# Høringsnotat – forslag til utfyllende forskrifter til ny lov om digital operasjonell motstandsdyktighet i finanssektoren (DORA-loven)

## 1. Innledning og bakgrunn

Finansdepartementet fremmet den 7. mars 2025 Prop. LS 54 (2024 – 2025) som blant annet inneholder forslag til nasjonal gjennomføring av forordning (EU) 2022/2554 om digital operasjonell motstandsdyktighet i finanssektoren (DORA) i en ny lov om digital operasjonell motstandsdyktighet i finanssektoren (DORA-loven).

I brev av samme dato ber Finansdepartementet om at Finanstilsynet utarbeider utkast til utfyllende forskrifter som bør være på plass samtidig med loven, med utgangspunkt i lovforslaget i proposisjonen. Departementet ber videre om at utkast til eventuelle forskriftsregler som kan settes i kraft senere enn den nye loven oversendes på et senere tidspunkt i 2025.

DORA med tilhørende delegerte kommisjonsforordninger innebærer en harmonisering av krav til IKT-sikkerheten i finansielle foretak i Europa, blant annet gjennom krav til foretakenes risikostyring, hendelsesrapportering, testing, avtaler om bruk av IKT-tjenester og oppfølging av IKT-leverandører samt tilsyn og tilsynssamarbeid. Sammenlignet med gjeldende rett, er DORA-regelverket et mer omfattende og detaljert regelverk. Regelverket stiller krav til både overordnet og nærmere rammeverk for styring av IKT-risiko, håndtering av IKT-hendelser, trusselbasert penetrasjonstesting og overvåkning av kritiske IKT-tjenesteleverandører.

Følgende foretak er omfattet av DORA:

- kredittinstitusjoner
- betalingsforetak
- opplysningsfullmektige
- e-pengeforetak
- verdipapirforetak
- tilbydere av tjenester knyttet til kryptoverdier
- verdipapirsentraler
- sentrale motparter
- handelsplasser
- transaksjonsregistre
- forvaltere av alternative investeringsfond
- forvaltningsselskaper
- leverandører av datarapporteringstjenester
- forsikrings- og gjenforsikringsforetak
- forsikringsformidlere, gjenforsikringsformidlere og tilknyttede forsikringsformidlere
- pensjonsforetak

- kredittvurderingsbyråer
- administratorer av kritiske referanseverdier
- tjenesteleverandører for folkefinansiering
- verdipapiriseringsregistre
- tredjepartstilbydere av IKT-tjenester.

Prop. 54 LS (2024–2025) med forslag til DORA-loven og samtykkevedtak til innlemmelse av DORA i EØS-avtalen, ble lagt fram for Stortinget 7. mars 2025. Lovforslaget vil gjennomføre DORA i norsk rett. Finansdepartementet har foreslått at DORA-loven skal inneholde hjemler som gir departementet adgang til å fastsette utfyllende regler til loven. I § 1 tredje ledd gis det en generell adgang til å fastsette utfyllende forskrifter til forordningen, herunder adgang til å gjennomføre utfyllende EU-rettsakter fastsatt i medhold av DORA som forskrift under DORA-loven. Dette inkluderer også utfyllende rettsakter som er fastsatt i EU, men foreløpig ikke inntatt i EØS-avtalen.

EU-kommisjonen har fastsatt flere delegerte kommisjonsforordninger med utfyllende regler til DORA:

| **Referanse** | **Innhold** |
|---|---|
| (EU) 2024/1502 | Kriterier for å peke ut kritiske tredjepartstilbydere av IKT-tjenester |
| (EU) 2024/1505 | Tilsynsavgift for kritiske tredjepartstilbydere av IKT-tjenester |
| (EU) 2025/295 | Harmonisering av vilkår som legger til rette for overvåkning |
| (EU) 2024/1772[1] | Kriterier for klassifisering av hendelser og cybertrusler |
| (EU) 2024/1773[1] | Krav til retningslinjer for kontraktsvilkår ved bruk av tredjepartstilbydere av IKT-tjenester som støtter kritiske eller viktige funksjoner |
| (EU) 2024/1774[1] | Krav til rammeverk for styring av IKT-risiko, inkludert forenklet rammeverk for nærmere definerte (små) foretak |
| (EU) 2024/2956 | Krav til register over IKT-tjenesteavtaler |
| (EU) 2025/301 | Krav til innhold og frister for rapportering av hendelser |
| (EU) 2025/302 | Krav til og maler for rapportering av hendelser |

I tillegg er ytterligere to delegerte kommisjonsforordninger under utarbeidelse og antas å bli vedtatt i EU tidligst juni/juli 2025. Den ene gir utfyllende regler for trusselbasert penetrasjonstesting (TLPT), mens den andre gjelder IKT-tjenesteleverandørers bruk av underleverandører.

