelser som faktisk innvirker negativt på tjenesteleveransen. Det skal ikke varsles om fare for slik virkning, ei heller kompromittering av konfidensialitet, tilgjengelighet eller integritet der dette ikke har betydning for tjenesteleveransen. Det er den forhåndsbestemte kompetente myndigheten eller CSIRTen som skal varsles.

Dersom hendelsen også fører til brudd på personvernet skal den kompetente myndigheten samarbeide med personvernmyndighetene.

3.2 Sikkerhet i nettverk og informasjonssystemer tilhørende tilbydere av digitale tjenester, se kap. V.

Direktivet pålegger medlemsstatene å sørge for at også tilbydere av digitale tjenester, jf. vedlegg III til direktivet, iverksetter flere sikkerhetstiltak, herunder risikostyring og varslingsplikt om svært alvorlige hendelser. Det går tydelig frem av premissene til direktivet at det skal stilles lavere sikkerhetskrav til disse tjenestene da de anses noe mindre viktige enn tjenestene omtalt i 3.1. Den kompetente myndigheten skal kun kontrollere disse virksomhetene dersom den får klare indikasjoner på at direktivets krav ikke er fulgt. Det forutsettes dessuten i premiss (57) at sikkerhetsnivået for denne kategorien virksomheter skal harmoniseres i EU gjennom utarbeidelse av gjennomføringsregler. ENISA har satt i gang med dette arbeidet på oppdrag fra Kommisjonen.

3.2.1 Virkeområde - Tilbydere av digitale tjenester

For denne kategorien skal medlemsstatene ikke foreta en utpeking av virksomheter. Direktivbestemmelsene skal gjelde alle virksomheter som faller inn under vedlegg III:

1. Nettbaserte markedsplasser, jf. art. 4(17)
2. Nettbaserte søkemotorer, jf. art. 4(18)
3. Skytjenester, jf. art. 4(19)

3.2.2 Sikkerhetstiltak

Medlemsstatene skal sørge for at tilbydere av digitale tjenester iverksetter sikkerhetstiltak som står i et rimelig forhold til risikoen virksomheten står overfor. Også overfor denne gruppen virksomheter skal det stilles krav om risikostyring. Det skal også iverksettes tiltak for å forebygge og minimere virkningen av hendelser i nettverk og informasjonssystemer, med henblikk på opprettholdelse av tjenesteleveransen.

Til forskjell fra tilbydere av samfunnsviktige tjenester kan medlemslandene, med visse unntak, ikke innføre strengere sikkerhetstiltak for tilbydere av digitale tjenester enn det direktivet legger opp til. Noe av begrunnelsen er at det for tilbydere av digitale tjenester er behov for unionsuniforme sikkerhetskrav.

Tilbydere av digitale tjenester skal også varsle en på forhånd bestemt kompetent myndighet om alvorlige hendelser. For tilbydere av digitale tjenester skal det i tillegg til nevnte momenter for tilbydere av samfunnsviktige tjenester også ses hen til:

- omfanget av forstyrrelsen for tjenestens funksjon
- omfanget av virkningen for økonomiske og samfunnsmessige aktiviteter

4. Gjennomføring av direktivet

For å sørge for like forutsetninger for gjennomføring av direktivet skal Kommisjonen, i henhold til premiss (68), utarbeide prosessuelle retningslinjer for Samarbeidsgruppen (art. 11) og for utarbeidelse av sikkerhets- og varslingskrav for tilbydere av digitale tjenester. Kommisjonen skal rådføre seg med ENISA.

5. Kort om andre regler

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

Behandling av personopplysninger skal etter art. 2 gjennomføres i samsvar med personverndirektivet 95/46/EF. Personverndirektivet er erstattet av EUs personvernforordning (EU) 2016/79, jf. personvernforordningen artikkel 94 og fortalepunkt 171.

Merknader og betydning for Norge forutsatt EØS-relevans

Hjemmel i EU-traktaten

Rettsakten er hjemlet i TFEU art. 114.

Gjeldende norsk lovgivning og politikk

1. Nasjonale rammer for nettverks- og informasjonssikkerhet

Nasjonal strategi for digital sikkerhet av 2019 dekker langt på vei de krav som direktivet stiller til den nasjonale nettverks- og informasjonssikkerhetsstrategien. De oppgavene som direktivet tillegger den kompetente myndigheten er langt på vei sammenfallende med de oppgaver NSM utfører i dag som fag- og tilsynsmyndighet innenfor sikkerhetslovens

rammer. Flere sektormyndigheter har dessuten ansvar og myndighet innen sine sektorer. Samlet sett dekkes store deler av direktivet, men direktivet innebærer regulering av IKT-sikkerheten for en del virksomheter som per i dag ikke er direkte regulert. Mottak og behandling av varsler vil antakelig øke, i tillegg til at oppfølging og gjennomføring av direktivet er nye oppgaver som må delegeres til en eller flere myndigheter.

De oppgaver direktivet tillegger den nasjonale CERTen, slik disse fremgår av direktivets artikkel 9 og av vedlegg 1, sammenfaller i stor grad med de oppgaver som allerede ivaretas av Nasjonalt cybersikkerhetssenter. Norge har dermed allerede på plass de grunnleggende kapasitetene direktivet pålegger hver medlemsstat å opprette.

2. Samarbeid mellom medlemslandene og mellom CSIRTene

Det nærmere innholdet i og omfanget for begge former for samarbeid er ment å utvikles over tid, og vil uansett ikke være klart før samarbeidet faktisk setter i gang. Per i dag er det for Norges del allerede etablert et godt samarbeid innen eksempelvis hendelseshåndtering med flere nasjoner. Deltakelse i de to samarbeidsgruppene som direktivet etablerer vil komme i tillegg til eksisterende internasjonalt samarbeid.

3. Virksomheters nettverks- og informasjonssystemsikkerhet

Det går frem av kommentarene til direktivet at begrepet sikkerhet i nettverk og informasjonssystemer omfatter både lagret, sendt og behandlet data. Videre er evne til å identifisere risiko for, forebygge, oppdage, håndtere og gjenopprette etter hendelser angitt som aktuelle sikkerhetstiltak. Direktivet fastsetter ikke konkrete og spesifikke krav til sikkerhet utover dette. I stedet skal den enkelte virksomhet som faller inn under direktivets virkeområde gjennomføre en risiko- og sårbarhetsanalyse. Resultatet av analysen skal danne grunnlaget for å iverksette proporsjonale og hensiktsmessige konsekvensreduserende tiltak tilpasset den enkelte virksomhet. I hvilken grad direktivet får konsekvenser for norske virksomheter vil i stor grad avhenge av dagens sikkerhetsnivå i den enkelte virksomhet.

Det kan likevel legges til grunn at flere norske vedlegg II-virksomheter allerede har et sikkerhetsnivå som helt eller delvis tilfredsstiller direktivets krav. Virksomheter som er underlagt sikkerhetsloven vil antakelig overoppfylle direktivets krav. Personopplysningsloven stiller krav til informasjonssikkerheten for virksomheter som etter personopplysningsloven behandler eller er ansvarlig for behandlings av personopplysninger. Kravene oppfyller antakelig langt på vei direktivets krav.

Andre virksomheter er underlagt forskjellige grader av krav til sikkerhet. Høringsinstansenes svar viser at det eksisterer relevant sektorregelverk innen sektorene finans, helse, transport, energi, bank, vannforsyning og IKT-infrastruktur, se nærmere om dette under økonomiske og administrative konsekvenser.

Høringssvarene gir i mindre grad svar på i hvilken grad det eksisterer regelverk for tilbydere av digitale tjenester. Det er grunn til å tro at det per i dag ikke foreligger særlig relevant regelverk spesifikt for denne kategorien virksomheter, utover tverrsektorielt regelverk som for eksempel personopplysningsloven. Det legges til grunn i direktivet at disse virksomhetene i stor grad operer i flere land og at de konkrete sikkerhetskravene derfor må

harmoniseres i størst mulig grad i hele EU. ENISA og EU-kommisjonen skal bistå i dette arbeidet.

Rettslige konsekvenser

Justis- og beredskapsdepartementet sendte 21. desember 2018 på høring et utkast til lov som forbereder gjennomføring av direktivet i norsk rett. En eventuell implementering av direktivet i norsk rett vil forutsette at det etableres en lovhjemmel for de krav direktivet oppstiller. Idet direktivet pålegger private virksomheter plikter, må direktivet av hensyn til legalitetsprinsippet alene, gjennomføres ved lov.

Justis- og beredskapsdepartementet har funnet det hensiktsmessig å gjennomføre direktivet i en ny lov om digital sikkerhet.

Der det er påkrevet av hensyn til legalitetsprinsippet eller informasjonsformål vil departementet utforme lovregler. Dette gjelder først og fremst i tilfeller hvor det pålegges plikter mht. gjennomføring av sikkerhetstiltak, varsling av hendelser, tilsyn og sanksjoner.

Gjennomføring av direktivets øvrige krav, det vil si plikt til å ha en nasjonal strategi for IKT-sikkerhet, et nasjonalt responsmiljø for IKT-hendelser, utpeking av en nasjonal kompetent myndighet og deltakelse i NIS samarbeidsgruppe og NIS CSIRT-nettverk, krever ikke lovregulering og vil følges opp i egne prosesser.

Departementet tar sikte på å legge frem en Prop. LS hvor NIS-direktivet og Kommisjonens gjennomføringsforordning (EU) 2018/151 om regler for anvendelse av NIS-direktivet hva angår ytterligere spesifisering av de elementer som tilbydere av digitale tjenester skal ta hensyn til for å håndtere risikoene knyttet til sikkerheten til nettverks og informasjonssystemer, og av parametrene for å fastslå om virkningene av en hendelse er betydelige, gjennomføres i ny lov om digital sikkerhet og hvor det bes om Stortingets samtykke til godkjennelse av EØS-komiteens beslutning.

Grunnet behovet for lovendring og mulige økonomiske konsekvenser tas det forbehold om Stortingets samtykke til å innlemme rettsakten i EØS-avtalen, jf. EØS-avtalen art. 103.

EØS-komiteen forventes 3.februar 2023 å treffe beslutning om innlemmelse av NIS-direktivet og gjennomføringsforordning (EU) 2018/151 i EØS-avtalen. Beslutningen gjør tilføyelser til EØS-avtalens vedlegg XI og protokoll 37.

Økonomiske og administrative konsekvenser

Forskjellen mellom dagens regelverk og virksomhetenes sikkerhetsnivå på den ene siden og direktivets krav på den andre siden vil utgjøre direktivets samlede økonomiske og administrative konsekvenser.

Norge har i stor grad allerede gjennomført de tiltak som følger av direktivet.

Nasjonal strategi for digital sikkerhet av 2019 dekker de krav som direktivet stiller til den nasjonale nettverks- og informasjonssikkerhetsstrategien. De oppgavene som direktivet tillegger den kompetente myndigheten er langt på vei sammenfallende med de oppgaver Nasjonal sikkerhetsmyndighet (NSM) utfører i dag som fag- og tilsynsmyndighet innenfor sikkerhetslovens rammer. Flere sektormyndigheter har dessuten ansvar og myndighet innen sine sektorer. Samlet sett dekkes store deler av direktivet. Mottak og behandling av varsler vil antakelig øke, i tillegg til at oppfølging og gjennomføring av direktivet er nye oppgaver som må delegeres til en eller flere myndigheter.

De oppgaver direktivet tillegger den nasjonale CERTen, slik disse fremgår av direktivets artikkel 9 og av vedlegg I, sammenfaller i stor grad med de oppgaver som allerede ivaretas av Nasjonalt cybersikkerhetssenter. Norge har dermed allerede på plass de grunnleggende kapasitetene direktivet pålegger hver medlemsstat å opprette. Antakelig vil ikke direktivet medføre vesentlige konsekvenser på dette området. Det kan bli aktuelt med infrastrukturinvesteringer og å styrke evnen til redundans og varians i sikker kommunikasjon med eksterne aktører. Det må likevel påregnes noe økte administrative oppgaver og kostnader som medfølger å ivareta funksjonen som kompetent myndighet og nasjonalt kontaktpunkt.

