FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Høringsnotat

Forslag til endringer i DORA-forskriften, finansforetaksforskriften og forskrift om systemer for betalingstjenester

29. oktober 2025

1. Innledning og bakgrunn for høringsnotatet

1.1. Innledning

Finanstilsynet mottok brev fra Finansdepartementet 7. mars 2025 med oppdrag om å utrede behovet for utfyllende regler til DORA-loven. Oppdraget var todelt, hvor den første delen omhandlet vurderingen av regler som burde fastsettes samtidig som DORA-loven trådte i kraft, mens den andre delen omhandlet vurderingen av hvilke regler som kunne tre i kraft senere. Del en hadde frist i april 2025 og del to har frist medio oktober 2025. Videre ba departementet om at Finanstilsynet tok med seg høringsinnspillene til første runde med forskriftsregler i arbeidet med å vurdere ytterligere forskriftsregler, jf. brev av 13. juni 2025. Finanstilsynet oversendte forslag til høringsnotat 7. april 2025 til departementet med utkast til forskrift. Forskrift 24. juni 2025 nr. 1296 om digital operasjonell motstandsdyktighet i finanssektoren (DORA-forskriften) trådte i kraft 1. juli 2025. Dette høringsnotatet omhandler del to av Finansdepartementets oppdrag.

Ved utarbeidelsen av dette høringsnotatet har Finanstilsynet lagt vekt på å ivareta formålet med reguleringen uten å påføre finansnæringen unødige kostnader. I både Norge og EU arbeides det med å fjerne unødvendig regulering og å redusere næringslivets kostnader til etterlevelse av regler. I 2021 vedtok Stortinget å fastsette et mål om å redusere næringslivets administrative kostnader blant annet knyttet til pålagte regler.[1] Nærings- og fiskeri-departementet publiserte i august 2025 en rapport om forenklingsarbeidet for næringslivet.[2] I rapporten viser departementet til at forenklingstiltak må veies opp mot behovet for kontroll, og at forenklingsarbeidet ikke ensidig kan bestå i å redusere antall regler, men å sikre at reguleringskrav ivaretar samfunnets behov og samtidig påfører næringslivet minst mulig administrativ byrde. I EU bygger arbeidet blant annet på Draghi-rapporten om EUs konkurransekraft, som ble lagt fram i 2024.[3]

I punkt 1.2 til 1.5 gir Finanstilsynet informasjon om bakgrunnen for høringsnotatet. Finanstilsynets vurderinger av forslaget til forskriftsendring framgår av punkt 2. De økonomiske og administrative konsekvensene som følge av Finanstilsynets forslag til regelendringer er omtalt i punkt 3. Som vedlegg til høringsnotatet følger utkast til lov om endring i DORA-loven og forskrift om endringer i DORA-forskriften mv.

1.2. Regulering av IKT i finanssektoren

DORA-loven og DORA-forskriften trådte i kraft 1. juli 2025. DORA-loven implementerer forordning (EU) 2022/2554 om digital motstandsdyktighet i finanssektoren (heretter DORA). Forordningen regulerer foretakenes krav til virksomhetsstyring, risikostyring, hendelseshåndtering, testing og styring av tredjepartsrisiko m.m. Frem til DORA-loven trådte i kraft, var IKT-virksomhet i finanssektoren hovedsakelig regulert gjennom IKT-forskriften. IKT-forskriften og DORA regulerer tilnærmet det samme. IKT-forskriften er imidlertid mer prinsippbasert, mens DORA er svært detaljert og inneholder mange krav.

Fra samme tidspunkt som DORA-loven trådte i kraft, ble foretak som nevnt i DORA artikkel 2 nr. 3 tatt ut av IKT-forskriften. I dag gjelder IKT-forskriften for finansieringsforetak, inkassoforetak og eiendomsmeglerforetak. Finanstilsynet får tilsynsansvar for Norsk naturskadepool fra 1. januar 2026. I den forbindelse er det foreslått at poolen skal underlegges IKT-forskriften. I tillegg skal gjeldsinformasjonsforetak og kredittopplysningsforetak etterleve IKT-forskriftens regler, jf. gjeldsinformasjonsforksriften[4] § 8. For nærmere omtale av

[1] Innst. 565 S (2020–2021)

[2] Nærings- og fiskeridepartementets rapport: Forenklingsarbeidet for næringslivet

[3] Kommisjonens nettside om Drahgi-rapporten

[4] Forskrift 31. oktober 2017 nr. 1691 om virksomhet etter gjeldsinformasjonsloven (gjeldsinformasjonsforskriften)

gjeldsinformasjonsforetak og kredittopplysningsforetak, se punkt 2.1 og 2.2.1. Foretak som nevnt i DORA artikkel 2 nr. 3 har ikke lenger lovpålagte krav for IKT. Deres IKT-virksomhet må derfor vurderes som en del av de generelle kravene til styring og kontroll i regelverk som for eksempel finansforetaksloven og risikostyringsforskriften. Låneformidlerforetak og morselskap i finanskonsern har hittil ikke hatt lovpålagte krav til IKT-virksomhet.

I Finanstilsynets risiko- og sårbarhetsanalyse 2025 ble trusselen mot den finansielle sektoren vurdert som høy.[5] Det vises både til geopolitisk uro og en stadig mer avansert form for digital kriminalitet. Trusselbildet tilsier at det er viktig for foretakene å ha god styring av og kontroll med IKT-virksomheten. Konsekvensene av et digitalt angrep kan bli store, både for foretaket selv, kunder og forbrukere. Det foreligger derfor gode grunner til at foretak i finanssektoren har krav eller forventninger til IKT-virksomheten. Samtidig må reguleringen være effektiv, slik at den regulatoriske byrden ikke blir unødvendig stor.

1.3. DORAs anvendelse på andre foretak

DORA-loven § 2 hjemler adgangen til at DORA helt eller delvis kan gjøres gjeldende for følgende foretak:

a. foretak nevnt i DORA-forordningen artikkel 2 nr. 3,
b. finansieringsforetak,
c. låneformidlingsforetak,
d. inkassoforetak,
e. eiendomsmeglerforetak og
f. morselskap i finanskonsern.

Finanstilsynet har vurdert behovet for å underlegge foretakene krav i DORA. Den nærmere vurderingen følger av punkt 2.2.

1.4. Trusselbasert penetrasjonstesting (TLPT)

Foretak som er omfattet av DORA, med unntak av foretak som er nevnt i artikkel 16 nr. 1 og mikroforetak, skal gjennomføre TLPT-testing minimum hvert tredje år, se forordningens artikkel 26. Tilsynsmyndigheten kan etter en nærmere vurdering beslutte å fravike testfrekvensen. Delegert kommisjonsforordning (EU) 2025/1190 artikkel 2 inneholder ytterligere krav for å peke ut foretak til testing, eller unnta foretak krav om testing etter en nærmere vurdering dersom et krav om testing vurderes som uforholdsmessig byrdefullt.