Finanstilsynet mener at innholdet i kommisjonsforordningene (EU) 2024/1502, 2024/1505 og 2025/295 tilsier at disse ikke behøver å tre i kraft samtidig med DORA-loven. Nevnte kommisjonsforordninger vil derfor ikke bli nærmere omtalt i høringsnotatet.

[1] Rettsakten ble inntatt i EØS-avtalen den 14. mars 2025.

For de resterende forordningene er Finanstilsynets vurdering at de har bestemmelser som nødvendiggjør at de trer i kraft samtidig med DORA regelverket i Norge.

I kapittel 2 gis en gjennomgang av gjeldende rett. Forventet EØS-rett omtales i kapittel 3. Finanstilsynets vurderinger av hvilke forordninger som bør inkluderes i utfyllende forskrifter gis i kapittel 4. Vurderinger av økonomiske og administrative konsekvenser som følger av regelverket er omtalt i kapittel 5. Til slutt følger utkast til forskrift om digital operasjonell motstandsdyktighet i finanssektoren (DORA-forskriften) i kapittel 6.

## 2. Gjeldende rett

Dagens norske IKT-regelverk og tilsynsmessige oppfølging bygger på de samme prinsippene som DORA, som begge har til formål å styrke IKT-sikkerheten i norsk finanssektor.

Foretakene i den norske finanssektoren har i mange år vært underlagt regelverk og tilsyn som skal bidra til en høy grad av IKT-sikkerhet. Særlig har forskrift 21. mai 2003 nr. 630 om bruk av informasjons- og kommunikasjonsteknologi (IKT-forskriften) stilt omfattende krav til IKT-sikkerhet i finanssektoren.

Etter IKT-forskriftens § 1 gjelder forskriften for norske:

- Banker
- Kredittforetak
- Finansieringsforetak
- Forsikringsforetak
- Private, kommunale og fylkeskommunale pensjonskasser og pensjonsfond
- Børser og autoriserte markedsplasser
- Verdipapirforetak
- Forvaltningsselskaper for verdipapirfond
- Inkassoforetak
- Eiendomsmeglerforetak
- Betalingsforetak og opplysningsfullmektiger
- E-pengeforetak
- Systemer for betalingstjenester.

I medhold av gjeldsinformasjonsforskriften § 8 gjelder IKT-forskriften også for gjeldsinformasjonsforetak og kredittopplysningsforetak.

IKT-forskriften § 2 gjelder planlegging og organisering av IKT-virksomheten. Det stilles krav til at foretakene skal fastsette overordnede mål, strategier og sikkerhetskrav for IKT-virksomheten. Bestemmelsen stiller også krav til utkontraktering av IKT-virksomhet, som er nærmere behandlet i § 12. I forskrift 15. september 2021 nr. 2777 om meldeplikt ved utkontraktering av virksomhet mv stilles det i § 1 krav til oversikt over utkontraktert virksomhet.

Krav til fastsettelse av kriterier for akseptabel risiko, dokumentert prosess for risikoanalyser av IKT-virksomheten og til å gjennomføre risikoanalyser minst årlig framgår av § 3. Etter § 4

stilles det krav til kvalitetsmål for IKT-virksomheten og dokumenterte prosedyrer for oppfølging, mens foretakene etter § 5 skal ha prosedyrer for beskyttelse av sin IKT-virksomhet mot skader, misbruk, uautorisert adgang og endring, samt hærverk.

Forskriftens §§ 6 og 7 stiller krav til at foretakene har skriftlige prosedyrer for anskaffelse, utvikling og testing av IKT-systemer, samt krav om å sikre at systemene vedlikeholdes og forvaltes på en måte som gir en stabil, planlagt og forutsigbar drift. Etter § 8 skal driften være basert på dokumenterte prosedyrer som sikrer fullstendig, rettidig og korrekt behandling og oppbevaring av data, samt en tilgjengelighet i tråd med foretakets dokumenterte krav. Foretaket skal gjennomføre regelmessige analyser og tiltak for å motvirke avvik, samt teste og dokumentere at driften fungerer i henhold til foretakets dokumenterte krav.