Det må påregnes møter internasjonalt for å ivareta Norges rolle både i samarbeidsgruppen og i CSIRT-nettverket. Det er foreløpig ikke klart hvor mange møter det blir per år i samarbeidsgruppen. Det må legges til grunn at denne møtevirksomheten vil medføre kostnader utover dagens nivå.

Det vil også kunne innebære økte kostander for offentlige myndigheter til gjennomføring av tilsyn og håndtering av varsler. Kostnadsnivået vil avhenge av i hvilken grad det allerede føres tilsyn med IKT-sikkerhet og hvorvidt det er etablert et system for sending og mottak av varsler i de sektorene direktivet gjelder for. En gjennomgang av gjeldende rett gjort i forbindelse med høring av forslag til ny lov om digital sikkerhet viser at det i mange sektorer er etablert myndigheter som fører tilsyn med det gjeldende regelverket. I Norge vil gjennomføring av tilsyn mest effektivt gjennomføres av sektormyndighetene, og ved å tilpasse normal tilsynsvirksomhet til også å omfatte IKT-tilsyn. På denne måten vil eventuelle merkostnader kunne holdes på et lavt nivå.

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

For berørte virksomheter vil etterlevelse av kravene om sikkerhet og varsling kunne innebære økte kostnader. Dette vil i stor grad avhenge av dagens sikkerhetsnivå i den enkelte virksomhet. Det legges til grunn at mange virksomheter, gitt dagens digitale trusselbilde prioriterer arbeidet med digital sikkerhet, og allerede har implementert et adekvat sikkerhetsnivå. Siden direktivet trådte i kraft i EU i 2018 har fokus på digital sikkerhet og regulering av krav IKT-sikkerhet i sektorregelverkene. Dette gjelder også siden

lovutkastet var på høring. Også i EU har fokuset på regulering av digital sikkerhet, både tverrsektorielt, men også i enkeltsektorer, økt betydelig de siste 3 årene. Direktivet regulerer et minimum av det som må forventes av virksomheter og myndigheter hva gjelder digital sikkerhet i 2023.

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

Sakkyndige instansers merknader

Merknader fra Justis- og beredskapsdepartementet

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

Direktivets hovedformål er å forbedre det indre markeds funksjon. Direktivet har direkte innvirkning på berørte virksomheters rammevilkår og indirekte for alle andre virksomheter ved at sikkerheten i sentral infrastruktur blir bedret. Gjennomføring av direktivet i EU, men ikke i EFTA-landene, vil føre til ulike rammevilkår for virksomheter innad i EØS, og er følgelig ikke i tråd med EØS-avtalens intensjon.

Flere av de berørte samfunnssektorene er allerede regulert i EØS-avtalen, eksempelvis transport og energi. Videre er det i EØS-avtalen protokoll art. 31 inntatt beslutninger om EØS-samarbeid om både IKT-sikkerhet og infrastruktursikkerhet.

At det er etablert EØS-samarbeid innen områder som har nær sammenheng med det foreslåtte NIS-direktivet - eksempelvis eID og andre elektroniske tillitstjenester, personvern og ekomsektoren, tilsier at det også bør samarbeides om tiltak for å sikre et høyt felles nivå for nettverks- og informasjonssikkerheten.

Det er dessuten grunn til å tro at direktivets intensjon ivaretas bedre ved at det gjennomføres i hele EØS enn kun i EU. Ett av flere eksempler er at Norge vil kunne bidra positivt til og dra nytte av CSIRT-nettverket.

Sett hen til det som er beskrevet ovenfor om kost- og nyttevirkninger av direktivet mener Justis- og beredskapsdepartementet at direktivet er akseptabelt.

Konklusjon:

Forslaget er EØS-relevant og akseptabelt

Merknader fra høringsinstansene:

Departementet mottok rundt 40 høringssvar. Ingen av høringsinstansene mener at direktivet ikke er EØS-relevant eller at det ikke er akseptabelt. Rundt 13 av høringsinstansene uttaler seg positivt til direktivet og mener at det er EØS-relevant.

Merknader fra SU kommunikasjoner:

EØS-posisjonsnotatet ble behandlet og godkjent i SU kommunikasjoner 1. desember 2016. Utvalget hadde enkelte mindre merknader som er innarbeidet i notatet.

Vurdering

Justis- og beredskapsdepartementet har konkludert med at NIS-direktivet er EØS-relevant og akseptabelt.

Direktivet anses for å være et godt tiltak for å styrke IKT-sikkerheten i Norge.

Direktivets hovedformål er å forbedre det indre markeds funksjon. Direktivet setter krav til medlemsstatenes arbeid med IKT-sikkerhet, til virksomheter som er tilbydere av samfunnsviktige tjenester innenfor gitte sektorer, og til tilbydere av enkelte digitale tjenester. Det er særlig fokus på å sikre kontinuitet i leveransen av de aktuelle tjenestene. Et høyt felles IKT-sikkerhetsnivå skal gjøre unionen mer konkurransedyktig i en globalisert verden, skape tillit til digitale tjenester og bidra til økonomisk vekst i Europa. Dette direktivet og cybersikkerhetsforordningen inngår begge i EUs satsning innen cybersikkerhet. Et styrket samarbeidet i EUs regi vil være av stor betydning for å løse fremtidige utfordringer innen digital sikkerhet. Det er viktig at Norge sikres en plass i dette samarbeidet, da nåværende og fremtidige utfordringer ikke kan løses av en stat alene.

Gjennomføring av direktivet vil for mange samfunnsviktige virksomheter innebære en styrking av arbeidet med IKT-sikkerhet. Dette vil bidra til å redusere digitale sårbarheter i den enkelte virksomhet, den enkelte sektor og samlet sett for nasjonen. En risikobasert tilnærming til sikkerhetsarbeid er et viktig skritt på veien til bedre digital sikkerhet. Krav om varsling av alvorlige digitale sikkerhetshendelser vil blant annet gi tilgang til informasjon om både trusler og sårbarhet – en kunnskap som vil bidra til enda bedre arbeid med IKT-sikkerhet i fremtiden.

Av hensyn til konkurranse er det en fordel om det er like krav til sikkerhet i hele EØS. Ulike rammevilkår i ulike deler av EØS er uheldig særlig for virksomheter som har aktivitet både i EU og EØS/EFTA-landene, og er heller ikke i tråd med EØS-avtalens intensjon. Videre vil norske virksomheter kunne antas å være enklere mål for angripere dersom vi ikke har samme nivå på IKT-sikkerheten her som i EU. Et tettere samarbeid med EU-landene om IKT-sikkerhetsrelaterte spørsmål vil også være positivt for Norge. At det er etablert EØS-samarbeid innen områder som har nær sammenheng med det foreslåtte NIS-direktivet, eksempelvis eID og andre elektroniske tillitstjenester, personvern og ekomsektoren, tilsier at

det også bør samarbeides om tiltak for å sikre et høyt felles nivå for nettverks- og informasjonssikkerheten.

Tilpasningstekst:

Justis- og beredskapsdepartementet mener det er behov for tilpasningstekst slik at Norges sikres deltakelse i Samarbeidsgruppen og CSIRT-nettverket. Slik tilpasningstekst er del av EØS-komiteens beslutning.

EFTA-sekretariatet har identifisert to mulige horisontale utfordringer ved direktivet, jf. skjema 2a.

1. Bestemmelser med henvisning til rettsakter som ikke er innlemmet i EØS-avtalen

1.1 NIS-direktivet art. 1(3) fastsetter at direktivet ikke får anvendelse for virksomheter som er omfattet av direktiv 2002/21/EU (rammedirektivet) og forordning EU 910/2014 (EIDAS). Etter Justis- og beredskapsdepartementets vurdering har det ikke betydning for vurderingen av NIS-direktivet at nevnte rettsakter ikke er innlemmet i EØS-avtalen, ettersom det kun fastslås hvilke virksomheter som ikke er omfattet av direktivet.

1.2 NIS-direktivet art. 1(4) fastsetter at direktivet får anvendelse uten hensyntagen til blant annet direktiv 2013/40/EU om angrep mot informasjonssystemer mm. Etter Justis- og beredskapsdepartementets vurdering har det ikke betydning for vurderingen av NIS-direktivet at nevnte rettsakt ikke er innlemmet i EØS-avtalen, ettersom det kun henvises til rettsakter som NIS-direktivet ikke skal få konsekvenser for.

1.3 NIS-direktivet art. 4(1)(a) viser til rammedirektivet. Etter Justis- og beredskapsdepartementets vurdering har det ikke betydning for vurderingen av NIS-direktivet at nevnte rettsakt ikke er innlemmet i EØS-avtalen. Det er ikke noe i veien for å benytte definisjonen i rammedirektivet selv om dette ikke er innlemmet i EØS-avtalen.

1.4 NIS-direktivet art. 4(5) viser til en annen rettsakts definisjonsbestemmelse. Etter Justis- og beredskapsdepartementets vurdering har det ikke betydning for vurderingen av NIS-direktivet at nevnte rettsakt ikke er innlemmet i EØS-avtalen.

2. Samarbeidsgruppen, jf. NIS-direktivet art. 11. Justis- og beredskapsdepartementet er enig med EFTA-sekretariatet at det er viktig at EFTA-statene sikres full deltakelse i Samarbeidsgruppen. EØS-komiteens beslutning legger til et nytt punkt 5cpa som presiserer, i tråd med EØS-avtalen artikkel 101 om tilknytning til komiteer, at EFTA-statene skal delta fullt ut i samarbeidsgruppen og skal ha de samme rettighetene og forpliktelsene som EU-medlemslandene, bortsett fra retten til å stemme.

Inneholder informasjon unntatt offentlighet, jf. offl. § 14

32018R0151 Kommisjonens gjennomføringsforordning (EU) 2018/151 av 30. januar 2018 om fastsettelse av regler for anvendelse av europaparlaments- og rådsdirektiv (EU) 2016/1148 med hensyn til ytterligere spesifisering av de elementene som tilbydere av digitale tjenester skal ta hensyn til for å håndtere risikoene knyttet til sikkerheten i nettverks- og informasjonssystemer, og av parametrene for å avgjøre om en hendelse har en betydelig innvirkning

Status

Gjennomføringsforordning 2018/151 ble vedtatt 30. januar 2018 og trådte i kraft 10. mai 2018. Forordningen er under vurdering i EØS/EFTA-statene. Gjennomføringsforordningen er gitt med hjemmel i Europaparlamentets og Rådets direktiv (EU) 2016/1148 om tiltak som skal sikre et høyt felles sikkerhetsnivå i nettverks- og informasjonssystemer i EU (NIS-direktivet) artikkel 16 (8).

EØS-komiteen forventes 3.februar 2023 å treffe beslutning om innlemmelse av både NIS-direktivet og denne gjennomføringsforordningen.

Sammendrag av innhold

Gjennomføringsforordning 2018/151 ble vedtatt 30. januar 2018 og trådte i kraft 10. mai 2018. Forordningen er under vurdering i EFTA-statene. Gjennomføringsforordningen er gitt med hjemmel i Europaparlamentets og Rådets direktiv (EU) 2016/1148 om tiltak som skal sikre et høyt felles sikkerhetsnivå i nettverks- og informasjonssystemer i EU (NIS-direktivet) artikkel 16 (8). I denne bestemmelsen står det; *Kommisjonen skal vedta gjennomføringsrettsakter for å angi nærmere elementene som er nevnt i nr. 1 og parametere som er oppført i nr. 4 i denne artikkel. Disse gjennomføringsrettsaktene skal vedtas etter fremgangsmåten med undersøkelseskomité nevnt i artikkel 22 nr. 2 innen 9. august 2017.*

Fordi forordningen er gitt med hjemmel i NIS-direktivet og disse innlemmes sammen tas det forbehold om Stortingets samtykke til å innlemme rettsakten i EØS-avtalen, jf. EØS-avtalen art. 103. Bakgrunnen for dette er behov for lovendring.