Norges Bank innga høringsuttalelse i forbindelse med høringen på DORA-forskriften. I høringsuttalelsen foreslo Norges Bank en fordeling av oppgaver og ansvar mellom Norges Bank og Finanstilsynet ved gjennomføring av trusselbasert penetrasjonstesting (TLPT) etter DORA, og at dette fastsettes i forskrift. Blant annet viste banken til ansvaret for utpeking av foretak og testfrekvens, godkjenning av funksjoner og omfang av testingen, oppgaver knyttet til gjennomføringen av tester, oppfølging av funn og muligheten for å ilegge testobjektet avgift. Finanstilsynets vurdering framgår av punkt 2.2.

1.5. Endringer i andre forskrifter

Forskrift 15. februar 2019 nr. 152 om systemer for betalingstjenester bør tilpasses for å unngå dobbeltregulering med DORA. I tillegg har både forskrift om systemer for betalingstjenester og forskrift 9. september 2016 nr. 1502 om finansforetak og finanskonsern (finansforetaks-forskriften) henvisninger til IKT-forskriften. Henvisningene må rettes til å gjelde til DORA-forordningen. For nærmere detaljer, se punkt 2.3.

[5] Se Finanstilsynets Risiko- og sårbarhetsanalyse 2025, punkt 2.2

2. Finanstilsynets vurderinger

2.1. Vurdering om foretakene bør underlegges krav i DORA

2.1.1. Innledning

I dag er finansieringsforetak, eiendomsmeglerforetak og inkassoforetak underlagt IKT-forskriften. I tillegg er det foreslått at Norsk naturskadepool skal underlegges forskriftens virkeområde, se nærmere omtale i punkt 2.1.2. Videre skal gjeldsinformasjonsforetak og kredittopplysningsforetak etterleve IKT-forskriften ifølge gjeldsinformasjonsforskriften § 8. IKT-forskriften gjaldt tidligere for foretak som er unntatt DORA i henhold til forordningens artikkel 2 nr. 3, men ble tatt ut av forskriftens virkeområde da DORA-loven trådte i kraft 1. juli 2025. Finanstilsynet vurderte at en eventuell underleggelse av krav i DORA for foretak som nevnt i forordningens artikkel 2 nr. 3 ikke var avgjørende å få på plass til ikrafttredelsen av DORA-loven, og valgte derfor å behandle tematikken i del to av Finansdepartementets forskriftsoppdrag.

Fra 1. januar 2026 får Finanstilsynet tilsynsansvaret med Norsk naturskadepool, se lov 20. juni 2025 nr. 78 om endringar i naturskadeforsikringslova m.m. (ansvarsgrense og tilsyn med Norsk naturskadepool). I høringsnotat om ny naturskadeforsikringslov av 24. juni 2024[6] foreslo Justis- og beredskapsdepartementet at Norsk naturskadepool skulle underlegges risikostyringsforskriften og IKT-forskriften. Norsk naturskadepool har ikke hatt innvendinger mot å underlegges IKT-forskriften, jf. deres høringssvar av 24. september 2024.[7]

Gjeldsinformasjonsforetak og kredittopplysningsforetak skal etterleve IKT-forskriftens regler, jf. gjeldsinformasjonsforskriften § 8. I høringsbrevet til høringen av DORA-loven ga Finansdepartementet uttrykk for at en innføring av DORA ville kunne kreve tilpasninger i gjeldsinformasjonsforskriften.[8] I forbindelse med utredningen av ny finanstilsynslov uttalte Finanstilsynslovutvalget at Finanstilsynet ikke lenger bør ha tilsyn med gjeldsinformasjons-foretak.[9] I proposisjonen til ny finanstilsynslov foreslo Finansdepartementet at tilsyn med gjeldsinformasjonsforetak overføres til Datatilsynet, se Prop. 75 L (2023-2024) punkt 4.1.4. Videre viste Finansdepartementet til at Barne- og familiedepartementet har ansvaret for gjeldsinformasjonsloven og burde være ansvarlig for å følge opp eventuelle endringer. I høring av 3. april 2025 om forslag til endringer i gjeldsinformasjonsloven og gjeldsinformasjonsforskriften uttrykte Barne- og familiedepartementet tvil om det var riktig å overføre tilsynsansvaret til Datatilsynet og ba om høringsinstansenes syn.[10] Dersom Finanstilsynet ikke skal ha tilsynsansvar for gjeldsinformasjonsforetak er det heller ikke naturlig at foretakene er underlagt finansregulatorisk regelverk.

Låneformidlingsforetak og morselskap i finanskonsern har ikke hatt krav til IKT-virksomheten tidligere. Basert på høringssvar i forbindelse med høring av DORA-loven uttalte Finansdepartementet i lovproposisjonen at nasjonale regler kan være aktuelt for låneformidlingsforetak og morselskap i finanskonsern, se Prop. 54 LS (2024–2025) punkt 2.5.3.3.

DORA-loven § 2 hjemler adgangen til å underlegge foretakene omtalt i dette punktet krav i DORA helt eller delvis, med unntak av Norsk naturskadepool, gjeldsinformasjonsforetak og kredittopplysningsforetak.

[6] Se Justis- og beredskapsdepartementets høringsnotat, punkt 5

[7] Norsk naturskadepools høringssvar

[8] Finansdepartementets høringsnotat til DORA-loven, punkt 4.2.2

[9] Se NOU 2023: 6 om utredning til ny lov om Finanstilsynet, punkt 13.1.3.7

[10] Forslag om endringer i gjeldsinformasjonsloven og gjeldsinformasjonsforskriften, punkt 13

Spørsmålet er om IKT-forskriften skal bestå side om side med DORA. For foretakene kan det oppstå utfordringer hvis de to regelverkene skal leve side om side. I praksis har det allerede oppstått spørsmål fra næringen der foretak har flere konsesjoner, hvor en er underlagt DORA, men den andre ikke. For eksempel har det vært tvil om hvilket regelverk slike foretak skal melde IKT- avtaler etter. Finanstilsynet mener at foretak med flere konsesjonstyper bør ha like krav til IKT uavhengig av konsesjon, slik at det ikke oppstår tvil om hva som gjelder. Et annet eksempel er der foretak som er underlagt DORA, men er tatt ut av virkeområdet til IKT-forskriften, har rapportert en IKT-hendelse i henhold til IKT-forskriften, siden hendelsen ikke ble ansett som rapporteringspliktig etter DORA grunnet alvorlighetsgrad.

Som følge av regelverkenes likhet kan den tilsynsmessige oppfølgingen av IKT i finanssektoren bli krevende. Det vil bli vanskelig for Finanstilsynet å skille praksis i de to regelverkene, noe Finanstilsynet for eksempel har erfart i forbindelse med melding av IKT-tjenesteavtaler versus IKT-utkontrakteringer. Det kan også vanskeliggjøre en helhetlig tilnærming til tilsyn på IKT-området og krever et todelt IKT-tilsynsrammeverk. For Finanstilsynet vil det være en forenkling å forvalte ett regelverk i stedet for to. Kommunikasjon med og informasjon til næringen blir i tillegg enklere, siden to regelverk vil kreve at veiledning og informasjon til foretakene må tilpasses til regelverket foretakene er underlagt. Dersom foretakene skal etterleve to forskjellige sett av regler, medfører det at veiledning vil være mer ressurskrevende for Finanstilsynet enn om alle er underlagt samme regelverk.