Etter IKT-forskriften § 9 stilles det krav om at foretakene sikrer at prosedyrer for avviks- og endringshåndtering foreligger og følges. Prosedyrer for avvikshåndtering skal blant annet omfatte alle avvik som oppstår i driften av IKT-systemene, og ha som formål å gjenopprette normal tilstand. Prosedyrer for endringshåndtering skal på sin side omfatte alle endringer som kan påvirke IKT-systemene og skal sikre forsvarlig, formell behandling og dokumentering av endringene. Foretakene skal sikre at prosedyrene for endringshåndtering gir en stabil, planlagt og forutsigbar drift. Bestemmelsen stiller også krav til at foretakene uten ugrunnet opphold rapporterer til Finanstilsynet om operasjonelle hendelser eller sikkerhetshendelser som medfører vesentlig reduksjon i funksjonalitet som følge av brudd på konfidensialitet (beskyttelse av data), integritet (sikring mot uautoriserte endringer) eller tilgjengelighet til IKT-systemer og/eller data.

Foretakene skal i henhold til § 11 ha en dokumentert kriseplan der foretakene minst en gang årlig skal gjennomføre opplæring, øvelse og testing av at kriseløsningen virker som forutsatt.

Til slutt stiller § 13 krav om at det skal foreligge en samlet oppdatert oversikt over organisasjon, utstyr, IKT-systemer og vesentlige forhold i IKT-virksomheten.

Verdipapirsentraler var tidligere underlagt IKT-forskriften, men ble i 2020 i stedet underlagt den nye verdipapirsentralloven med tilhørende regelverk på området.

# 3. Forventet EØS-rett - Innholdet i de delegerte kommisjonsforordningene

## 3.1 Innledning

Kommisjonsforordningene som foreslås inkludert i utfyllende forskrifter til DORA blir nærmere omtalt i delkapittel 3.2 til 3.5 nedenfor. Rettsaktene omhandler krav til hendelsesrapportering, retningslinjer for kontraktsvilkår ved bruk av tredjepartstilbydere av IKT-tjenester som støtter kritiske eller viktige funksjoner, rammeverket for styring av IKT-risiko og register over IKT-tjenesteavtaler.

## 3.2 Hendelseshåndtering

*3.2.1 (EU) 2024/1772 - Kriterier for klassifisering hendelser og cybertrusler*

Kommisjonsforordningens formål er å sikre at IKT-relaterte hendelser og cybertrusler blir likt vurdert av foretakene på tvers av landene i EU/EØS. Artikkel 1 til 7 inneholder detaljerte regler for klassifisering av IKT-relaterte hendelser. Etter artikkel 8 og 9 skal klassifiseringsmomentene i de foregående artiklene benyttes i vurderingen av om en hendelse skal klassifiseres som en alvorlig IKT-relatert hendelse som er rapporteringspliktig. Terskelverdiene for når en cybertrussel skal klassifiseres som betydelig står i artikkel 10. Til slutt gir artikkel 11 og 12 utfyllende regler knyttet til vurderingen av om en alvorlig hendelse er relevant for andre myndigheter i EU/EØS og hva slags informasjon som skal deles med disse.

*3.2.2 (EU) 2025/301 - Krav til innhold og frister for rapportering av hendelser*

For å sikre harmonisering rundt rapportering av IKT-hendelser og cybertrusler, inneholder kommisjonsforordningen detaljerte krav til innholdet i rapporter om alvorlige IKT-relaterte hendelser og betydelige cybertrusler i henholdsvis artikkel 1 til 4 og artikkel 6. Tidsfrister for innsending av de ulike rapporttypene[2] ved rapportering av alvorlige IKT-relaterte hendelser til nasjonale tilsynsmyndigheter framgår av artikkel 5.

*3.2.3 (EU) 2025/302 - Krav til og maler for rapportering av hendelser*

For at hendelsesrapporteringen fra foretak skal skje i samme format på tvers av landene i EU/EØS inneholder kommisjonsforordningen krav til maler som skal benyttes.