NIS-direktivet forplikter virksomheter som har en særlig viktig rolle i opprettholdelsen av et funksjonelt indre marked til å gjennomføre IKT-sikkerhetstiltak og varsle om alvorlige hendelser. Virksomhetene faller i to kategorier. For det første; tilbydere av samfunnsviktige tjenester innenfor samfunnssektorene energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur. For det andre; tilbydere av digitale tjenester, nærmere bestemt nettbaserte markedsplasser, nettbaserte søkemotorer og skytjenester. Til forskjell fra tilbydere av samfunnsviktige tjenester kan medlemslandene, med visse unntak, ikke innføre strengere sikkerhetstiltak for tilbydere av digitale tjenester enn det direktivet legger opp til. Noe av begrunnelsen er at det for tilbydere av digitale tjenester er behov for unionsuniforme sikkerhetskrav. I direktivet stilles strengere krav til tilbydere av samfunnsviktige tjenester enn til tilbydere av digitale tjenester.

Medlemsstatene skal sørge for at tilbydere av digitale tjenester iverksetter sikkerhetstiltak som står i et rimelig forhold til risikoen virksomheten står overfor. Det skal også iverksettes tiltak for å forebygge og minimere virkningen av hendelser i nettverk og informasjonssystemer, med henblikk på opprettholdelse av tjenesteleveransen. Dette innebærer at det skal utarbeides strategi for sikkerhetsarbeidet, etablere en IKT-sikkerhetsberedskapsenhet (CSIRT) og pålegge operatører og leverandører av samfunnsviktige og digitale tjenester IKT-sikkerhetskrav og varslingsplikt ved alvorlige IKT-sikkerhetshendelser.

For kategorien "tilbydere av digitale tjenester" skal medlemsstatene ikke foreta en utpeking av virksomheter. Direktivbestemmelsene skal gjelde alle virksomheter som faller inn under NIS-direktivets vedlegg III:

1.Nettbaserte markedsplasser, jf. NIS-direktivet art. 4(17)

2.Nettbaserte søkemotorer, jf. NIS-direktivet art. 4(18)

3.Skytjenester, jf. NIS-direktivet art. 4(19)

Tilbydere skal også varsle en på forhånd bestemt kompetent myndighet om alvorlige hendelser. For tilbydere av digitale tjenester skal det tas hensyn til følgende parametere når det skal fastslås om virkningen av en hendelse er betydelig:

- antallet brukere som påvirkes av hendelsen, særlig brukere som er avhengig av tjenesten for å kunne yte egne tjenester

- hendelsens varighet

- størrelsen på det geografiske området som berøres av hendelsen

- omfanget av forstyrrelsen for tjenestens funksjon

- omfanget av virkningen for økonomiske og samfunnsmessige aktiviteter

Virksomhetene som omfattes av direktivet får i hovedsak to forpliktelser. De skal gjennomføre sikkerhetstiltak som står i et rimelig forhold til den risikoen virksomheten står overfor og de skal varsle om alvorlige IKT-sikkerhetshendelser.

I gjennomføringsforordning 2018/151 spesifiseres hvilke momenter tilbydere av digitale tjenester skal ta i betraktning når de fastsetter og iverksetter tiltak for å garantere et nivå av sikkerhet i nett- og informasjonssystemer som benyttes i leveransen av tjenester som nevnt i vedlegg III til NIS-direktivet. Videre spesifiseres hvilke kriterier som skal tas i betraktning ved fastsettelsen av hvorvidt en hendelse har betydelige konsekvenser for leveringen av disse tjenestene.

Forordningen presiserer hva som ligger i de elementer som følger av NIS-direktivets artikkel 16 nr. 1, som virksomheter skal vurdere for å håndtere risikoene knyttet til sikkerheten og iverksette passende sikkerhetstiltak for egenbeskyttelse.

Der NIS-direktivet omtaler *sikkerheten i systemer og utstyr* i artikkel16 nr. 1 bokstav a, presiserer forordningen at dette innebærer, systematisk forvalting av nettverks og

informasjonssystemer, fysisk og miljømessig sikkerhet, forsyningssikkerhet og adgangskontroll, jf. artikkel 2 nr. 1.

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

I NIS-direktivet artikkel 16 nr. 1 bokstav c omtales *håndtering av kontinuitet i virksomheten*. Etter forordningen artikkel 2 nr. 3 at dette vil innebære utarbeidelse av beredskapsplanverk og opprettholde en katastrofeberedskapskapasitet som vurderes og testes jevnlig.

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

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

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

Den andre hoveddelen av gjennomføringsforordningen omhandler parameterne i NIS-direktivets artikkel 16 (4) bokstav a-e som skal vektlegges ved avgjørelse om hvorvidt en hendelse er å anse som betydelig, og dermed meldepliktig etter direktivets artikkel 16.

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

Forordningen artikkel 3 nr. 2 presiserer hva som mener med en hendelses «varighet». Med varighet forstås tidsrommet hvor avbrytelse av tjenesteleveranse hva gjelder tilgjengelighet, autentisitet eller fortrolighet, til det tidspunkt hvor tjenesten er gjenopprettet.

Artikkel 3 nr. 3 presiserer at ved avgjørelse av hendelsens geografiske omfang, må tilbyderne være i stand til å fastslå om hendelsen påvirker leveransen av tjenester i bestemte EU-land.

Artikkel 3 nr. 4 presiserer at omfanget av driftsforstyrrelser i tjenesten skal måles basert på om en eller flere av følgende egenskaper svekkes som følge av en hendelse, dvs. dataenes

eller dermed tilknyttede tjenesters tilgjengelighet, autentisitet, integritet eller konfidensialitet.

Artikkel 3 nr. 5 presiserer hva gjelder omfanget av virkningen på økonomisk og samfunnsmessig virksomhet, at tilbydere skal kunne avgjøre om hendelsen har medført betydelige materielle eller ikke-materielle tap for brukerne, f.eks. med hensyn til helse, sikkerhet eller skade på eiendom.

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

Forordningens artikkel 4 fastsetter konkrete måleparametere for å fastslå om en hendelse har betydelige konsekvenser. Etter artikkel 4. nr. 1 bokstav a-d, har en hendelse betydelige konsekvenser dersom tjenesten ikke er tilgjengelig i over 5 000 000 brukertimer. 1 brukertime viser til antallet berørte brukere i EU i en periode på 60 minutter. En hendelse har betydelige konsekvenser hvis den har ført til tap av integritet, autentisitet eller konfidensialitet for arkiverte, overførte eller behandlede data eller tilknyttede tjenester og dette berører mer enn 100 000 brukere i EU. Videre vil en hendelse være å anse som betydelig dersom den har medført risiko for offentlig sikkerhet eller tap av menneskeliv, eller hendelsen har forårsaket materiell skade på over 1 000 000 Euro for minst en bruker i EU.

Artikkel 4 nr. 2 fastsetter at Kommisjonen kan revidere grenseverdier som fastsatt for øvrig i artikkel 4.

Artikkel 5 omhandler ikrafttredelse.

Merknader

Rettslige konsekvenser

Gjennomføringsforordningen kan ikke tre i kraft før NIS-direktivet er en del av EØS-avtalen. Norge forbereder innføring av NIS-direktivet i egen lov.

Forordningen pålegger private plikter og krever således gjennomføring i lov. Departementets vurdering er at den bør vedtas som forskrift til den loven som gjennomfører NIS-direktivet.

NIS-direktivet er planlagt gjennomført i en ny lov om digital sikkerhet.

Økonomiske og administrative konsekvenser

Rettsakten gjelder kun for tilbydere av digitale tjenester etter NIS-direktivet. Forordningen utdyper og presiserer innholdet i kravene som følger av NIS-direktivet. Det er forholdet mellom de krav som i dag stilles på den ene siden, og NIS-direktivets krav på den andre siden som vil utgjøre direktivets og gjennomføringsforordningens økonomiske og administrative konsekvenser. En total oversikt over konsekvensene vil medføre en konkret vurdering av sikkerhetsnivået i hver virksomhet som underlegges regelverket. Ut fra forordningens

presisering av overordnede krav innebærer dette i stor grad å utarbeide retningslinjer og planverk knyttet til de krav NIS-direktivet oppstiller. Forordningens presiseringer medfører således ikke økonomiske eller administrative konsekvenser som ikke allerede er forutsatt at vil påløpe som følge av innføringen av NIS-direktivet i norsk rett.

Sakkyndige instansers merknader

EØS-posisjonsnotat ble lagt frem i SU Kommunikasjoner 13. september 2019 og i etterkant skriftlig klarert.

Vurdering

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

Gjennomføringsforordningen er en viktig presisering av overordnede krav for tilbydere av digitale tjenester. Presiseringene knyttet til elementer som skal vektlegges av virksomhetene når de skal etablere et sikkerhetsnivå som står i forhold til risikoen er funksjonelt utformet. Dette er i tråd med NIS-direktivets kravstilling, og i tråd med hvordan departementet vil gjennomføre NIS-direktivet, med tilhørende gjennomføringsforordninger, i norsk rett.

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

Forordningen anses som et positivt tilskudd til NIS-direktivet.

Konklusjon: Gjennomføringsforordningen er EØS relevant og det er ikke nødvendig med tilpasningstekst.

32019R0881 Europaparlaments- og rådsforordning (EU) 2019/881 av 17. april 2019 om ENISA (Den europeiske unions cybersikkerhetsbyrå), om cybersikkerhetssertifisering av informasjons- og kommunikasjonsteknologi og om oppheving av forordning (EU) nr. 526/2013 (cybersikkerhetsforordningen)

Status

Rådet vedtok sin posisjon på meldingen om EUs reviderte cybersikkerhetsstrategi – Resilience, Deterrence and Defence: Building strong cybersecurity in Europe – på møtet i Rådet for allmenne saker 20. november 2017. Konklusjonene fra møtet støtter opp om et permanent mandat for ENISA i form av at det opprettes et EU Cybersecurity Agency. De maner videre til at Europa utvikler en verdensledende sertifiseringsordning for å øke sikkerheten og tilliten til digitale produkter og tjenester.

Rettsakten er vedtatt og trådt i kraft i EU 27. juni 2019.

Rettsakten er under vurdering i EØS-/EFTA-landene. Standardskjema ble returnert til EFTA-sekretariatet 20.12.2019.

EØS-komiteen forventes 3.februar 2023 å treffe beslutning om innlemmelse av cybersikkerhetsforordningen i EØS-avtalen. Beslutningen gjør tilføyelser til EØS-avtalens vedlegg XI og protokoll 37.

Sammendrag av innhold

Forordningen gjennomføres som en konsekvens av global digitalisering og økt risiko for cybersikkerhetshendelser. Forordningen innebærer at ENISA får et styrket budsjett, flere ansatte og et styrket og permanent mandat og vil dermed spille en større rolle i EUs cybersikkerhetslandskap. ENISA vil med et permanent mandat ivareta rollen som Den Europeiske Unions Byrå for Cybersikkerhet (the European Union Agency for Cyber Security). ENISA skal etter anmodning kunne bistå medlemslandene med grenseoverskridende hendelseshåndtering, herunder blant annet rådgivning, analyse og tekniske undersøkelser. ENISA skal også særlig bistå og legge til rette for medlemslandenes kapasitetsutbygging, operasjonelt samarbeid og forskning og utvikling.

Forordningen etablerer også et felleseuropeisk rammeverk for frivillig sertifisering av IKT-produkter, tjenester og prosesser (Definert i artikkel 2 nr. 12,13 og 14). ENISA får også viktige oppgaver i forbindelse med å utvikle og administrere dette rammeverket. Forordningen setter i denne sammenheng også et krav om at medlemslandene skal etablere tilsynsmyndigheter og andre roller for sikkerhetssertifisering.

Grunnet behovet for lovendring og budsjettmessige konsekvenser tas det forbehold om Stortingets samtykke til å innlemme rettsakten i EØS-avtalen, jf. EØS-avtalen art. 103.

Bakgrunn og formål

I forbindelse med EU-kommisjonens president Jean-Claude Junckers State of the Union-tale 13. september 2017 presenterte EU-kommisjonen, i samarbeid med EUs representant for utenrikssaker og sikkerhetspolitikk, en felles kommunikasjon om EUs arbeid med digital

sikkerhet. Her ble kommisjonens «Cyber Security package» lansert med konkrete tiltak for å møte trusselbildet.