I tillegg til spørsmålet om IKT-forskriften skal bestå er det spørsmål om foretakene som er nevnt i DORA-loven § 2 skal underlegges krav i DORA helt eller delvis. Dersom IKT-forskriften oppheves, blir også spørsmålet hvordan IKT-virksomheten hos Norsk naturskadepool, gjeldsinformasjonsforetak og kredittopplysningsforetak skal reguleres.

2.1.2. Foretak som etterlever IKT-forskriften

2.1.2.1 Generelt

Finansieringsforetak, eiendomsmeglerforetak og inkassoforetak er i dag underlagt IKT-forskriften. Foretakene har vært underlagt forskriften siden den kom i 2003 og kravene etter forskriften tilsvarer langt på vei kravene etter DORA, se også Prop. 54 LS (2024–2025) punkt 2.5.3.3. Som eksempler kan det vises til krav til virksomhetsstyring, hendelsesrapportering (med unntak av eiendomsmeglerforetak) og IKT-tjenesteavtaler. Norsk naturskadepool har ikke tidligere hatt krav til IKT, men er foreslått inntatt i IKT-forskriftens virkeområde. Gjeldsinformasjonsforetak og kredittopplysningsforetak har hatt krav om å etterleve IKT-forskriften siden gjeldsinformasjonsforskriften trådte i kraft i 2017.

DORA er et omfangsrikt og detaljert regelverk sammenlignet med IKT-forskriften. Forordningen inneholder krav til virksomhetsstyring, rammeverk for risikostyring, testing, hendelsesrapportering, tredjepartsrisikostyring og IKT-tjenesteavtaler. Det gjøres oppmerksom på at IKT-tjenesteavtaler i DORA er et videre begrep en IKT-utkontrakteringer i IKT-forskriften, se definisjonen av IKT-tjeneste i DORA artikkel 3 nr. 21. IKT-forskriften er overordnet og prinsippbasert, mens DORA inneholder en rekke krav foretakene må forholde seg til. Finansieringsforetak, eiendomsmeglerforetak og inkassoforetak varierer alle i størrelse. Hvordan foretakene eventuelt skal underlegges krav i DORA kan tilpasses. Det vises også til at DORA inneholder en egen proporsjonalitetsbestemmelse i forordningens artikkel 4. Selv om DORA er et mer detaljert regelverk å forholde seg, kan kravene i stor grad innfortolkes i IKT-forskriften. En underleggelse av krav i DORA vil medføre at foretakene i større grad vil få kjennskap til hva som forventes av dem, noe som kan bidra til større grad av forutsigbarhet. Alternativet er at foretakene må tilegne seg denne kunnskapen ved for eksempel å lese tilsynsrapporter. Finanstilsynet har ikke til hensikt å endre rettstilstanden vesentlig.

Finanstilsynet anser det som aktuelt å underlegge foretakene regler om virksomhetsstyring, rammeverk for risikostyring, testing, hendelsesrapportering, tredjepartsrisikostyring og IKT-tjenesteavtaler. Det er imidlertid ikke hensiktsmessig eller praktisk å la hele forordningen

komme til anvendelse. En underleggelse av krav i DORA kan også kreve tilpasning til den enkelte konsesjonstype og på foretaksnivå.

Finanstilsynet vurderer at gjeldsinformasjonsforetak og kredittopplysningsforetak ikke bør underlegges DORA. Den nærmere begrunnelsen framgår av punkt 2.1.2.3.

2.1.2.2 Overordnet om foretakene

Finansieringsforetak

Et finansieringsforetak kan drive følgende virksomhet, jf. finansforetaksloven § 2-9, første ledd:

a. leasing, factoring og annen finansieringsvirksomhet,
b. forretninger for foretakets eller kunders regning i penge- eller valutamarkedet,
c. omsetning av valuta eller andre særlige tjenester.

Finansieringsforetak kan i tillegg gis konsesjon som e-pengeforetak, betalingsforetak eller opplysningsfullmektig dersom visse vilkår er oppfylt, jf. finansforetaksloven § 2-9 annet ledd.

I Norge hadde 26 foretak konsesjon som finansieringsforetak per september 2025. Foretakene varierer i størrelse og kompleksitet. Det finnes eksempler på foretak som i tillegg til konsesjon som finansieringsforetak har konsesjon som e-pengeforetak eller betalingsforetak. Finansieringsforetakene har mye til felles med både kredittinstitusjoner og betalingsforetak, som begge er konsesjonstyper som er underlagt DORA.

Eiendomsmeglerforetak

I 2024 ble det solgt ca. 186 000 boliger i Norge for til sammen ca. 595 milliarder kroner.[11] Foretakene forvalter dermed et betydelig beløp. Per september 2025 hadde 496 eiendomsmeglingsforetak konsesjon.

Inkassoforetak

I Norge hadde 66 foretak konsesjon som inkassoforetak, hvorav 60 er fremmedinkassoforetak og 6 oppkjøps-/egeninkassoforetak per september 2025.

Norsk naturskadepool

Norske forsikringsselskaper som yter erstatning for naturskader i henhold til naturskadeforsikringsloven[12] § 1, skal være medlemmer av Norsk naturskadepool. Naturskadepoolen er bindeleddet mellom Statens naturskadefond og den norske forsikringsbransjen. Forsikringsselskapene er forsikringsgiver og foretar oppgjør overfor sine kunder. Naturskadepoolen utlikner på sin side naturskadeerstatninger mellom forsikringsselskapene for skader som er definert i naturskadeloven.

Gjeldsinformasjonsforetak

Tre foretak har i dag konsesjon som gjeldsinformasjonsforetak. Foretak med konsesjon har tillatelse til å motta, innhente, registrere og utlevere gjeldsopplysninger, jf. gjeldsinformasjonsloven[13] § 1 bokstav a).

[11] Tall fra Statistisk sentralbyrå

[12] Lov 16. juni 1989 nr. 70 om naturskadeforsikring (naturskadeforsikringsloven)

[13] Lov 16. juni 2017 om gjeldsinformasjon ved kredittvurdering av privatpersoner (gjeldsinformasjonsloven)

Kredittopplysningsforetak

I 2025 er det fem foretak som kredittvurderer både privatpersoner og virksomheter samt ytterligere fire foretak som kun kredittvurderer virksomheter[14]. Kredittopplysningsforetakene utfører blant annet kredittsjekker og må etterleve krav til behandling av kredittopplysninger etter kredittopplysningsloven[15] og kredittopplysningsforskriften[16]. Foretakene er i dag underlagt tilsyn fra Datatilsynet.