Artikkel 1 inneholder mal for de ulike rapporttypene ved rapportering av alvorlige IKT-hendelser. Etter artikkel 4 stilles det krav til at rapporteringen av alvorlige IKT-hendelser skal skje i sikre kanaler.

Foretakenes mulighet for å sende inn flere rapporttyper samtidig ved rapportering av alvorlige IKT-hendelser reguleres i artikkel 2. Etter artikkel 3 skal foretakene rapportere samlet om tilbakevendende IKT-hendelser som sammen kan klassifiseres som en alvorlig hendelse. Foretak som tidligere har rapportert om en hendelse som senere viser seg ikke å ha vært alvorlig har etter artikkel 5 en plikt til å varsle kompetente myndigheter om dette.

Rettsakten stiller også krav til melding om utkontraktering av hendelsesrapportering i artikkel 6. Rettsaktens artikkel 7 åpner videre for aggregert hendelsesrapportering ved at tredjepartsleverandører kan rapportere på vegne av flere foretak.

Mal for frivillig rapportering av betydelige cybertrusler følger av artikkel 8.

[2] Innledende varsel, statusrapporter og endelig rapport.

### 3.3 (EU) 2024/1773 - Krav til retningslinjer for kontraktsvilkår ved bruk av tredjepartstilbydere av IKT-tjenester som støtter kritiske eller viktige funksjoner

Kommisjonsforordningen angir nærmere krav til foretakenes retningslinjer for kontraktsvilkår ved bruk av tredjepartstilbydere av IKT-tjenester som støtter kritiske og viktige funksjoner.

Artikkel 1 angir at kravet til retningslinjer blant annet skal vurderes ut fra foretakets størrelse og risikoprofil. Etter artikkel 2 vil morselskapet i et konsern være ansvarlig for at retningslinjene anvendes konsekvent og effektivt på tvers av konsernets foretak.

I artikkel 3 stilles det blant annet krav til ledelsesorganets ansvar overfor retningslinjene, mens artikkel 4 stiller nærmere krav til retningslinjenes innhold. Artikkel 5 stiller krav til retningslinjenes innhold knyttet til elementer som skal inngå i risikovurderingen ved avtaleinngåelse med en IKT-tjenesteleverandør. Krav til prosess for vurdering og valg av leverandør framgår av artikkel 6, mens krav til retningslinjenes innhold om håndtering av eventuelle interessekonflikter og innhold om kontraktsvilkår framgår henholdsvis av artikkel 7 og 8. Retningslinjenes innhold om krav til overvåking av avtaleforholdet og til exit-planer følger henholdsvis av artikkel 9 og 10.

### 3.4 (EU) 2024/1774 – Krav til rammeverk for styring av IKT-risiko, inkludert forenklet rammeverk for nærmere definerte (små) foretak

Kommisjonsforordningen inneholder regler som skal styrke foretakenes oppfølging av IKT-risiko. Hvilke elementer det kan tas hensyn når det gjelder proporsjonalitet framgår av artikkel 1.

I artiklene 2 til 26 stilles det detaljerte krav til utarbeidelse, dokumentering og implementering av retningslinjer, rutiner, protokoller og verktøy knyttet til IKT-risiko og -sikkerhet som skal inngå i foretakets IKT-risikostyringsrammeverk. Rammeverket skal inneholde retningslinjer, rutiner, protokoller og verktøy for informasjonssikkerhet, blant annet for forvaltning av IKT-eiendeler, bruken av kryptering og kryptografi, fysisk og miljømessig sikkerhet knyttet til IKT-driften og -virksomheten, styring av nettsikkerhet, styring av IKT-prosjekter og -endringer, styring av tilganger og adganger, håndtering av IKT-hendelser, styring av IKT-driftsstabilitet, planer for IKT-beredskap og -gjenoppretting og testing av disse og testing av IKT-sikkerhet.

For foretak som faller inn under definisjonen i DORA artikkel 16 nr. 1, vil et forenklet IKT-risikostyringsrammeverk være tilstrekkelig. Det vil være enkelte verdipapirforetak, betalingsinstitusjoner, e-pengeforetak, og små tjenestepensjonsforetak.