EU-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 er også vist til at de økonomiske konsekvensene av IKT-kriminalitet ble femdoblet fra 2013 til 2017, og at de kan ytterligere firedobles innen 2019. Undersøkelser synes å vise at befolkningen flere steder i verden anser at IKT-angrep fra andre stater er blant de største truslene mot nasjonal sikkerhet.

Formålet med denne forordningen er å sikre et velfungerende indre marked med et høyt nivå av cybersikkerhet, motstandsdyktighet og tillit i EU. Dette skal oppnås ved å fastsette mål, oppgaver og organisatoriske forhold for EUs Cybersikkerhetsbyrå (ENISA), samt etablere et felleseuropeisk rammeverk for sikkerhetssertifisering av IKT-produkter, tjenester og prosesser. (jf. artikkel 1).

Forordningen inngår som et element i EUs digitaliseringsstrategi, som har som formål å stimulere til økonomisk vekst og øke EUs konkurransekraft. Forordningen gir ENISA en sterkere og mer sentral rolle ved at de skal understøtte medlemslandenes gjennomføring av direktiv (EU) 2016/1148 (NIS-direktivet), og ved å motvirke trusler på en mer aktiv måte.

I dette EØS-posisjonsnotatet benyttes begrepene "IKT-sikkerhet", «digital sikkerhet» og "cybersikkerhet" synonymt.

Forordningens innhold

AVSNITT 1 – GENERELLE BESTEMMELSER

Generelle bestemmelser og definisjoner følger av artikkel 1 og 2.

Av artikkel 1 fremgår forordningens formål. Formålet er å sikre et velfungerende indre marked og å oppnå et høyt nivå av cybersikkerhet, motstandsdyktighet og tillitt innad i EU. Dette skal oppnås ved å:

1. fastsette mål, oppgaver og organisatoriske forhold for ENISA,
2. etablere et rammeverk for opprettelse av europeiske cybersikkerhetssertifiseringsordninger, som igjen har to formål:
    a. å sikre et tilstrekkelig sikkerhetsnivå for IKT-produkter, -tjenester og –prosesser i EU
    b. å unngå fragmentering av det indre marked med hensyn til cybersikkerhetsertifiseringsordninger i EU.

Cybersikkerhetssertifiseringsrammeverket kommer til anvendelse uten at det berører andre spesifikke EU-rettsakter som omhandler frivillig eller obligatorisk sertifisering.

Forordningen berører ikke medlemsstatenes kompetanse med hensyn til aktiviteter vedrørende offentlig sikkerhet, forsvar, statssikkerhet og innenfor det strafferettslige området.

Av artikkel 2 fremgår en rekke definisjoner hvor flere viser til begrep som er definert i NIS-direktivet. Det vises også til definisjoner som benyttes i forordning om akkrediterings- og markedstilsynskrav i forbindelse med markedsføring av produkter (EF) 765/2008.

AVSNITT 2 – ENISA (Den Europeiske Unions Byrå for Cybersikkerhet)

Kapittel I – Mandat og formål

ENISA (European Network and Information Security Agency) ble opprettet i 2004 og har siden opprettelsen hatt et midlertidig mandat for sitt arbeid. Utfordringen med et tidsavgrenset mandat er at det gir begrensede muligheter for langsiktig planlegging og bæredyktig støtte til EUs medlemsland. Et midlertidig mandat er ikke i tråd med NIS-direktivet som gir ENISA oppgaver av permanent karakter. Et midlertidig mandat underbygger heller ikke EUs visjon for IKT-sikkerhetsområdet.

I 2017 ble det gjennomført en evaluering av ENISA på måloppnåelse og oppgaveløsning. Resultatet var positivt og konkluderte med at byrået i all hovedsak har nådd sine mål og løst sine oppgaver tilfredsstillende. Evalueringen pekte på enkelte utfordringer, bl.a. at ENISA har et bredt mandat, men at det er begrensede finansielle og menneskelige ressurser. Kommisjonen har vedtatt å gi ENISA et permanent og styrket mandat, jf. art. 3.

ENISA skal utføre oppgavene de pålegges gjennom denne forordningen, det vil si primært støtte medlemslandene, EU-institusjonene, organene, kontorene og byråene til å forbedre cybersikkerheten, og gjennom dette oppnå sitt hovedformål, å oppnå et felles høyt cybersikkerhetsnivå i EU. ENISAs oppgaver følger også av andre rettsakter som vedrører cybersikkerhet, blant annet NIS-direktivet.

ENISAs oppgaver skal utføres for å sørge for en ensartet gjennomføring av relevante rettslige rammer, med særskilt henvisning til en effektiv gjennomføring av NIS-direktivet. ENISA skal handle uavhengig når de utfører sine pålagte oppgaver, og ta hensyn til medlemsstatenes ekspertise og unngå overlapping av medlemsstatenes aktiviteter.

Målene for ENISAs arbeid (jf. art. 4):

Byrået skal

- være et ekspertisesenter og bistå i EU-kommisjonens arbeid med digital sikkerhet.

- bistå EU og EUs institusjoner og medlemsland med å utvikle og gjennomføre EU-strategier for digital sikkerhet, herunder også sektorspesifikke strategier.

- støtte kapasitetsbygging og beredskap ved å bistå EU, EUs institusjoner, medlemslandene og offentlige og private interessenter, for å øke egenbeskyttelsen av nettverks- og informasjonssystemer, forbedre cyberresiliens og responskapasiteter og utvikle ferdigheter og kompetanse innenfor digital sikkerhet.

- fremme samarbeid, informasjonsutveksling og koordinering mellom medlemsland, Unionen, Unionens institusjoner og relevante interessenter, herunder privat sektor, om saker knyttet til cybersikkerhet.

- bidra til å øke cybersikkerhetskapabiliteter på EU-nivå for å støtte medlemslandenes tiltak for å forebygge og håndtere cybertrusler, særlig i grenseoverskridende cyberhendelser.

- fremme bruken av Europeisk cybersikkerhetssertifisering, bl.a. ved å bidra til etablering og vedlikehold av et felleseuropeisk rammeverk for sikkerhetssertifisering, for å øke transparens og verifisering av IT-produkter, tjenester og prosesser med formål om å styrke tilliten til og unngå fragmentering av det digitale indre marked.

- bidra til økt kunnskap og kompetanse om cybersikkerhet, herunder cyberhygiene og cyberferdigheter, for både privatpersoner og virksomheter.

Kapittel II Oppgaver:

1) Policyutvikling og lovregulering (jf. art. 5)

ENISA får i oppgave å bidra proaktivt i policyutvikling og lovgivning for cybersikkerhetsfeltet, samt til andre politiske initiativ med cybersikkerhetselementer innenfor ulike sektorer (f.eks. energi, transport og finans). ENISA får i denne sammenheng en styrket rådgivende rolle, da i form av uavhengige vurderinger, analyser og forarbeider til policy- og lovutvikling. ENISA skal også støtte medlemslandene med implementeringen av NIS-direktivet, hvis formål er å etablere et høyt felles sikkerhetsnivå for nett- og informasjonssikkerhet innenfor en rekke samfunnsviktige sektorer (energi, transport, finans, helse, vannforsyning, IKT-infrastruktur osv.). Dette innebærer blant annet å bistå medlemslandene med å oppnå en ensartet gjennomføring av direktivet på tvers av grenser og sektorer ved å utstede uttalelser, retningslinjer, beste praksis mv. Tilsvarende skal ENISA støtte arbeidet i NIS-samarbeidsgruppen (NIS-direktivet artikkel 11), som har som oppgave å støtte medlemslandene i implementeringen av NIS-direktivet samt understøtte strategisk samarbeid og erfaringsutveksling mellom medlemslandene.

ENISA skal understøtte utvikling og gjennomføring av policyer innen elektronisk kommunikasjon og tillitstjenester og fremme et høyere sikkerhetsnivå i elektronisk kommunikasjon gjennom rådgivning og ved å utgi tekniske retningslinjer, samt fremme utveksling av beste praksis mellom kompetente myndigheter.

ENISA skal også understøtte en jevnlig gjennomgang av EUs aktiviteter og avgi årlige rapporter, basert på innrapporteringer, på status og etterlevelse av EU-policy og -regulering, jf. art. 10(3) i NIS-direktivet, art. 19(3) i forordning om eID og elektroniske tilleggstjenester og art. 40 i ekomkodeksen

2) Kapasitetsbygging (jf. art. 6)

ENISA får i oppgave å bidra til å øke EUs og de nasjonale offentlige myndigheters kapasitet og ekspertise til å forebygge, detektere og analysere hendelser blant annet gjennom å bistå med utvikling av nasjonale strategier for cybersikkerhetsområdet, tilby kurs, fremme samarbeid og informasjonsutveksling, og støtte CERT-EU (EUs Computer Emergency Response Team) i deres arbeid, og bidra i etableringen av ulike lands nasjonale CSIRT'er (Computer Security Incident Response Team). I denne forbindelse vil ENISA tilrettelegge for cybersikkerhetsøvelser på EU-nivå minimum annethvert år.

ENISA skal særlig støtte informasjonsutveksling i og mellom sektorer oppført i NIS-direktivets vedlegg II ved å stille til rådighet beste praksis og prosedyrer.

Byrået skal også bidra i etableringen av sentrene for informasjonsutveksling og analyse (ISAC'er) innen ulike sektorer ved å stille til rådighet beste praksis og veiledning i tilgjengelige verktøy og prosedyrer.

3) Operasjonelt samarbeid på EU nivå(jf. art. 7)

Etter forordningen får ENISA myndighet til å støtte det operasjonelle samarbeidet på tvers av Unionen og på tvers av medlemslandene, herunder i CSIRT-nettverket (bestående av medlemslandenes CSIRT'er (iht. NIS-direktivet)). I den forbindelse inngår ENISA i et strukturert samarbeid med CERT-EU for å utnytte synergier og unngå overlapp av aktiviteter. ENISA skal også ivareta sekretariatsfunksjon for CSIRT-nettverket.

ENISA skal støtte medlemslandene i det operasjonelle samarbeidet innen CSIRT-nettverket med generell rådgivning om forebygging, deteksjon og håndtering, eventuelt etter anmodning også knyttet til spesifikke hendelser. På anmodning fra et eller flere berørte medlemsland, og med formål om å skulle levere rådgivning om forebygging av fremtidige hendelser, vil ENISA kunne gi støtte til eller utføre en påfølgende teknisk undersøkelse av hendelser med betydelig eller vesentlig virkning i henhold til NIS-direktivet.

ENISA skal legge til rette for regelmessige cybersikkerhetsøvelser annet hvert år.

ENISA vil også få i oppgave å regelmessig utarbeide en teknisk EU-cybersikkerhetsrapport, i nært samarbeid med medlemslandene om hendelser og trusler. Dette skal være basert på offentlig tilgjengelig informasjon, ENISAs egne analyser og rapporter, som på frivillig basis deles av bl.a. medlemslandenes CSIRTer eller NIS-direktivets sentrale kontaktpunkter, jf. art. 14(5) i NIS-direktivet, Det Europeiske senter for bekjempelse av cyberkriminalitet (EC3) hos Europol eller CERT-EU.

Ved større såkalte "grenseoverskridende cybersikkerhetshendelser eller -kriser", og med formål om å fremme operasjonelt samarbeid, får ENISA myndighet til å: a) sammenstille rapporter fra nasjonale kilder for å skape felles situasjonsforståelse, b) sikre effektiv informasjonsflyt og sørge for at det er eskaleringsmekanismer på plass mellom CSIRT-nettverket og de tekniske og politiske beslutningstagere på EU-nivå, c) etter anmodning støtte teknisk håndtering av en hendelse, inkludert frivillig deling av tekniske løsninger mellom medlemslandene, d) støtte kommunikasjon til offentligheten/publikum om en hendelse, og e) teste samarbeidsplaner for håndtering av slike hendelser.