2.1.2.3 Spesielt om gjeldsinformasjonsforetak og kredittopplysningsforetak

Når det gjelder gjeldsinformasjonsforetak og kredittopplysningsforetakene vurderer Finanstilsynet at en underleggelse av krav i DORA vil være uforholdsmessig byrdefullt. Det vises til fokuset på forenklinger for foretak i næringslivet og at foretakene fortsatt vil ha krav til å sikre nødvendig konfidensialitet, integritet og tilgjengelighet for deres tjenester etter gjeldsinformasjonsloven, jf. gjeldsinformasjonsforskriften § 8. Ifølge bestemmelsen er foretakene også pålagt å følge nasjonale standarder og internasjonalt anerkjente standarder. For kredittopplysningsforetakene vises det i tillegg til at de er unntatt konsesjonsplikt. Det kan eventuelt stilles forventninger til foretakenes oppfølging av IKT-virksomheten i en veiledning. Finanstilsynet er noe usikker på behovet for veiledning i tillegg til gjeldsinformasjonsforskriften § 8.

2.1.2.4 Definisjoner og proporsjonalitet

Definisjoner av begreper anvendt i DORA følger av forordningens artikkel 3. Videre inneholder DORA en egen bestemmelse om proporsjonalitet i artikkel 4. Finanstilsynet vurderer det som relevant å gjøre begge bestemmelser gjeldende for foretak som foreslås underlagt regler i DORA, siden bestemmelsene gjelder den praktiske anvendelsen av regelverket.

2.1.2.5 Virksomhetsstyring

Krav til organisering av IKT-virksomheten framgår av IKT-forskriften § 2. Bestemmelsen inneholder krav til fastsettelse av overordnede formål, strategier og sikkerhetskrav. Videre skal det foreligge en beskrivelse av ansvaret for administrasjon, anskaffelse, utvikling, drift, systemvedlikehold, sikring av informasjon og at avvikling utføres på en betryggende måte. Foretaket skal ha retningslinjer for utkontraktering og det skal oppnevnes ansvarlige, det vil si en funksjon eller stilling, for de enkelte delene av IKT-virksomheten. I tillegg stilles det krav til styrets behandling av utkontrakteringer. Utover dette må krav til styring og kontroll hos finansieringsforetak vurderes ut ifra reglene i finansforetaksloven og CRR/CRD-forskriften, mens kravene til styring og kontroll for eiendomsmeglerforetak og inkassoforetak må vurderes ut ifra risikostyringsforskriften. Samlet sett gir reglene få konkrete holdepunkter for krav til IKT-virksomheten. Foretakene kan imidlertid finne veiledning i publiserte tilsynsrapporter.

DORA artikkel 5 stiller krav til at foretaket skal ha et rammeverk for virksomhetsstyring, for å sikre en effektiv og forsvarlig håndtering av IKT-risiko. Det bemerkes at DORA bruker begrepet 'management body' (heretter ledelsesorganet), som vil si styret og daglig leder.[17] Videre regulerer bestemmelsen konkret hvilket ansvar styret og ledelsen har. På et overordnet nivå

[14] Datatilsynets oversikt over virksomheter som kredittvurderer

[15] Lov 20. desember 2019 nr. 109 om behandling av opplysninger i kredittopplysningsvirksomhet (kredittopplysningsloven)

[16] Forskrift 20. mai 2022 om behandlinger av opplysninger i kredittopplysningsvirksomhet (kredittopplysningsforskriften)

[17] Se Prop. 54 LS (2024–2025), punkt 2.5.4.3

tilsvarer ansvarsbeskrivelsene kravene i finansforetaksloven sammenholdt med CRR/CRD-forskriften og risikostyringsforskriften. DORA artikkel 5 er imidlertid mer IKT-spesifikk og regulerer konkrete forhold som det er nødvendig at er en del av foretakets styring av og kontroll med IKT-virksomheten. Bestemmelsen stiller blant annet krav til at ledelsesorganet skal sørge for at foretaket har retningslinjer som sikrer tilgjengelighet, autentisitet, integritet og konfidensialitet på et høyt nivå. Videre skal ledelsesorganet definere roller og ansvar for IKT-funksjoner, fastsette en strategi for digital operasjonell motstandsdyktighet, godkjenne foretakets IKT-kontinuitetsplan, godkjenne revisjonsplaner på IKT-området, godkjenne retningslinjene for IKT-tjenesteavtaler og etablere rapporteringslinjer for IKT-tjenesteavtaler.

Visse foretak er unntatt artikkel 5 og skal etterleve et forenklet rammeverk for risikostyring, se DORA artikkel 16 og notatets punkt 2.1.2.6. For foretakene som skal etterleve det forenklede rammeverket for risikostyring gjelder også forenklede regler for virksomhetsstyring. De forenklede reglene for virksomhetsstyring framgår av delegert kommisjonsforordning (EU) 2024/1774 artikkel 28. Ifølge bestemmelsen skal foretaket sikre at ledelsesorganet har det overordnede ansvaret for at rammeverket for risikostyring understøtter foretakets forretningsstrategi og risikoappetitt, samt at IKT-virksomheten vurderes som en del av dette. Ledelsesorganet skal fastsette klare roller og ansvarsområder, definere mål for informasjonssikkerhet og krav til IKT. Videre skal ledelsesorganet godkjenne, overvåke og jevnlig gjennomgå klassifisering av informasjon, identifiserte risikoer og beredskapsplaner. Ledelsesorganet skal også sikre tilstrekkelig budsjett og opplæring, implementere relevante retningslinjer og tiltak for å identifisere, vurdere og håndtere IKT-risiko, beskytte IKT- og informasjonsaktiva, ivareta kompetanseutvikling blant ansatte og etablere hensiktsmessige rapporteringsrutiner for informasjonssikkerhet og digital operasjonell motstandsdyktighet.

Ledelsesorganet har det overordnede ansvaret for IKT-virksomheten i foretaket. Finanstilsynet vurderer det derfor som grunnleggende at det stilles krav til ledelsesorganets oppfølging på området. Videre vurderer Finanstilsynet at en strategi danner grunnlaget for hvordan IKT-virksomheten skal drives. Ut ifra strategien må foretaket definere hvilke IKT-funksjoner og retningslinjer det er behov for. Tilsynspraksis har vist at foretakenes organisering på IKT-området ofte har mangler, blant annet i form av mangelfull kompetanse på IKT-risiko og manglende ressurser hos kontrollfunksjoner. Et tydeligere regelverk, der det framgår hva som kreves, kan bidra til å heve nivået hos foretakene. Finanstilsynet mener at foretakene bør underlegges krav til virksomhetsstyring. Om foretakene skal underlegges DORA artikkel 5 eller de forenklede kravene i (EU) 2024/1774 artikkel 28 avhenger av hvilket rammeverk for risikostyring foretaket skal etterleve, se punkt 2.1.2.6.