For elementer som skal inngå i forenklede IKT-risikostyringsrammeverk framgår de detaljerte kravene til utarbeidelse, dokumentering og implementering av retningslinjer, rutiner, protokoller og verktøy knyttet til IKT-risiko og –sikkerhet av artiklene 28 til 40. Rammeverket skal inneholde retningslinjer, rutiner, protokoller og verktøy for informasjonssikkerhet, blant annet for forvaltning av IKT-eiendeler, fysisk og miljømessig

sikkerhet knyttet til IKT-driften og -virksomheten, styring av nettsikkerhet, styring av IKT-prosjekter og -endringer, styring av tilganger og adganger, håndtering av IKT-hendelser, styring av IKT-driftsstabilitet, test av IKT-beredskapsplaner og IKT-sikkerhet.

Artikkel 27 gir nærmere krav til myndighetsrapportering av foretakets årlige gjennomgang av rammeverket for IKT-risikostyring. For foretak som kvalifiserer til å ha et forenklet IKT-risikostyringsrammeverk (jf. DORA art. 16 nr. 1) følger nærmere krav til myndighetsrapportering av artikkel 41.

### 3.5 (EU) 2024/2956 – Krav til register over IKT-tjenesteavtaler

Noe av hensikten med de detaljerte kravene til registerføringen er at registrene skal videresendes for bruk av de europeiske finanstilsynsmyndighetenes (EBA, ESMA og EIOPA) utpeking av kritiske IKT-tjenesteleverandører.

Artikkel 1 i kommisjonsforordningen inneholder definisjoner som benyttes i forordningen. Maler for utfylling av foretakenes register over IKT-tjenesteavtaler og generelle krav til malene framgår av artikkel 3. Vedlegg III til kommisjonsforordningen oppgir hvilke typer IKT-tjenester som skal inkluderes i registre over IKT-tjenesteavtaler. Rettsakten inneholder også regler for hvordan malene skal fylles ut og hvilken informasjon registeret skal inneholde i artikkel 5. Krav til registerets innhold presiseres nærmere i artikkel 2, 4 og 6 som henholdsvis regulerer hvordan leverandører skal rangeres, krav til dataformat og hvilke leverandører/foretak som skal inkluderes ved konsolidert rapportering i konsern.

## 4. Vurderinger

### 4.1 Innledning

En rekke bestemmelser i de delegerte kommisjonsforordningene til DORA-regelverket regulerer den praktiske gjennomføringen av bestemmelser i DORA. I proposisjonen til DORA-loven pekes det derfor på at det vil være uheldig for norske foretak og kunne svekke effekten av DORA-regelverket dersom delegerte kommisjonsforordninger med regler av en slik karakter trer i kraft vesentlig senere enn i EU grunnet forsinkelse som følge av EØS-prosessen.

### 4.2 Vurdering av kommisjonsforordninger som er inntatt i EØS-avtalen

Kommisjonsforordningene (EU) 2024/1772, (EU) 2024/1773 og (EU) 2024/1774 ble inntatt i EØS-avtalen den 14. mars 2025. De vurderes alle å inneholde krav av en slik karakter at en forsinket implementering vil svekke effekten av DORA-regelverket.

Kommisjonsforordning (EU) 2024/1772 inneholder utfyllende krav til hvordan foretak skal kunne avgjøre om en IKT-relatert hendelse er rapporteringspliktig. Reglene om hendelsesrapportering i DORA ville mistet sin effekt dersom den delegerte kommisjonsforordningen ikke trer i kraft samtidig med reglene i DORA.

Bestemmelser som retter seg mot foretakenes kritiske og viktige funksjoner står sentralt i DORA-regelverket. De utdypende kravene i (EU) 2024/1773 til retningslinjer for kontraktsvilkår for bruk av tredjepartstilbydere av IKT-tjenester som støtter slike funksjoner er viktig i foretakenes arbeid med å sørge for at eksisterende avtaler er i samsvar med DORA-regelverket, men også ved inngåelse av nye avtaler.

I kommisjonsforordning (EU) 2024/1774 stilles det detaljerte krav til styring og oppfølging av IKT-risiko og -sikkerhet som skal inngå i foretakets IKT-risikostyringsrammeverk. Eksempelvis stiller ikke DORA nærmere krav til kryptering og forvaltning av krypteringsnøkler. Det stilles derimot nærmere krav til nevnte momenter i kommisjonsforordningen. Effekten av DORA-regelverket vil følgelig bli betydelig svekket dersom de mer spesifikke kravene til IKT-risikostyring i kommisjonsforordningen ikke trer i kraft samtidig med DORA. Viktigheten av overholdelsen av kravene i kommisjonsforordningen kan også underbygges ved at det brudd på enhver bestemmelse i rettsakten er foreslått som grunnlag for sanksjonering.