4) Oppgaver relatert til markedet, cybersikkerhetssertifisering, og standardisering (jf. art. 8)

ENISA får i oppgave å understøtte det indre marked, ved å analysere utviklingstendenser innenfor cybersikkerhetsmarkedet, og ved å understøtte EUs policyutvikling for IKT-standardisering og IKT-sikkerhetssertifisering. Detaljer om sertifiseringsordningen følger lenger ned i teksten.

5) Oppgaver relatert til kunnskap og kompetansebygging (jf. art. 9)

ENISA skal være EUs informasjonsknutepunkt vedr. nett- og informasjonssikkerhet. Det innebærer å fremme og utveksle beste praksis og initiativer på tvers av EU. Byrået skal stille til rådighet rådgivning, veiledning og beste praksis vedrørende sikkerheten i kritiske infrastrukturer. ENISA skal i samarbeid med nasjonale myndigheter og relevante interessenter gi råd og veiledning knyttet til sikkerhet i nett- og informasjonssystemer særlig knyttet til sikkerhet i de infrastrukturer som understøtter sektorer under NIS-direktivet, og tilbydere av digitale tjenester som omfattes av nevnte direktiv. Etter en vesentlig grenseoverskridende hendelse skal ENISA dessuten få i oppgave å utarbeide rapporter for å gi veiledning til virksomheter og borgere i hele EU på bakgrunn av den aktuelle hendelsen.

6) Oppgaver relatert til bevisstgjøring og utdannelse (jf. art. 10)

ENISA skal bevisstgjøre offentligheten om risiko forbundet med cybersikkerhet og drive målrettet veiledning mot brukere, organisasjoner og virksomheter om blant annet cyberhygiene og cyberferdigheter. Byrået skal i samarbeid med medlemslandene etterstrebe økt bevissthet og fremme utdannelse, gjennom opplysningskampanjer og tilretteleggelse for offentlig debatt.

7) Oppgaver relatert til forskning og innovasjon (jf. art. 11)

ENISA skal med sin ekspertise rådgi EU og nasjonale myndigheter i forskningsbehov og prioriteringer for cybersikkerhetsområdet. ENISA vil også der Kommisjonen har gitt nødvendig bemyndigelse, delta i gjennomførelsen av EUs finansieringsprogram for forskning og innovasjon på cybersikkerhetsområdet. ENISA skal bidra til den strategiske forsknings- og innovasjonsdagsordenen i EU innen cybersikkerhet.

8) Oppgaver relatert til internasjonalt samarbeid (jf. art. 12)

ENISA skal bidra til EUs innsats for å fremme internasjonalt samarbeid på cybersikkerhetsfeltet ved å delta som observatør og i tilretteleggelsen av internasjonale øvelser. ENISA skal, på anmodning fra Kommisjonen, fremme utveksling av beste praksis mellom relevante internasjonale organisasjoner - samt stille ekspertise til rådighet for Kommisjonen, og rådgi og støtte Kommisjonen i spørsmål knyttet til avtaler om gjensidig anerkjennelse av cybersikkerhetsattester med tredjeland i samarbeid med ECCG jf. art 62.

Kapittel III - Organisasjon:

Artikkel 13 til 23 omhandler organiseringen av byrået og beskriver ansvar, myndighet og organiseringen av arbeidet som tilligger "Management Board", "Executive Board" og "Executive Director". Dette er i stor grad samsvarende med den organiseringen som følger av denne forordnings forløper (EU) 526/2013.

En ENISA-rådgivningsgruppe og et nettverk av nasjonale forbindelsesoffiserer (National Liaison Officers Network) opprettes som en del av ENISAs struktur etter denne forordningen jf. artikkel 13 bokstav d og e, jf., artikkel 21.

ENISAs rådgivingsgruppe blir bredt sammensatt etter forslag fra administrerende direktør, og skal rådgi ENISA med hensyn til hvordan ENISA skal utføre sine oppgaver, med unntak av denne forordnings kapittel III.

Det opprettes også en «Cybersikkerhetssertifiseringsgruppe for Interessenter» med medlemmer valgt av Kommisjonen etter forslag fra ENISA, jf. artikkel 22. Gruppen skal blant annet rådgi Kommisjonen om strategiske spørsmål knyttet til det europeiske rammeverket for cybersikkerhetssertifisering, rådgi og bistå ENISA om utførelse av ENISAs oppgaver.

Artikkel 24 til 28 omhandler bestemmelser knyttet til ENISAs drift og forvaltning.

Kapittel IV - Budsjett

Artikkel 29 til 33 tar for seg budsjett, regler for finansiering og hvordan man skal motarbeide bedrageri.

Kapittel V - Personale

Artikkel 34 til 37 omhandler ENISAs ansatte.

Kapittel VI - Generelle bestemmelser om ENISA

Artikkel 38 til 45 tar for seg generelle bestemmelser relatert til ENISAs juridiske status og ansvar, språkordninger, beskyttelse av personopplysninger, samarbeid med tredjeland og internasjonale organisasjoner og sikkerhetsregler for behandling av gradert og sensitiv ugradert informasjon osv.

AVSNITT 3 RAMMEBETINGELSER FOR CYBERSIKKERHETSSERTIFISERING

Forordningen inneholder et nytt regelverk for sikkerhetssertifisering av IKT-produkter, tjenester og prosesser jf. artikkel 46 flg.

Noe av bakgrunnen for dette er at trusselbildet og økningen av IKT-kriminalitet har fremtvunget ulike nasjonale sertifiseringsregelverk. Konsekvensen er bl.a. fragmenterte og lite hensiktsmessige ordninger som ikke samspiller effektivt inn mot EUs indre marked (interoperabilitetsutfordringer).

Målet med et felleseuropeisk regelverk er å fremme IKT-sikkerhet som et konkurransefortrinn og bidra til forbrukernes tillit til IKT-produktene, samtidig som IKT sikkerhetsnivået blir hevet. Et felles regelverk vil også kunne redusere sertifiseringskostnader. Initiativet supplerer og støtter også gjennomførelsen av NIS-direktivet ved å gi de virksomheter som er omfattet av direktivet et verktøy for å påvise etterlevelse av direktivet for hele EU. Forordningen innfører ikke direkte operasjonelle sertifiseringsordninger, men etablerer et rammeverk av regler for innførelse av spesifikke europeiske sertifiseringsordninger for IKT-produkter, tjenester og prosesser, som blir utarbeidet etter forslag fra ENISA og vedtatt ved "gjennomførelsesrettsakter" fra Kommisjonen (beskrevet lenger ned).

En cybersikkerhetssertifiseringsordning vil i henhold til forordningen attestere at IKT-produktene, tjenestene og prosessene som er sertifisert i overensstemmelse med ordningen og oppfyller fastsatte sikkerhetskrav. For eksempel hva gjelder beskyttelsesevne mot kompromittering, tilgjengelighet, autentisering, integritet og konfidensialitet av de data som oppbevares eller behandles i produktet, tjenesten eller prosessen. De europeiske sertifiseringsordningene vil ikke selv utvikle tekniske standarder, men benytte eksisterende

standarder om tekniske krav og evalueringsprosedyrer som produktene skal overholde. Sertifiseringsordningene skal utformes slik at de, basert på relevans for den aktuelle prosess, produkt- eller tjenestegruppen, tar hensyn til flere sikkerhetsmål, (jf. art. 51), herunder:

- Beskytte data mot utilsiktet eller uautorisert lagring, behandling eller offentliggjøring, og beskytte data mot utilsiktet eller uautorisert ødeleggelse, tap eller endring, i hele IKT-produktet, tjenesten eller prosessens levetid.

- Sikre at kun autoriserte personer, programmer eller maskiner har adgang til dataene, herunder bl.a. gjennom tilstrekkelig logging av type data og hvilke handlinger som er utført.

- Verifisere at IKT-produkter, tjenester eller prosesser ikke inneholder kjente sårbarheter, og at disse er sikre som følge av standardinnstillinger og innebygget sikkerhet.

- Sikre tilgjengelighet og tilgang til data (restore) ved tilfeller av fysiske eller tekniske hendelser.

- Sikre at IKT-produkter og -tjenester innehar ajourført software og hardware fri for kjente sårbarheter, samt er gitt mekanismer for sikker oppdatering.

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

Tilbydere av sertifiserte IKT-produkter, tjenester eller prosesser skal også offentliggjøre enkelte supplerende opplysninger, herunder veiledninger, anbefalinger for å bistå sluttbrukere med sikker konfigurasjon drift og vedlikehold mv. Det skal angis hvor lenge det tilbys sikkerhetsstøtte og det skal gjøres mulig for sluttbruker å orientere seg om sårbarheter samt å kunne melde om sårbarheter de selv oppdager.

Det skal være frivillig å benytte seg av sertifiseringsregelverket. Kommisjonen vil imidlertid regelmessig vurdere effekten og anvendelsen av de vedtatte sertifiseringsordningene, og hvorvidt en ordning skal gjøres obligatorisk gjennom EU-retten. Den første vurderingen av en sertifiseringsordning skal gjøres senest innen utløpet av 2023. På bakgrunn av evalueringen og etter en nærmere prosess identifiseres hvilke IKT-produkter, tjenester og prosesser som bør omfattes av eventuelle obligatoriske ordninger, herunder vil Kommisjonen prioritere de sektorer som omfattes av NIS-direktivets vedlegg II jf. art 56.

Om forberedelse og vedtakelse av sertifiseringsordninger:

Kommisjonen skal offentliggjøre et «rullende arbeidsprogram» for europeisk cybersikkerhetssertifisering som peker ut strategiske prioriteringer for fremtidige cybersikkerhetssertifiseringsordninger. Arbeidsprogrammet skal omfatte en oversikt over

produkter, tjenester og prosesser som bør omfattes av en ordning, basert på bl.a. hvilke ordninger som eksisterer, etterspørsel i markedet, utvikling i cybertrussebildet mv.

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

Kommisjonen vedtar sertifiseringsordningene ved hjelp av gjennomføringsrettsakter, jf. art. 49 og etter en bred prosess. De ulike ordningene skal publiseres på en webside drevet av ENISA, jf. art. 50.

Om cybersikkerhetssertifisering:

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

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

Nasjonale tilsynsmyndigheter skal for hver europeisk sertifiseringsordning orientere Kommisjonen om akkrediterte etterlevelsesorganer. Kommisjonen vil på bakgrunn av dette, og innen et år etter ikrafttredelsen, offentliggjøre en liste over innmeldte etterlevelsesorganer. Cybersikkerhetsattestene utstedes for den perioden som er fastsatt for den enkelte sertifiseringsordning, og vil kunne forlenges såfremt kravene fortsatt er oppfylt. En europeisk cybersikkerhetsattest skal anerkjennes i alle medlemsland, jf. art. 56 (10).

Om nasjonale ordninger og myndigheter:

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

Medlemslandene må heller ikke vedta nye nasjonale sertifiseringsordninger for IKT-produkter, tjenester og prosesser som allerede er omfattet av en europeisk ordning.

Med hensyn på å unngå fragmentering av det indre marked, skal medlemslandene meddele initiativ til å opprette nye nasjonale ordninger til Kommisjonen og ECCG.

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

Den nasjonale myndigheten skal være uavhengig av de enheter den fører tilsyn med, og medlemslandene skal sikre at nasjonale sertifiseringsmyndigheters aktiviteter vedrørende utstedelse av sertifiseringsattester etter art. 56 (5a) og (6) er strengt adskilt fra sine tilsynsaktiviteter etter art. 58.

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

Forordningen etablerer også en ordning med en «fagfellevurdering» jf. art 59. Dette for å sikre en ensartet standard for cybersikkerhetsattester og overenstemmelseserklæringer innad i EU. Vurderingene skal gjennomføres av minst to nasjonale sertifiseringsmyndigheter fra andre stater og av Kommisjonen. Dette skal gjennomføres minst hvert femte år. Vurderingen skal innebære undersøkelser av sertifiseringsmyndighetens aktiviteter knyttet til utstedelser av attester og at dette er adskilt fra tilsynsvirksomhet, at prosedyrer for tilsyn med og håndhevelse av oppfølging av attester og etterlevelsesorganenes aktiviteter overholdes og hvis relevant om myndighetene har den tilstrekkelige ekspertise til å utstede attester for tillitsnivået «høyt».