2.1.2.6 Rammeverk for risikostyring

Ifølge IKT-forskriften § 3 skal foretaket fastsette kriterier for risikoappetitt forbundet med IKT-systemene. Videre kreves det at foretakene skal ha en dokumentert prosess for gjennomføring av risikoanalyser, med definerte ansvarsforhold. Ansvarsforholdene skal omfatte oppfølgingen av tiltak som iverksettes som et resultat av gjennomførte risikoanalyser. Foretaket skal gjennomføre en risikovurdering minimum årlig og ved endringer som har betydning for IKT-systemene.

Et rammeverk for risikostyring gir foretaket en strukturert metode for å identifisere, vurdere, håndtere og overvåke risikoer. Rammeverket gir videre foretakets ledelse et grunnlag for å ta informerte og strategiske beslutninger. Hittil har Finanstilsynet også innfortolket forventninger til et slikt rammeverk i tilsynspraksisen, som en del av kravene til risikostyring i finansforetaksloven og CRR/CRD-forskriften for finansieringsforetak, og i risikostyrings-forskriften for eiendomsmeglerforetak og inkassoforetak.

DORA har to varianter av rammeverk for risikostyring. Det foreligger et fullt rammeverk (artikkel 5 til 15) og et forenklet (artikkel 16). Begge rammeverkene er ytterligere regulert i delegert kommisjonsforordning (EU) 2024/1774.

Formålet med rammeverket er å gjøre foretaket i stand til å ivareta og håndtere IKT-risiko samt å oppnå et høyt nivå av digital operasjonell motstandsdyktighet. På et overordnet nivå skal foretaket ha strategier, rutiner og retningslinjer for å ivareta IKT-virksomheten. Videre skal foretaket ha kontrollfunksjoner i tråd med de tre forsvarslinjer eller lignende og krav til internrevisjon. Det stilles også krav til foretakenes systemer. Rammeverket er hovedsakelig bygget på NIST-rammeverket[18], der foretaket skal identifisere IKT-risiko samt beskytte seg mot, avdekke, håndtere og gjenopprette driften ved en uønsket hendelse. For ytterligere informasjon, se Prop. 54 LS (2024–2025) punkt 2.4.2.2.

Formålet med det forenklede rammeverket er at foretaket skal oppnå en rask, effektiv og helhetlig håndtering av IKT-risiko. Rammeverket stiller krav til at foretaket skal overvåke sikkerheten og driften av IKT-systemene. Videre skal foretakene identifisere uregelmessigheter i driften og leverandøravhengigheter. Det stilles også krav til kontinuitet, herunder til kontinuitetsplan og oppdatering av denne. Rammeverket skal gjennomgås periodisk.

Finanstilsynet vurderer at alle foretak bør ha et rammeverk for å håndtere risiko. I en tid med geopolitisk uro og stadig mer sofistikerte digitale angrep, er det nødvendig å ha et bevisst forhold til foretakets risiko og hvordan foretaket håndterer den. Det digitale landskapet er stadig i utvikling og det introduseres stadig nye teknologier. Med nye teknologier kommer også nye sårbarheter. Derfor er det viktig at foretaket kontinuerlig følger med på risikoutviklingen og iverksetter risikoreduserende tiltak for å beskytte kunder, forbrukere og foretaket selv. Finanstilsynet mener derfor at finansieringsforetak, eiendomsmeglerforetak, inkassoforetak og Norsk naturskadepool bør underlegges regler om et rammeverk for risikostyring, som gjelder spesifikt for IKT-virksomheten.

For finansieringsforetak, eiendomsmeglerforetak og inkassoforetak vurderer Finanstilsynet at det er to alternativer for hvilket rammeverk for risikostyring foretakene bør underlegges:

Det første alternativet er at foretakene underlegges det fulle rammeverket. For de store foretakene behøver ikke det bli en stor omstilling, men det kan bli det for de mindre. Reglene inneholder flere absolutte krav til etterlevelse. Samtidig er reglene utformet for at foretakene skal kunne oppnå en høy grad av digital operasjonell motstandsdyktighet. Ettersom trusselen mot finanssektoren vurderes som høy, kan det tale for at mer kreves av foretakene for å beskytte seg mot eventuelle digitale angrep. Proporsjonalitetsbestemmelsen i DORA artikkel 4 medfører også at de mindre foretakene vil vurderes mindre strengt enn de større.

Det andre alternativet er at de største foretakene må etterleve det fulle rammeverket, mens mindre foretak må etterleve det forenklede. Hvilke foretak som skal etterleve hvilket rammeverk må i så fall avgjøres ut ifra en fastsatt terskel. Man kan for eksempel sette grensen ved foretak som er mellomstore eller større, se DORA artikkel 3 (64). Finanstilsynet er også åpen for at andre parametere kan legges til grunn. Det kan for eksempel være foretakenes midler på klientkonto i løpet av et år eller salgsinntekter. For inkassoforetak kan fordringsmasse til inndrivelse være en relevant parameter.

For finansieringsforetak er Finanstilsynets foreløpige vurdering at foretakene bør underlegges det fulle rammeverket for risikostyring. Det vises til at flere finansieringsforetak også har konsesjon som betalingsforetak, og at betalingsforetakene er underlagt det fulle rammeverket.

For eiendomsmeglerforetak og inkassoforetak er Finanstilsynets foreløpige vurdering at foretak som kvalifiserer til å være mellomstore eller større bør underlegges det fulle rammeverket for risikostyring. Det vises til at foretakenes størrelse kombinert med konsekvenser manglende håndtering av IKT i foretaket kan få for foretakenes kunder. **Finanstilsynet ønsker innspill på hvilke parametere som bør legges til grunn for å være omfattet av det fulle rammeverket versus det forenklede.**

[18] The NIST Cybersecurity Framework (CSF) 2.0

Finanstilsynet vurderer at Norsk naturskadepool bør underlegges det forenklede rammeverket for risikostyring. Det vises til foretakets kompleksitet og risiko og betydning for den finansielle stabiliteten. Videre vises det til at det ikke er vedtatt at Norsk naturskadepool skal etterleve kravene til virksomhetsstyring i Solvens II-regelverket, men er underlagt egne krav i naturskadeforsikringsforskriften kapittel 2.[19]

2.1.2.7 Hendelser

Finansieringsforetak og inkassoforetak er omfattet av plikten til å rapportere IKT-hendelser, jf. IKT-forskriften § 9. Eiendomsmeglerforetak er unntatt plikten. Finanstilsynet foreslår å videreføre plikten til å rapportere hendelser for finansieringsforetak og inkassoforetak. Videre foreslår Finanstilsynet å innføre plikt til å rapportere alvorlige IKT-hendelser som er relatert til oppgjørsfunksjonen hos eiendomsmeglerforetak.