## 4.3 Vurdering av kommisjonsforordninger som ikke er inntatt i EØS-avtalen

Kommisjonsforordningene (EU) 2025/301 og (EU) 2025/302 spesifiserer henholdsvis krav til innhold og frister, samt nærmere krav til, og maler for, foretakenes innrapportering av alvorlige IKT-relaterte hendelser og betydelige cybertrusler til Finanstilsynet. Krav til innrapportering er i all hovedsak en videreføring av dagens regler og praksis, og er en viktig del at det løpende tilsynet og ivaretakelse av Finanstilsynets rolle som sektorvis responsmiljø. DORA-regelverket innfører er nytt krav til at alvorlige hendelser skal rapporteres videre til de europeiske finanstilsynsmyndighetene, som så vil videreformidle informasjonen til eventuelle andre berørte lands tilsynsmyndigheter.

Hensynet til viktigheten av innrapportering og videreformidling av alvorlige IKT-hendelser tilsier at rettsaktene (EU) 2025/301 og (EU) 2025/302 bør implementeres samtidig som DORA-loven trer i kraft, selv om dette medfører en førtidig ikrafttredelse.

Kommisjonsforordning (EU) 2024/2956 gir utfyllende regler til kravet i DORA om at foretakene må føre et register over alle IKT-tjenesteavtaler. Foretakene skal årlig rapportere registeret til Finanstilsynet ettersom det skal inngå som en del av grunnlaget for å peke ut kritiske IKT-tjenesteleverandører i EU/EØS. Første innrapportering for Norge skal skje i begynnelsen av 2026. Finanstilsynet skal rapportere registrene videre til de europeiske finanstilsynsmyndighetene innen 31. mars 2026. På bakgrunn av kravet om rapportering av register bør foretakene gjennomføre testrapportering for å se at deres registre er utfylt i samsvar med kravene og at innrapporteringen fungerer etter sin hensikt. På denne måten vil man kunne avdekke eventuelle feil og andre utfordringer hos foretakene før rapporteringen skal gjennomføres i begynnelsen av 2026. Foretakene bør derfor ha registrene på plass i god tid før første rapportering. En førtidig implementering av kommisjonsforordningen vil bidra til dette.

De nærmere angitte kravene til innholdet i registre over IKT-tjenesteavtaler som følger av kommisjonsforordningen skal sikre at informasjonen i foretakenes registre er komplett og

tydelig. På bakgrunn av reglenes karakter, bør kommisjonsforordningen tre i kraft samtidig som DORA-loven. Rettsaktens krav til registerets format bidrar i tillegg til forutsigbarhet for næringen, til effektiv bruk av informasjonen i Finanstilsynets tilsynsarbeid og ved videre rapportering til de europeiske finanstilsynsmyndighetene.

Finanstilsynet vil fremholde at det har blitt avholdt flere seminarer og andre informasjonstiltak overfor næringen, blant annet om rapportering av hendelser og register over IKT-tjenesteavtaler. Det er derfor grunn til å tro at foretakene vil kunne håndtere en førtidig implementering av de nevnte kommisjonsforordningene.

### 4.4 Oppsummering

Basert på vurderingene i delkapittel 4.2 og 4.3 mener Finanstilsynet det er viktig at samtlige av kommisjonsforordningene vil gjelde som forskrift når DORA-loven trer i kraft på grunn av deres innhold, selv om tre av forordningene foreløpig ikke er inntatt i EØS-avtalen og vil medføre en førtidig implementering.

## 5. Økonomiske og administrative konsekvenser

### 5.1 Innledning

Kommisjonsforordningene som inngår i DORA-regelverket og som foreslås innlemmet i forskrifter stiller mer detaljerte krav til foretakene sett opp mot krav etter dagens regelverk. Foretakene må derfor påregne noe innsats i overgangen til nytt regelverk der deler av innsatsen vil være knyttet til foretakenes tilpasninger til det mer detaljerte regelverket i forordningene. Graden av innsats og de økonomiske og administrative konsekvenser som følger av denne antas imidlertid å variere etter hvordan foretakene etterlever dagens regelverk.