Forordningen legger opp til at det etableres en europeisk cybersikkerhetssertifiseringsgruppe (ECCG), jf. art. 62, bestående av alle medlemslands nasjonale sertifiseringstilsynsmyndigheter. Gruppen skal både gi råd til Kommisjonen i cybersikkerhetssertifiseringspolitikk, samt samarbeide med ENISA om å utarbeide forslag til europeiske cybersikkerhetssertifiseringsordninger, følge utviklingen, fremme samarbeid og støtte gjennomføringen av ordningen med fagfellevurdering jf. art. 59. Gruppen kan også foreslå for Kommisjonen konkrete ordninger som ENISA bør få i oppdrag å utarbeide. Kommisjonen innehar formannskapet og sekretariatsfunksjonen for gruppen med bistand fra ENISA, jf. art. 62(5). Medlemslandene skal etter forordningen fastsette regler for sanksjoner for brudd på forordningens bestemmelser og de europeiske sertifiseringsordninger. Sanksjonene skal være effektive, stå i rimelig forhold til bruddet og ha avskrekkende effekt, jf. art. 65.

AVSNITT IV AVSLUTTENDE BESTEMMELSER

Effekten av ENISAs nye rolle og virkningen av sertifiseringsordningen skal evalueres hvert femte år.

Europaparlaments- og rådsforordning (EU) nr. 526/2013 av 21. mai 2013 om Det europeiske byrå for nett- og informasjonssikkerhet (ENISA) og om oppheving av forordning (EF) nr. 460/2004 oppheves.

Artikkel 58 om nasjonale cybersikkerhetssertifiseringsmyndigheter, artikkel 60 om etterlevelsesorganer, artikkel 61 om rapportering av akkreditering, artikkel 63 om klage, artikkel 64 om rett til effektive rettsmidler og artikkel 65 om sanksjoner trer ikke kraft før 28. juni 2021.

Vurdering

Forordningen vurderes som positiv sett opp mot de utfordringene man ser innenfor cybersikkerhetsfeltet. ENISA ble opprettet i 2004 og har siden opprettelsen hatt et midlertidig mandat for sitt arbeid. Utfordringen med et tidsavgrenset mandat er at det gir begrensede muligheter for langsiktig planlegging og bæredyktig støtte til medlemsstatene. En styrking av ENISA vil tilrettelegge for langsiktig planlegging samt understøtte NIS-direktivet som gir ENISA oppgaver av permanent karakter. Alle medlemsstatene i EU har likevel et selvstendig ansvar for å sørge for egen cybersikkerhet. En utvidelse av ENISAs mandat skal ikke være til erstatning for dette ansvaret. Det er likevel klart at ENISA får en fremtredende rolle innen EUs cybersikkerhetssatsning. En felles satsning innen EU gjør statene i stand til å dele situasjonsforståelse og respondere på alvorlige sikkerhetshendelser mer effektivt. Denne forordning og NIS-direktivet inngår begge i EUs satsning innen cybersikkerhet. Et styrket samarbeidet i EUs regi vil være av stor betydning for å løse fremtidige utfordringer innen digital sikkerhet. Det er viktig at Norge sikres en plass i dette samarbeidet, da nåværende og fremtidige utfordringer ikke kan løses av en stat alene.

Omforent sertifisering for både EU og EØS anses i utgangspunktet for å være et positivt tiltak. Målet med et felleseuropeisk regelverk er å fremme cybersikkerhet som et konkurransefortrinn og bidra til forbrukernes tillit til IKT-produktene, samtidig som sikkerhetsnivået blir hevet. Et felles regelverk vil også kunne redusere sertifiseringskostnader. Initiativet supplerer og støtter også gjennomførelsen av NIS-direktivet ved å gi de virksomheter som er omfattet av direktivet et verktøy for å påvise etterlevelse av direktivet for hele EU.

Sertifisering vil etter forordningen inntil videre være frivillig. Innen en viss tid skal Kommisjonen ha gjort en første vurdering av hvorvidt enkelte sertifiseringsordninger skal gjøres obligatoriske. Det vil i første omgang være snakk om sektorer som er omfattet av NIS-direktivet. Flere norske virksomheter vil dermed kunne bli bundet av krav til sertifisering av IKT-produkter, tjenester eller prosesser. Ettersom leverandører av slike tjenester ofte er globale og/eller europeiske, er felles-europeiske løsninger riktig. Sertifisering av produkter og tjenester vil ikke motvirke norske interesser. Et sertifiseringsrammeverk bør i størst mulig grad være beskrivende med tanke på kvalitets- og sikkerhetsnivået som oppnås, og det bør legges til rette for at det vil være attraktivt å benytte i markedsføringssammenheng. Da vil det være mindre behov for regulering, og effekten vil komme på grunn av etterspørsel. En felles overbygning i et rammeverk vil bidra til at man unngår at produkter, tjenester og prosesser må sertifiseres flere ganger avhengig av hvor produktet er produsert eller skal

selges, og man vil unngå at produsenter velger ordninger som gir en raskere og enklere sertifisering enn andre ordninger. Rammeverket skaper også fleksibilitet til å etablere tilpassede ordninger avhengig av produktets, tjenestens eller prosessenes egenart, og påkrevd sikkerhetsnivå.

Det er viktig at ny sertifiseringsløsning ikke kommer i konflikt med andre etablerte internasjonale sertifiseringsløsninger, men komplementerer eller understøtter disse. Forordningen ivaretar internasjonalt samarbeid gjennom ENISA. Det følger også av artikkel 54 bokstav t, at hver europeiske sertifiseringsordning skal oppstille betingelser for gjensidig anerkjennelse av sertifiseringsordninger med tredjeland. Det er således Kommisjonen som inngår avtalene med tredjelandene.

Siden gjennomføringen av EØS-komiteens beslutninger i norsk rett vil kreve lovendring og innebære budsjettmessige konsekvenser, er Stortingets samtykke til godkjennelse av EØS-komiteens beslutning nødvendig i medhold av Grunnloven § 26 annet ledd. I henhold til EØS-avtalen artikkel 93 nr. 2 skal beslutninger i EØS-komiteen treffes ved enighet mellom EU på den ene siden og EØS/EFTA-statene, som opptrer samstemt, på den andre. Det følger av artikkel 103 nr. 1 at beslutningen først blir bindende for Norge etter at man fra norsk side har meddelt de andre partene at de forfatningsmessige kravene er oppfylt.

Konklusjon

Forordningen anses som EØS-relevant. Forordningen anses som akseptabel, med de foreslåtte tilpasninger som sikrer EØS-EFTA statenes deltakelse og status i ENISA og ECCG (uten stemmerett).

Andre opplysninger

Oversikt over identifiserte rettslige konsekvenser:

Gjeldende forordning om ENISA er en del av EØS-avtalen, og er i dag gjennomført i ekomforskriften §8-7. Justis- og beredskapsdepartementet har funnet det mer hensiktsmessig å gjennomføre forordningen i forskrift til ny lov om digital sikkerhet, som også gjennomfører NIS-direktivet i norsk rett.

Et utkast til en slik lov ble sendt på høring 21. desember 2018.

Justis- og beredskapsdepartementet tar sikte på å legge frem en Prop. LS med en ny lov om digital sikkerhet og om Stortingets samtykke til godkjennelse av EØS-komiteens beslutning.

Medlemsstatene skal sørge for en nasjonal tilsynsmyndighet for sertifisering, hvis oppgaver bl.a. vil være kontroll med etterlevelsen av ordningen, sanksjoner ved brudd og klagebehandling. Myndighetene skal også få hjemmel til å få adgang til kontorlokaler for undersøkelser.

Myndighetene skal også samarbeide med andre sertifiseringsmyndigheter eller øvrige myndigheter, samt utveksle informasjon om manglende overholdelse av regelverket.

Etterlevelsesorganer skal akkrediteres av nasjonale akkrediteringsorganer som er utpekt etter (EU) 756/2008.

Økonomiske- og administrative konsekvenser

Norge er allerede assosiert medlem av ENISA (uten stemmerett). Medlemskapet ivaretas av både Justis- og beredskapsdepartementet og Kommunal- og distriktsdepartementet, og kostnadene fordeles likt mellom departementene og dekkes innenfor det enkelte departementets budsjett. Etter at forordningen trådte i kraft i EU i 2019, har kontingenten for medlemmer av ENISA økt. For 2021 og 2022 utgjorde den samlede kontingenten for norsk deltakelse i ENISA henholdsvis 5 643 744 og 5 271 246 kroner. De økte kostnadene er kostnader som allerede effektueres, uavhengig av om forordningen implementeres i EØS-avtalen eller ikke. Organisering og styring av ENISA er lite forandret etter forordningen trådte i kraft i EU i 2019, og departementet kan ikke se at innlemmelse av forordningen i EØS-avtalen vil medføre store endringer for Norges rolle i ENISA.

Hva gjelder cybersikkerhetssertifiseringsordningen forutsetter vurderingen av administrative og økonomiske konsekvenser i det følgende at det legges opp til en løsning hvor staten kun ivaretar den obligatoriske myndighetsrollen. Dette innebærer at kommersielle sertifiseringsorganer i størst mulig grad står for sertifisering av produkter, tjenester og prosesser, og at det kun utpekes en nasjonal cybersikkerhetssertifiseringsmyndighet (jf. artikkel 58).

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

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

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

Kravet om etablering av nasjonale organ i henhold til rammeverket for cybersikkerhetssertifisering vil innebære økonomiske konsekvenser. NSM har avsatt to stillinger til arbeid med sertifiseringsordningen for IT-sikkerhet (SERTIT). Disse stillingene har

både ansvar for rollen som sertifiseringsmyndighet og sertifiseringsorgan. Dette innebærer både forvaltning av sertifiseringsordningen etter ISO/IEC 15408 (Common Criteria), internasjonal oppfølging av CCRA og SOG-IS MRA samt sertifisering av produkter etter ordningene. Ved innføringen av forordningen vil ikke lenger den nasjonale sertifiseringsmyndigheten inneha rollen som sertifiseringsorgan. Samtidig vil den nasjonale sertifiseringsmyndigheten blant annet ha ansvar for mottak av klager, egenerklæringer, utpeking av sertifiseringsorgan samt føre tilsyn med disse. Grunnet stor fleksibilitet i hvordan de nasjonale sertifiseringsmyndighetene kan utføre sine oppgaver og manglende erfaringsgrunnlag, er det vanskelig å vurdere ressursbehovet med særlig nøyaktighet. Det anslås at det vil måtte avsettes ressurser til å følge opp den enkelte sertifiseringsordning, herunder utpeking av sertifiseringsorgan, mottak av eventuelle klager og egenerklæringer og tilsyn med sertifiseringsorganene. Videre vil det være behov for ressurser til oppfølging av den Europeiske cybersikkerhetssertifiseringsgruppen, kontakt med Norsk Akkreditering og andre relevante myndighetsaktører. Basert på tilgjengelig kunnskap om den fremtidige ordningen, anslås det ressursmessige merbehovet derfor til minimum to årsverk (ett årsverk per ordning).

Innføringen av forordningen vil utvide virkeområdet for sertifisering fra kun produkter til også å dekke tjenesteleveranser og prosesser. Riktig bruk av gode sertifiseringsordninger kan bidra til å øke den samlede evnen til å motstå ulike former for cyberoperasjoner og dermed gi samfunnsøkonomisk gevinst. Videre vil også anskaffelsesprosesser kunne forenkles gjennom å stille krav til bruk av sertifiserte produkter, tjenester eller prosesser. Norske virksomheter som har ønsket å få produkter sertifisert etter ISO/EIC 15408, har til nå nytt godt av at selve sertifiseringen har blitt utført vederlagsfritt gjennom SERTIT. Etter forordningen vil sertifisering i utgangspunktet gjøres av kommersielle sertifiseringsorganer, og dette medfører en betydelig merkostnad for disse virksomhetene. Samtidig er det viktig å understreke at bruken av sertifiserte produkter, tjenester og prosesser i utgangspunktet er frivillig, derfor vil et marked for sertifiserte produkter, tjenester eller prosesser være styrt av tilbud og etterspørsel. Dette må også sees i sammenheng med EU-kommisjonens forslag til et revidert direktiv for sikkerhet i nettverk og informasjonssystemer (NIS2), hvor det i noen grad legges opp til krav om sertifisering.