Krav til håndtering og rapportering av hendelser følger av DORA kapittel 3, delegert kommisjonsforordning (EU) 2024/1772 om klassifisering av hendelser, delegert kommisjonsforordning (EU) 2025/301 om innhold og frister for rapportering av alvorlige IKT-hendelser og betydelige cybertrusler og kommisjonens gjennomføringsforordning (EU) 2025/302 om maler og prosedyrer for rapportering av alvorlige IKT- hendelser og frivillig rapportering av betydelige cybertrusler. Reglene for hendelsesrapportering etter DORA er mer omfattende og detaljerte enn i IKT-forskriften. Samtidig samsvarer kravene i DORA hovedsakelig med Finanstilsynets forventninger til vurderinger som må gjøres etter IKT-forskriften etter en oppstått hendelse.

Eiendomsmeglerforetak er unntatt krav til hendelsesrapportering etter IKT-forskriften § 9. I utgangspunktet finner Finanstilsynet det hensiktsmessig å videreføre unntaket, men mener at hendelser tilknyttet oppgjørsfunksjonen bør være rapporteringspliktige. I 2024 ble det solgt 186.000 boliger i Norge for til sammen ca. 595 milliarder kroner. Det tilsier et gjennomsnittlig oppgjør på 3,2 millioner kroner. Oppgjørsfunksjonen kan langt på vei sammenlignes med pengeoverføringer i et betalingsforetak. Pengene innhentes fra kjøper og utbetales til selger. Til forskjell fra eiendomsmeglerforetakene, har ikke betalingsforetakene adgang til å besitte eller råde over kundens midler, se finansavtaleloven § 4-17. Eiendomsmeglerforetak forvalter imidlertid klientmidler på klientkonto. Det er ofte tale om høye summer og konsekvensene for partene, eventuelt også banker med lånekrav, kan bli store ved en alvorlig IKT-hendelse.

Finanstilsynet vurderer det som viktig å få kjennskap til hendelser ved oppgjørsfunksjonen hos større eiendomsmeglerforetak ut ifra en risikobasert tilnærming. Videre kan det være hensiktsmessig at Finanstilsynet har kjennskap til hendelser, dersom hendelsen skulle få oppmerksomhet i media, slik at Finanstilsynet som ansvarlig myndighet er kjent med saken og sitter med førstehåndskunnskap. Finanstilsynet er ikke kjent med at slike hendelser har oppstått tidligere, men utelukker ikke at de kan oppstå. Finanstilsynet foreslår derfor at eiendomsmeglerforetak omfattes av plikten til å rapportere hendelser knyttet til oppgjørsfunksjon.

Finanstilsynet vurderer det som hensiktsmessig at Norsk naturskadepool får krav til å rapportere hendelser. Det vises til at poolen forvalter betydelige summer på vegne av forsikringsforetakene, og at en alvorlig IKT-hendelse kan medføre konsekvenser for flere foretak i forsikringssektoren. Det vises også til at Finanstilsynet som tilsynsmyndighet bør være kjent med slike hendelser.

Med tanke på dagens fokus på forenklinger av regelverksbyrde for foretak i finansnæringen, skal det i utgangspunktet være en høy terskel for å underlegge foretakene nye regelkrav. Selv om innføringen av en plikt til å rapportere hendelser kan medføre en administrativ og økonomisk byrde for foretakene som blir omfattet av plikten, vurderer Finanstilsynet at myndighetenes behov for kontroll må veie tyngre.

[19] Naturskadeforsikringsforskriften kapittel 2

2.1.2.8 Testing

IKT-forskriften § 6 stiller krav til at foretaket skal ha skriftlige prosedyrer for testing av IKT-systemer og at den ansvarlige i foretaket skal godkjenne før et system settes i produksjon.

DORA artikkel 24 stiller krav til at foretak, utenom mikroforetak,[20] skal ha et program for å teste den digitale operasjonelle motstandsdyktigheten. I artikkel 25 stilles det krav til selve testingen. Artikkel 26 stiller krav til trusselbasert penetrasjonstesting (TLPT), som er en mer avansert testform.

Finanstilsynet vurderer at krav til IKT-testing bør videreføres og at reglene i DORA i hovedsak kodifiserer nåværende tilsynspraksis. Finanstilsynet anser det ikke som nødvendig å underlegge foretakene krav til å gjennomføre TLPT-testing. Det vises til at et slikt krav vil medføre en uforholdsmessig stor byrde for foretakene og at det anses som tilstrekkelig at foretakene er underlagt de generelle kravene til testing i artikkel 24 og 25.

2.1.2.9 Styring av IKT-tredjepartsrisiko

IKT-forskriften § 2 annet ledd stiller krav til at foretaket skal ha retningslinjer for utkontraktering av IKT-virksomhet. Retningslinjene skal oppfylle kravene i forskriftens § 12. Videre stilles det krav til foretakets behandling av utkontrakteringsavtalen i forskriftens § 2 fjerde ledd. IKT-forskriften § 12 regulerer foretakets plikter ved utkontraktering og presiserer at foretaket står ansvarlig selv om IKT-virksomhet er utkontraktert. Foretaket skal påse at det foreligger en skriftlig avtale, at foretaket har tilsyns- og revisjonsrett, at foretaket kan revidere aktiviteter i tilknytning til avtalen, at avtalen sikrer håndtering av taushetsbelagt informasjon og at foretaket besitter tilstrekkelig kompetanse til å forvalte avtalen. Avtalen skal også sikre Finanstilsynets tilsyns- og innsynsrett.

DORA kapittel V del I regulerer styring av IKT-tredjepartsrisiko. Ifølge DORA artikkel 28 skal foretakene ha et rammeverk for styring av IKT-tredjepartsrisiko som en del av rammeverket for risikostyring. Bestemmelsen stiller også nærmere krav til innholdet i rammeverket. Det presiseres at foretaket til enhver tid er ansvarlig for etterlevelsen av DORA ved bruk av IKT-leverandører. Bestemmelsen angir videre krav til hvilke vurderinger som må gjøres i forkant av inngåelse av en IKT-tjenesteavtale og angir krav som være på plass for at en avtaleinngåelse kan finne sted. Foretakene skal rapportere IKT-tjenesteavtaler til tilsynsmyndigheten og skal ha et register over IKT-tjenesteavtaler, se egen omtale i henholdsvis punkt 2.1.2.10 og 2.1.2.11.

Foretaket skal gjennomføre en risikovurdering av avtaleforholdet i forkant av kontraktsinngåelse, se artikkel 29. Det stilles flere krav til forhold som skal vurderes som en del av risikovurderingen. I tillegg stilles det flere konkrete krav til klausuler som må være en del av avtalen i artikkel 30.

Bestemmelsene i artikkel 28 til 30 er nærmere utdypet i kommisjonens gjennomførings-forordninger (EU) 2024/1773 om retningslinjer for inngåelse av kritiske og viktige avtaler og i (EU) 2025/532 om bruk av underleverandører.