EØS-avtalen innebærer at Norge har plikt til å gjennomføre de delegerte kommisjonsforordningene når de er innlemmet i EØS-avtalen. Det er derfor ikke grunnlag for å vurdere alternative løsninger.

### 5.2 Konsekvenser for foretakene i finanssektoren

*5.2.1 Innledning*

Krav etter IKT-forskriften og annet sektorregelverk tilsvarer langt på vei kravene som følger av DORA-regelverket. De delegerte kommisjonsforordningene vil innebære at kravene til foretakene i finanssektoren styrkes, selv om dagens norske regelverk og tilsynsmessige oppfølging bygger på de samme prinsippene som de nye kravene. I den grad de nye kravene fører til bedre styring og lavere risiko for skadelige IKT-hendelser, kan det gi besparelser for foretakene. Lovproposisjonen til DORA-loven peker på at tilpasning til nye sikkerhetskrav mv. isolert sett vil innebære lavere kostnader og gevinster sammenlignet med foretak i land som har hatt et mindre utviklet regelverk.

*5.2.2 Hendelseshåndtering*

De delegerte kommisjonsforordningene (EU) 2024/1772, (EU) 2025/301 og (EU) 2025/302 om hendelseshåndtering medfører at foretakene må innrette sine prosedyrer og rapportering til Finanstilsynet i samsvar med de mer detaljerte kravene. Selv om kommisjonsforordningene gir en mer konkret spesifikasjon av klassifisering av hendelser og krav til et standard format på rapporteringen, er Finanstilsynets vurdering at foretakene i hovedtrekk er underlagt tilsvarende krav etter dagens regelverk.

*5.2.3 Avtaler om bruk av IKT-tjenester*

Kravene som følger av kommisjonsforordning (EU) 2024/1773 om retningslinjer ved bruk av tredjepartstilbydere av IKT-tjenester som støtter kritiske og viktige funksjoner kan innebære at foretakene må gjøre endringer i sine leverandøravtaler. Dette kan gi foretakene økte kostnader. Foretakene må også følge opp og oppdatere eksisterende retningslinjer knyttet til avtaler om bruk av IKT-tjenester som nevnt ovenfor.

*5.2.4 Risikostyring*

Kravene til styring av IKT-risiko i kommisjonsforordning (EU) 2024/1774 utdyper kravene i DORA og inneholder regler som skal styrke foretakenes oppfølging av IKT-risiko. Foretakene må innrette sine risikostyringsrammeverk for IKT og oppdatere sine prosesser, prosedyrer, rutiner og rapportering i samsvar med de nye kravene, som i hovedtrekk er mer omfattende og detaljerte enn de som stilles i eksisterende sektorregelverket.

Med bakgrunn i prinsippet om proporsjonalitet, stiller rettsakten egne krav til mindre foretak som nevnt i artikkel 16 nr. 1 i DORA. Disse kvalifiserer til å ha et forenklet IKT-risikostyringsrammeverk.

Sammenholdt med eksisterende sektorregelverk og retningslinjer utarbeidet av de europeiske finanstilsynsmyndighetene vil de samlede kravene til styring av IKT-risiko i DORA og (EU) 2024/1774 hovedsakelig være på samme nivå. Endringene antas derfor ikke bli betydelig selv om (EU) 2024/1774 stiller absolutte krav, i motsetning til retningslinjer fra de europeiske finanstilsynsmyndigheter i dagens regelverk. Noen krav vil likevel være nye og medføre et behov for å endre på eksisterende rutiner, systemer mv., samt behov for å lære opp personell slik at de nye kravene etterleves.

*5.2.5 Register over IKT-tjenesteavtaler*

Når det gjelder registerføring av IKT-tjenesteavtaler, vil kravene i (EU) 2024/2956 innebære at foretakene må endre eksisterende og/eller etablere nye registre i samsvar med de mer detaljerte kravene i kommisjonsforordningen. Bestemmelsene innebærer også at registrene må oppdateres i henhold til kravene for alle foretakets IKT-tjenesteavtaler. Kravene til registerføring er mer omfattende enn dagens krav for slike avtaler, samt at kravene også omfatter nye avtaletyper.