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

Sakkyndige instansers merknader

Faglige innspill til et tidligere utkast til forslag KOM 2017/477 er mottatt fra NSM, SD, Nkom, FD, KMD og NFD.

Det ble første gang orientert om forslag (KOM 2017/477) til rettsakt i spesialutvalget for kommunikasjoner der Samferdselsdepartementet, Kommunal- og

moderniseringsdepartementet, Barne- og likestillingsdepartementet, Justis- og beredskapsdepartementet, Utenriksdepartementet og Nasjonal kommunikasjonsmyndighet er representert, i januar 2018 og muntlig fremlagt for utvalget 2. februar 2018. Det ble videre muntlig redegjort for den vedtatte forordningen i møte i SU Kommunikasjoner i september 2019 og EØS-posisjonsnotat ble behandlet ved skriftlig prosedyre i november 2019. SU kommunikasjoner fant rettsakten relevant og akseptable for innlemming i EØS-avtalen med de tilpasninger som foreslås. Standardskjema ble returnert til EFTA-sekretariatet 20.12.2019.

KUNNSKAPSDEPARTEMENTET

32019R0128 Europaparlaments- og rådsforordning (EU) 2019/128 av 16. januar 2019 om opprettelse av et europeisk senter for utvikling av yrkesrettet opplæring (Cedefop) og om oppheving av rådsforordning (EØF) nr. 337/75

Status

EØS/EFTA-statene sendte 7. mars 2017 en felles uttalelse til EU hvor vi støttet forslaget til forordning, se lenke under "annen informasjon".

Forordningen trådde i kraft i januar 2019.

Forordningsteksten har vært til vurdering hos EFTA-arbeidsgruppen for utdanning.

Sammendrag av innhold

Det tas forbehold om Stortingets samtykke i medhold av EØS-avtalen artikkel 103, fordi dette er budsjettforpliktelser ut over ett budsjettår.

En viktig begrunnelse for en ny forordning er å tilpasse Cedefops virksomhet i tråd med nye mål og oppgaver som følge av store politiske prosesser innen fag- og yrkesopplæring i Europa de seneste årene. Cedefops rolle og oppgave har vært i sterk endring, fra å være et dokumentasjonssenter for fag- og yrkesopplæring til å bistå kommisjonen og medlemslandene i å utvikle verktøy som skal fremme mobilitet både i utdanning og arbeidslivet. Særlig viktige oppgaver for Cedefop de siste årene, som Norge har deltatt aktivt i, har vært å utvikle:

- EUROPASS
- European qualifications framework for life long learning (EQF)
- European credit system for VET (ECVET)
- European quality assurance framework for VET (EQAVET)
- Principles for guidance and councelling
- Principles for validating informal and non formal learning

En annen begrunnelsene for en ny forordning er å harmonisere bestemmelsene for alle EU-sentrene som bygger på 3-partsprinsippet, dvs. samarbeid mellom arbeidstakerorganisasjoner, arbeidsgiverorganisasjoner og nasjonale myndigheter. Dette gjelder Cedefop, Eurofound (senter for forbedring av leve- og arbeidsvilkår) og EU-OSHA (senter for europeiske arbeidsmiljøsaker). Forslaget til ny forordningen vil bygge videre på 3-partsprinsippet, men det foreslås å endre dagens styreform fra Governing Board (GB) til Managing Board (MB).

Merknader

Rettslige konsekvenser

Gjennomføring av forordningen vil ikke medføre noen endringer i norsk lovgivning eller annet regelverk.

Økonomiske og administrative konsekvenser

Norge har hatt en bilateral avtale med Cedefop vedrørende finansiering siden 1996. Det å innlemme Cedefop-forordningen i EØS-avtalen innebærer administrativ forenkling av EØS/EFTA-landenes innbetaling av kontingent til Cedefop.

Rettsakten ventes ikke å medføre økonomiske eller administrative konsekvenser av betydning. Fremtidig nivå på kontingenten er ventet å være på omtrent samme nivå som tidligere, og vil følge av EUs utbetalingsbudsjett som hensyntar valutakursendringer og BNP i sin beregning av programforpliktelser.

Sakkyndige instansers merknader

Kunnskapsdepartementet har vurdert rettsakten til å være EØS-relevant og akseptabel.

Vurdering

Kunnskapsdepartementet mener at endringen av forordningen er hensiktsmessig. Dette medfører at Cedefops mål og oppgaver er i samsvar med de reelle oppgavene senteret har. Forordningen foreslår å ytterligere utvide oppgaveporteføljen til også å omfatte kompetanse i arbeidslivet og analyser og prognoser for framtidig arbeidskraftsbehov. Etter departementets mening er en slik utvidelse naturlig, men det er viktig at en slik utvidelse ikke går på bekostning av Cedefops hovedansvar for VET-området.

Andre opplysninger

I 1996 inngikk EØS EFTA landende en bilateral avtale med Cedefop. Avtalen innebar at Norge og Island har full tilgang til alle Cedefops aktiviteter mot en årlig kontingent. Norge og Island har observatørstatus i styret og Norge er representert med en person fra KD, en fra LO og en fra NHO.

II. Rettsakter som krever forskriftsendring som ikke griper vesentlig inn i norsk handlefrihet, samt rettsakter som ikke har konsekvenser for norsk lovgivning

FINANSDEPARTEMENTET

32021R0369 Kommisjonens gjennomføringsforordning (EU) 2021/369 av 1. mars 2021 om fastsettelse av de tekniske spesifikasjonene og framgangsmåtene som kreves for systemet for sammenkobling av sentrale registre omhandlet i europaparlaments- og rådsdirektiv (EU) 2015/849 – EØS-notat

32022R2058 Delegert kommisjonsforordning (EU) 2022/2058 av 28. februar 2022 om utfylling av europaparlaments- og rådsforordning (EU) nr. 575/2013 med hensyn til tekniske reguleringsstandarder for likviditetsperioder for den alternative metoden med interne modeller som omhandlet i artikkel 325bd nr. 7 – EØS-notat

32022R2059 Delegert kommisjonsforordning (EU) 2022/2059 av 14. juni 2022 om utfylling av europaparlaments- og rådsforordning (EU) nr. 575/2013 med hensyn til tekniske regulerings standarder som presiserer de tekniske detaljene for krav til ettertesting og resultatanalyse i henhold til artikkel 325bf og 325bg i forordning (EU) nr. 575/2013 – EØS-notat

32022R2060 Delegert kommisjonsforordning (EU) 2022/2060 av 14. juni 2022 om utfylling av europaparlaments- og rådsforordning (EU) nr. 575/2013 med hensyn til tekniske reguleringsstandarder som spesifiserer kriteriene for vurdering av risikofaktorenes modellerbarhet etter metoden med interne modeller og hyppigheten av denne vurderingen i henhold til artikkel 325be nr. 3 i nevnte forordning– EØS-notat

32022R1299 Delegert kommisjonsforordning (EU) 2018/1229 av 24. mars 2022 om utfylling av europaparlaments- og rådsdirektiv 2014/65/EU med hensyn til tekniske reguleringsstandarder som spesifiserer innholdet i handelsplassers posisjonshåndteringskontroller – EØS-notat

32022R1300 Kommisjonens gjennomføringsforordning (EU) 2022/1300 av 24. mars 2022 om endring av gjennomføringsforordning (EU) 2017/1093 om fastsettelse av tekniske gjennomføringsstandarder for formatet til verdipapirforetaks og markedsoperatørers posisjonsrapporter – EØS-notat

32022R0975 Delegert kommisjonsforordning (EU) 2022/975 av 17. mars 2022 om endring av de tekniske reguleringsstandardene fastsatt i delegert forordning (EU) 2017/653 med hensyn til forlengelse av overgangsordningen fastsatt i artikkel 14 nr. 2 i nevnte forordning og om endring av de tekniske reguleringsstandardene fastsatt i delegert forordning (EU) 2021/2268 med hensyn til anvendelsesdatoen for nevnte forordning – EØS-notat

32021R0466 Delegert kommisjonsforordning (EU) 2021/466 av 17. november 2020 om utfylling av europaparlaments- og rådsforordning (EU) 2019/1700 ved å spesifisere antallet av og titler på variablene for området inntekter og levekår med hensyn til helse og livskvalitet – EØS-notat

HELSE- OG OMSORGSDEPARTEMENTET

32022R1418 Kommisjonens gjennomføringsforordning (EU) 2022/1418 av 22. august 2022 om endring av gjennomføringsforordning (EU) 2015/1375 med hensyn til trikinkontroll ved nedskjæring av skrotter og alternative analysemetoder – EØS-notat

32022R0519 Delegert kommisjonsforordning (EU) 2022/519 om endring av delegert forordning (EU) 2016/127 med hensyn til proteinkrav til morsmelkerstatninger og tilskuddsblandinger framstilt av proteinhydrolisat – EØS-notat

32022R0641 Europaparlaments- og rådsforordning (EU) 2022/641 av 12. april 2022 om endring av forordning (EU) nr. 536/2014 med hensyn til et unntak fra visse forpliktelser for visse utprøvingslegemidler som er gjort tilgjengelige i Storbritannia med hensyn til Nord-Irland, samt i Kypros, Irland og Malta – EØS-notat

32022R1255 Kommisjonens gjennomføringsforordning (EU) 2022/1255 av 19. juli 2022 om bestemmelse av antimikrobielle midler eller grupper av antimikrobielle midler som er forbeholdt behandling av visse infeksjoner hos mennesker, i samsvar med europaparlaments- og rådsforordning (EU) 2019/6 – EØS-notat

32022R2239 Delegert kommisjonsforordning (EU) 2022/2239 av 6. september 2022 om endring av europaparlaments- og rådsforordning (EU) nr. 536/2014 med hensyn til krav til merking av ikke-godkjente utprøvings- og tilleggslegemidler til mennesker – EØS-notat

32022R1107 Kommisjonens gjennomføringsforordning (EU) 2022/1107 av 4. juli 2022 om fastsettelse av felles spesifikasjoner for visse typer medisinsk utstyr til *in vitro*-diagnostikk i klasse D i samsvar med europaparlaments- og rådsforordning (EU) 2017/746 – EØS-notat

JUSTIS- OG BEREDSKAPSDEPARTMENTET

32021D1436 Kommisjonens gjennomføringsbeslutning (EU) 2021/1436 av 31. august 2021 om endring av europaparlaments- og rådsdirektiv 2008/68/EF om innlands transport av farlig gods for å godkjenne visse nasjonale unntak – EØS-notat

32022D1095 Kommisjonens gjennomføringsbeslutning (EU) 2022/1095 av 29. juni 2022 om endring av europaparlaments- og rådsdirektiv 2008/68/EF om innlands transport av farlig gods for å godkjenne visse nasjonale unntak – EØS-notat

32021R0887 Europaparlaments- og rådsforordning (EU) 2021/887 av 20. mai 2021 om opprettelse av Det europeiske kompetansesenter for cybersikkerhet innen industri, teknologi og forskning og av nettverket av nasjonale samordningssentre – EØS-notat

KLIMA- OG MILJØDEPARTEMENTET

32022R0835 Kommisjonens gjennomføringsbeslutning (EU) 2022/835 av 25. mai 2022 om de uløste innvendingene med hensyn til vilkårene for godkjenning av biocidproduktet Primer Stain TIP i samsvar med europaparlaments- og rådsforordning (EU) nr. 528/2012 – EØS-notat

32022D0866 Kommisjonens gjennomføringsbeslutning (EU) 2022/866 av 25. mai 2022 om de uløste innvendingene med hensyn til vilkårene for godkjenning av biocidproduktet Primer PIP i samsvar med europaparlaments- og rådsforordning (EU) nr. 528/2012 – EØS-notat