De fleste foretak benytter seg av IKT-leverandører i en eller annen grad. Noen foretak bruker IKT-leverandører til all IKT-virksomhet. Leverandørene benytter ofte underleverandører, som i noen tilfeller medfører lange leverandørkjeder og et komplekst leverandørbilde. Siden foretaket forblir ansvarlig, er det etter Finanstilsynets vurdering viktig at foretaket har god styring av og kontroll med av leverandørens aktiviteter, ved å gjøre risikovurderinger, inngå gode avtaler og å følge opp avtaleforholdet så lenge det varer. Reglene i DORA kapittel V del II legger til rette for at foretaket kan oppnå det.

[20] Se DORA artikkel 3 nr. 60

DORA kapittel V del II omhandler overvåkning av kritiske tredjepartstilbydere gjennom en egen overnasjonal myndighet. Overvåkningsmyndigheten er en av de europeiske finanstilsynsmyndighetene (EBA, ESMA eller EIOPA), eller EFTA, dersom det er tale om en kritisk tredjepartstilbyder fra et EFTA-land. For nærmere omtale av overvåkningsinstituttet, se Prop. 54 LS (2024–2025) punkt 2.4.2.6. Overvåkningsmyndigheten skal kontrollere aktiviteten til de utpekte kritiske tredjepartstilbydere og deretter utstede anbefalinger om forhold tredjepartstilbyderen bør rette. Overvåkningsmyndigheten kan ikke gi direkte pålegg, men tilsynsmyndigheten skal følge opp at foretakene tar anbefalingene i betraktning ved sin risikohåndtering og gjennom å følge opp leverandøren, se DORA artikkel 42. Siden overvåkningsinstituttet begrenser tilsynsmyndighetens kontroll og oppfølgning med leverandører direkte, vurderer Finanstilsynet at det er relevant å gjøre bestemmelsen gjeldende for foretakene.

2.1.2.10 Rapportering av IKT-tjenesteavtaler

Avtaler om utkontraktering skal meldes til Finanstilsynet minst 60 dager før iverksettelse, jf. finanstilsynsloven § 4-6. Kun kritiske og viktige avtaler skal meldes, jf. meldepliktforskriften § 3. Kravene til melding framgår av forskriftens § 4.

DORA artikkel 28 nr. 3 inneholder krav om minst årlig rapportering av antall nye inngåtte IKT-tjenesteavtaler m.m. Finanstilsynet vurderer det som unødvendig at foretakene er omfattet av en slik rapportering.

Finansieringsforetak og gjeldsinformasjonsforetak er i dag omfattet av krav til å melde IKT-avtaler i henhold til finanstilsynsloven § 4-6 jf. meldepliktforskriften § 3. Eiendoms-meglerforetak og inkassoforetak er unntatt meldeplikten, jf. meldepliktforskriften § 2 bokstav e og f. I og med at Finanstilsynet får tilsynsansvaret for Norsk naturskadepool fra og med 1. januar 2026, vil Norsk naturskadepool underlegges krav til å melde utkontrakteringer i medhold av finanstilsynsloven § 4-6 og meldepliktforskriften. Det er foreløpig ikke foreslått at Norsk naturskadepool skal unntas meldeplikten, jf. meldepliktforskriften § 2. Ifølge DORA artikkel 28 nr. 3 skal planlagte IKT-tjenesteavtaler som støtter kritiske eller viktige funksjoner meldes til tilsynsmyndigheten i rimelig tid. Det samme gjelder når en funksjon har blitt kritisk eller viktig. Bestemmelsen inneholder ikke formkrav til meldingen og angir ikke hva som skal regnes som rimelig tid. Finanstilsynet har derfor utarbeidet en egen veiledning om melding av IKT-tjenesteavtaler.[21] Som et resultat av innføringen av DORA ble kravet til melding om IKT-avtaler forenklet, slik at kravene ble like for foretak underlagt IKT-forskriften og foretak underlagt DORA. Kravet om at meldingen skulle inneholde avtalen med vedlegg, styremøteprotokoll og risikovurdering av avtalen ble fjernet fra meldepliktforskriften 1. juli 2025. 60-dagersfristen gjelder imidlertid fortsatt for finansieringsforetakene, jf. finanstilsynsloven § 4-6, mens for DORA-foretakene er fristen senket til 30 dager.

Finanstilsynet vurderer at meldeplikten bør videreføres for finansieringsforetak. Spørsmålet er om eiendomsmeglerforetak, inkassoforetak og Norsk naturskadepool også bør omfattes.

Når det gjelder eiendomsmeglerforetakene, mener Finanstilsynet at IKT-tjenesteavtaler som er relevante for oppgjørsfunksjonen bør være meldepliktige. Det vises til at 595 milliarder kroner gikk gjennom disse systemene i 2024. Det er en betydelig sum. At det er snakk som så store beløp tilsier at tilsynsmyndigheten bør ha anledning til å vurdere planlagte avtaleinngåelser som ledd i den tilsynsmessige oppfølgingen. Finanstilsynet antar at det ikke vil være tale om mange avtaler og en innføring av meldeplikt antas derfor ikke å bli spesielt byrdefull.

For inkassoforetakenes del mener Finanstilsynet at det også kan være hensiktsmessig å innføre meldeplikt for de største foretakene. Det vises til at 12 foretak har en samlet fordringsmasse til inndrivelse i milliardklassen per september 2025, hvorav fire har en samlet

[21] Finanstilsynets veiledning om melding av IKT-tjenesteavtaler

fordringsmasse på over 10 milliarder kroner. Det store omfanget tilsier at det bør innføres meldeplikt for disse foretakene som ledd i den tilsynsmessige oppfølgingen. Finanstilsynet er noe usikker på hvor grensen bør gå for hvilke inkassoforetak som skal omfattes av meldeplikten. Finanstilsynets foreløpige vurdering er å innføre meldeplikt for foretak som blir omfattet av det fulle rammeverket for risikostyring.

Finanstilsynet vurderer at Norsk naturskadepool bør omfattes av plikten til å melde IKT-tjenesteavtaler. Det vises til at poolen forvalter betydelige summer, noe som tilsier at det bør stilles krav til avtalene, men også at tilsynsmyndigheten bør ha anledning til å vurdere planlagte avtaleinngåelser som ledd i den tilsynsmessige oppfølgingen.

Med tanke på dagens fokus på forenklinger av regelverksbyrde for foretak i finansnæringen, skal det i utgangspunktet være en høy terskel for å underlegge foretakene nye krav. Selv om innføringen av meldeplikt for IKT-tjenesteavtaler vil medføre noe administrativ og økonomisk byrde for foretakene, vurderer Finanstilsynet at myndighetenes behov for kontroll må veie tyngre.

2.1.2.11 Register over IKT-tjenesteavtaler

Foretak som er underlagt IKT-forskriften plikter i dag å ha en samlet oversikt over avtaler om utkontraktering, se finanstilsynsloven § 4-6 tredje ledd jf. meldepliktforskriften § 1. IKT-tjenesteavtaler i henhold til DORA er ikke omfattet av finanstilsynsloven § 4-6, se bestemmelsens første ledd.