### 5.3 Konsekvenser for IKT-leverandører

Leverandører av IKT-tjenester til foretak i finanssektoren må forholde seg til de mer omfattende kravene som stilles til foretakenes bruk av IKT-leverandører i DORA-regelverket, bl.a. krav til oppfølging og innholdet i avtaler, samt oversikt over informasjon som skal inngå i foretakenes register over IKT-tjenesteavtaler. Dette antas likevel ikke å ha større økonomiske eller administrative konsekvenser for IKT-leverandørene, jf. dagens krav i IKT-forskriften.

### 5.4 Konsekvenser for kunder og norsk økonomi

DORA-forordningen skal bidra til å redusere sannsynligheten for skadelige IKT-hendelser i den europeiske finanssektoren. De delegerte kommisjonsforordningene gir nærmere regler om blant annet styring av IKT-risiko, der formålet er å redusere sannsynligheten for hendelser og konsekvensene dersom hendelser oppstår. Det kan gi grunnlag for økt trygghet og tillit til finanssektoren også i Norge, selv om den finansielle infrastrukturen i Norge vurderes som robust. Siden IKT-hendelser som forstyrrer betalingsformidlingen eller ødelegger finansielle data kan ha store samfunnsøkonomiske kostnader, kan selv små forbedringer i sikkerhet og beredskap ha stor betydning for foretakenes kunder og økonomien som helhet. Norske foretaks tilpasning til det nye regelverket antas ikke å ha vesentlig betydning for prisingen av finansielle tjenester.

### 5.5 Konsekvenser for myndigheter

Når det gjelder økonomiske og administrative konsekvenser på myndighetssiden, antas det at de detaljerte kravene som følger av kommisjonsforordningene vil medføre mindre eller moderate konsekvenser. De nye kravene til å motta og lagre hendelsesrapportering og registerrapportering fra foretakene og videresende disse til de europeiske finanstilsynsmyndighetene vil blant annet kreve utvikling av tekniske løsninger som muliggjør dette, samt et behov for oppdatering og opplæring av ansatte i Finanstilsynet i nye rutiner.

## 6. Utkast til forskrift

**Forskrift om digital operasjonell motstandsdyktighet i finanssektoren (DORA-forskriften)**

Hjemmel: Lov 00. måned 2025 nr.00 om digital operasjonell motstandsdyktighet i finanssektoren § 1 tredje ledd

**§ 1 Formål**

Denne forskriften gir utfyllende bestemmelser til lov 00. måned 2025 nr.00 om digital operasjonell motstandsdyktighet i finanssektoren (DORA-loven).

**§ 2 Virkeområde**

Forskriften gjelder for foretak som er omfattet av DORA-loven § 1.

**§ 3 Utfyllende regelverk etter DORA-forordningen**

Følgende kommisjonsforordninger gjelder som forskrift så langt det passer:

a. EØS-avtalen vedlegg IX nr. 31qa (delegert kommisjonsforordning (EU) 2024/1772 om tekniske reguleringsstandarder med utfyllende regler til europaparlamentets- og rådsforordning (EU) 2022/2554 om digital operasjonell motstandsdyktighet i finanssektoren) gjelder som forskrift med de tilpasninger som følger av vedlegg IX, protokoll 1 til avtalen og avtalen for øvrig,
b. EØS-avtalen vedlegg IX nr. 31qb (delegert kommisjonsforordning (EU) 2024/1773 om tekniske reguleringsstandarder med utfyllende regler til europaparlamentets- og rådsforordning (EU) 2022/2554 om digital operasjonell motstandsdyktighet i finanssektoren) gjelder som forskrift med de tilpasninger som følger av vedlegg IX, protokoll 1 til avtalen og avtalen for øvrig,
c. EØS-avtalen vedlegg IX nr. 31qc (delegert kommisjonsforordning (EU) 2024/1774 om tekniske reguleringsstandarder med utfyllende regler til europaparlamentets- og rådsforordning (EU) 2022/2554 om digital operasjonell motstandsdyktighet i finanssektoren) gjelder som forskrift med de tilpasninger som følger av vedlegg IX, protokoll 1 til avtalen og avtalen for øvrig,
d. (EU) 2024/2956,
e. (EU) 2025/301 og
f. (EU) 2025/302.

**§ 4 Ikrafttredelse**

Forskriften trer i kraft fra den tid departementet bestemmer.