32022D0874 Kommisjonens gjennomføringsbeslutning (EU) 2022/874 av 1. juni 2022 om vilkårene for godkjenning av et biocidprodukt som inneholder N-(triklormetyltio)ftalimid (folpet), forelagt av Nederland i samsvar med artikkel 36 nr. 1 i europaparlaments- og rådsforordning (EU) nr. 528/2012 – EØS-notat

32022R0477 Kommisjonsforordning (EU) 2022/477 av 24. mars om endring av vedlegg VI–X til europaparlaments- og rådsforordning (EF) nr. 1907/2006 om registrering, vurdering og godkjenning av samt begrensninger for kjemikalier (REACH) – EØS-notat

32021D2267 Kommisjonens gjennomføringsbeslutning (EU) 2021/2267 av 17. desember 2021 om fastsettelse av formatet for rapportering av data og opplysninger om innsamlet avfall etter forbruk av tobakksvarer med filter og av filtre som markedsføres for bruk i kombinasjon med tobakksvarer – EØS-notat

32022D0162 Kommisjonens gjennomføringsbeslutning (EU) 2022/162 av 4. februar 2022 om fastsettelse av regler for anvendelse av europaparlaments- og rådsdirektiv (EU) 2019/904 med hensyn til beregning, verifisering og rapportering av reduksjonen i forbruket av visse engangsprodukter av plast og tiltak truffet av medlemsstatene for å oppnå reduksjonen – EØS-notat

LANDBRUKS- OG MATDEPARTEMENTET

32022D1377 Kommisjonens gjennomføringsavgjerdbeslutning (EU) 2022/1377 av 4. august 2022 om endring av vedlegget til vedtak 2007/453/EU med omsyn til BSE-statusen til Frankrike – EØS-notat

32022L0905 Kommisjonens gjennomføringsdirektiv (EU) 2022/905 av 9. juni 2022 om endring av direktiv 2003/90/EF og 2003/91/EF med omsyn til protokollane for gransking av visse sortar av jordbruksvekstar og grønsaker – EØS-notat

32022R0740 Kommisjonens gjennomføringsforordning (EU) 2022/740 av 13. mai 2022 om avslag på godkjenning av det aktive stoffet 1,3-diklorpropen i samsvar med europaparlaments- og rådsforordning (EF) nr. 1107/2009 om omsetning av plantevernmidler – EØS-notat

32022R0751 Kommisjonens gjennomføringsforordning (EU) 2022/751 av 16. mai 2022 om avslag på godkjenning av det aktive stoffet kloropikrin i samsvar med europaparlaments- og rådsforordning (EF) nr. 1107/2009 om omsetning av plantevernmidler – EØS-notat

32022R0800 Kommisjonens gjennomføringsforordning (EU) 2022/800 av 20. mai 2022 om endring av gjennomføringsforordning (EU) nr. 540/2011 med hensyn til vilkår for godkjenning av de aktive stoffene «parafinoljer» med CAS-nr. 64742-46-7, CAS-nr. 72623-86-0 og CAS-nr. 97862-82-3 – EØS-notat

32022R0801 Kommisjonens gjennomføringsforordning (EU) 2022/801 av 20. mai 2022 om endring av gjennomføringsforordning (EU) nr. 540/2011 for å oppdatere listen over aktive stoffer som er godkjent eller som anses som godkjent i henhold til europaparlaments- og rådsforordning (EU) nr. 1107/2009 – EØS-notat

32022R0808 Kommisjonens gjennomføringsforordning (EU) 2022/808 av 23. mai 2022 om endring av gjennomføringsforordning (EU) nr. 540/2011 med hensyn til godkjenningsperioden for det aktive stoffet bispyribac – EØS-notat

32022R0814 Kommisjonens gjennomføringsforordning (EU) 2022/814 av 20. mai 2022 om endring av gjennomføringsforordning (EU) nr. 540/2011 med hensyn til forlengelse av godkjenningsperioden for det aktive stoffet heptamaloksyloglukan – EØS-notat

32022R1252 Kommisjonens gjennomføringsforordning (EU) 2022/1252 av 19. juli 2022 om endring av gjennomføringsforordning (EU) 2015/408 for å oppdatere listen over stoffer som bør erstattes – EØS-notat

32022R1443 Kommisjonens gjennomføringsforordning (EU) 2022/1443 av 31. august 2022 om avslag på godkjenning av kalsiumpropionat som basisstoff i samsvar med europaparlaments- og rådsforordning (EF) nr. 1107/2009 om omsetning av plantevernmidler – EØS-notat

32022R1444 Kommisjonens gjennomføringsforordning (EU) 2022/1444 av 31. august 2022 om avslag på godkjenning av svart såpe E470a som basisstoff i samsvar med europaparlaments- og rådsforordning (EF) nr. 1107/2009 om omsetning av plantevernmidler – EØS-notat

32022R1468 Kommisjonens gjennomføringsforordning (EU) 2022/1468 av 5. september 2022 om endring av gjennomføringsforordning (EU) nr. 540/2011 med hensyn til vilkårene for godkjenning av det aktive stoffet penflufen, og om oppheving av gjennomføringsforordning (EU) 2018/185 – EØS-notat

32022R1474 Kommisjonens gjennomførelsesforordning (EU) 2022/1474 av 6. september 2022 om fornyet godkjenning av sauefett som et aktivt stoff med lav risiko i samsvar med europaparlaments- og rådsforordning (EU) 1107/2009 om omsetning av plantevernmidler, og om endring av vedlegget til Kommisjonens gjennomføringsforordning (EU) 540/2011 – EØS-notat

32022R1480 Kommisjonens gjennomføringsforordning (EU) 2022/1480 av 7. september 2022 om endring av gjennomføringsforordning (EU) nr. 540/2011 med hensyn til forlengelse

av godkjenningsperiodene for de aktive stoffene 2-fenylfenol (herunder saltene, for eksempel natriumsalt), 8-hydroksykinolin, amidosulfuron, bensulfuron, bifenoks, klormekvat, klortoluron, klofentezin, klomazon, daminozid, deltametrin, dikamba, difenokonazol, diflufenikan, dimetaklor, esfenvalerat, etofenproks, fenoksaprop-P, fenpropidin, fenpyrazamin, fludioksonil, flufenacet, flumetralin, fostiazat, lenacil, MCPA, MCPB, nikosulfuron, parafinoljer, parafinolje, penkonazol, pikloram, proheksadion, propakizafop, prosulfokarb, kizalofop-P-etyl, kizalofop-P-tefuryl, natrium-5-nitroguaiakolat, natrium o-nitrofenolat, natrium p-nitrofenolat, svovel, tebufenpyrad, tetrakonazol, tri-allat, triflusulfuron og tritosulfuron – EØS-notat

LANDBRUKS- OG MATDEPARTEMENTET OG NÆRINGS- OG FISKERIDEPARTEMENTET

32022R1457 Kommisjonens gjennomføringsforordning (EU) 2022/1457 av 2. september 2022 om endring av gjennomføringsforordning (EU) 2017/2330 med hensyn til vilkårene for godkjenning av jern(II)kelat av aminosyrehydrat som tilsetningsstoff i fôr til alle dyrearter – EØS-notat

NÆRINGS- OG FISKERIDEPARTEMENTET

32020R1668 Kommisjonens gjennomføringsforordning (EU) 2020/1668 av 10. november 2020 om fastsettelse av detaljene og funksjonene i informasjons- og kommunikasjonssystemet som skal benyttes i henhold til europaparlaments- og rådsforordning (EU) 2019/515 om gjensidig godkjenning av varer som omsettes lovlig i en annen medlemsstat – EØS-notat

SAMFERDSELSDEPARTEMENTET

32022R1398 Delegert kommisjonsforordning (EU) 2022/1398 av 8. juni 2022 om endring av europaparlaments- og rådsforordning (EU) 2019/2144 for å ta hensyn til den tekniske utviklingen og regelverksutviklingen med hensyn til endringer i kjøretøyregulativer vedtatt innenfor rammen av De forente nasjoners økonomiske kommisjon for Europa – EØS-notat vedlagt som eget dokument

32022R0694 Kommisjonens gjennomføringsforordning (EU) 2022/694 av 2. mai 2022 om endring av forordning (EU) 2016/403 med hensyn til nye alvorlige overtredelser av Unionens regler som kan føre til at et veitransportforetak ikke oppfyller vandelskravet – EØS-notat

Endringer sammenlignet med foreløpig liste oversendt Stortinget 12. januar 2023

I. Rettsakter som krever lov- eller budsjettendring samt rettsakter som krever forskriftsendring som vurderes å gripe vesentlig inn i norsk handlefrihet

KUNNSKAPSDEPARTEMENTET

32019R0128 Europaparlaments- og rådsforordning (EU) 2019/128 av 16. januar 2019 om opprettelse av et europeisk senter for utvikling av yrkesrettet opplæring (Cedefop) og om oppheving av rådsforordning (EØF) nr. 337/75 – *Tilføyd etter at foreløpig liste ble sendt*.

II. Rettsakter som krever forskriftsendring som ikke griper vesentlig inn i norsk handlefrihet, samt rettsakter som ikke har konsekvenser for norsk lovgivning

FINANSDEPARTEMENTET

32022RXXXX Delegert kommisjonsforordning (EU) …/... om endring av de tekniske reguleringsstandardene fastsatt i delegert forordning (EU) 2016/2251 med hensyn til anvendelsesdatoen for visse framgangsmåter for risikostyring for utveksling av sikkerhet – *Trukket av EU* 32022RXXXX Delegert kommisjonsforordning (EU) …/... om endring av de tekniske reguleringsstandardene fastsatt i delegert forordning (EU) 2015/2205, (EU) 2016/592 og (EU) 2016/1178 med hensyn til ikrafttredelsesdatoen for clearingplikten for visse typer kontrakter – *Trukket av EU* 32022R0750 Kommisjonsforordning (EU) 2022/750 av 8. februar 2022 om endring av de regulatoriske tekniske standardene fastsatt i forordning (EU) 2015/2205 om overgangen til nye referanseverdier som anvendes som referanse i visse OTC-derivatkontrakter – *Trukket av EU*

32020R1148 Kommisjonens gjennomføringsforordning (EU) 2020/1148 av 31. juli 2020 om fastsettelse av metodologiske og tekniske spesifikasjoner i samsvar med europaparlaments- og rådsforordning (EU) 2016/792 med hensyn til harmoniserte konsumprisindekser og boligprisindeksen – *Trukket av EU*

NÆRINGS- OG FISKERIDEPARTEMENTET

32007D0421 Kommisjonsvedtak av 14. juni 2007 om oppheving av vedtak 96/587/EF om offentliggjøring av en liste over godkjente organisasjoner meldt av medlemsstatene i samsvar med rådsdirektiv 94/57/EF – *Trukket av EU*

52007XC0619(01) Liste over organisasjoner anerkjent på grunnlag av rådsdirektiv 94/57/EF om felles regler og standarder for organisasjoner som skal inspisere og besikte skip, og for sjøfartsmyndighetenes virksomhet i den forbindelse – *Trukket av EU*

SAMFERDSELSDEPARTEMENTET

32022R0862 Kommisjonens gjennomføringsforordning (EU) 2022/862 av 1. juni 2022 om endring av forordning (EF) nr. 474/2006 med hensyn til listen over luftfartsselskaper som er underlagt driftsforbud eller driftsbegrensninger i Unionen – *Trukket av EU*

32022R1174 Kommisjonens gjennomføringsforordning (EU) 2022/1174 av 7. juli 2022 om endring av gjennomføringsforordning (EU) 2015/1998 med hensyn til visse detaljerte tiltak for gjennomføring av de felles grunnleggende standardene for luftfartssikkerhet – *Trukket av EU*

C(2022)4638 Kommisjonens gjennomføringsbeslutning C(2022) 4638 om endring av gjennomføringsbeslutning C(2015) 8005 med hensyn til visse detaljerte tiltak for gjennomføring av de felles grunnleggende standardene for luftfartssikkerhet – *Trukket av EU*