DORA artikkel 28 nr. 3 krever at foretaket skal ha et register på foretaksnivå samt konsolidert og sub-konsolidert nivå i konsern. Finanstilsynet vurderer at det er tilstrekkelig at foretakene kun har et register på foretaksnivå. Det foreslås derfor å gjøre unntak for kravet om register på konsolidert og sub-konsolidert nivå i konsern.

Kravene til registerføring er utdypet i Kommisjonens gjennomføringsforordning (EU) 2024/2956. Kravene er svært omfattende, og Finanstilsynet vurderer derfor at det vil være uforholdsmessig byrdefullt for foretakene å etterleve dem. Det er imidlertid viktig at foretakene har en fullstendig oversikt over leverandørene sine. Derfor bør det stilles krav til at foretakene skal ha et register, slik det følger av meldepliktforskriften § 1 i dag.

Finanstilsynet foreslår at foretakene ikke underlegges kravene til register i gjennomføringsforordning (EU) 2024/2956. Det bør imidlertid innføres egne regler om krav til register over IKT-tjenesteavtaler i DORA-forskriften, som følge av at IKT-tjenesteavtaler i henhold til DORA er unntatt i finanstilsynsloven § 4-6. Finanstilsynet vurderer det som tilstrekkelig å innføre krav til register som tilsvarer meldepliktforskriften § 4. Siden foretakene ikke er omfattet av DORAs virkeområde, kan Norge utforme egne krav på dette området. For nærmere detaljer, se § 11 i forskriftsutkastet.

2.1.2.12 Informasjonsdeling

DORA artikkel 45 gir foretakene adgang til å utveksle informasjon om cybertrusler m.m. NFCERT[22] er et eksempel på en slik informasjonsdelingsordning. I forbindelse med oppfølging av hendelser har Finanstilsynet flere ganger oppfordret foretak til å delta i slike informasjonsdelingsordninger. Foretakene får raskt tilgang på relevant informasjon, som kan gjøre dem bedre rustet til å følge opp sin egen IKT-virksomhet. Finanstilsynet anser det derfor som en fordel for foretakene å være omfattet av DORA artikkel 45.

2.1.2.13 Pålegg og overtredelsesgebyr

[22] NFCERTs hjemmeside

Finanstilsynet kan gi foretak pålegg om retting dersom et foretak ikke etterlever krav gitt i medhold av lov eller forskrift, se finanstilsynsloven § 4-1. Videre kan Finanstilsynet ilegge tvangsmulkt hvis et foretak ikke retter seg etter pålegg gitt i medhold av lov eller forskrift, jf. finanstilsynsloven § 4-3. DORA hjemler adgang til å gi pålegg om retting i artikkel 50. Bestemmelsen hjemler også adgang til å ilegge overtredelsesgebyr. DORA-loven § 4 angir hvilke bestemmelser i DORA Finanstilsynet kan ilegge overtredelsesgebyr ved manglende etterlevelse.

Tilgjengelighet, autentisitet, konfidensialitet og integritet til data er nødvendig for at tjenestene blir utført riktig. Noen av foretakene forvalter også store pengesummer og foretakenes drift er i hovedsak IKT-basert. Det digitale trusselnivået er høyt og det forekommer mange digitale angrep. Skulle en alvorlig feil oppstå i et system eller et foretak bli angrepet, kan det få store konsekvenser, spesielt for forbrukere, men også for bedriftskunder. Muligheten til å gi overtredelsesgebyr kan bidra til bedre etterlevelse i foretakene, noe som både kommer foretaket og kundene til gode.

2.1.2.14 Taushetsplikt og vern av personopplysninger

Artikkel 55 regulerer generelle krav til taushetsplikt.. Ansatte i Finanstilsynet er underlagt taushetsplikt, se finanstilsynsloven § 2-7. Finanstilsynet vurderer at artikkel 55 ikke er i motstrid med norske regler og viser i tillegg til at taushetsplikten er til for å beskytte foretakene. Finanstilsynet vurderer derfor at bestemmelsen bør gjøres gjeldende for foretakene.

Artikkel 56 regulerer krav til behandling personopplysninger. I tillegg gjelder reglene i personopplysningsloven, herunder personvernforordningen GDPR, når Finanstilsynet får tilgang til personopplysninger Vernet av personopplysninger beskytter foretaket og deres kunder. Finanstilsynet vurderer derfor at det også er hensiktsmessig å innføre denne bestemmelsen for foretakene.

2.1.2.15 Tilpasninger i regelverk

Utkast til forskrift om endring i DORA-forskriften mv. følger vedlagt. I utkastets kapittel 3 følger de konkrete forslagene for hvilke regler i DORA som skal få anvendelse for foretakene.

Ettersom Finanstilsynet foreslår at foretakene som i dag er underlagt IKT-forskriften skal etterleve bestemmelser i DORA er konsekvensen at IKT-forskriften må oppheves. Finanstilsynet bemerker at uttalelsene i Prop. 53 L (2024–2025) ikke burde være til hinder for at IKT-forskriften oppheves og at Norsk naturskadepool heller etterlever regler i DORA.

For Norsk naturskadepool har Finanstilsynet foreslått at foretakene må etterleve det forenklede rammeverket for risikostyring. Alternativet til en underleggelse av krav i DORA er at poolen må etterleve en veiledning tilsvarende foretakene som er unntatt i DORA artikkel 2 nr. 3 og foretakene uten IKT-regulering, se punkt 2.1.3 og 2.1.4. Når Justis- og beredskaps-departementet har vurdert at Norsk naturskadepool skal underlegges IKT-forskriften, mener Finanstilsynet at et alternativ der poolen kun skal etterleve en veiledning samsvarer dårlig med departementets signaler i Prop. 53 L (2024–2025). Dersom Norsk naturskadepool skal underlegges krav i DORA helt eller delvis, kreves hjemmel i lov. Finanstilsynet foreslår derfor at Norsk naturskadepool legges til som en ny bokstav g i DORA-loven § 2.

Finanstilsynet får tilsynsansvaret for Norsk naturskadepool fra og med 1. januar 2026. En eventuell lovendring vil antagelig tidligst tre i kraft 1. juli 2026. Et alternativ er å underlegge Norsk naturskadepool IKT-forskriften inntil loven er endret og underleggelse av krav i DORA kan finne sted. Finanstilsynet vurderer det som lite hensiktsmessig at poolen skal etterleve et regelverk i et halvt år, for deretter å underlegges et nytt regelverk.

Alternativet til å innta Norsk naturskadepool i DORA-loven § 2 er å gi DORA anvendelse gjennom en ny bestemmelse i naturskadeforsikringsforskriften, der det stilles krav til

etterlevelse av DORA. Finanstilsynet vurderer en slik løsning som lite hensiktsmessig, siden Finanstilsynet skal ha tilsynsansvaret og at det vil medføre en mer omfattende prosess ved eventuelle regelverksendringer.

Finanstilsynet vurderer at gjeldsinformasjonsforetak og kredittopplysningsforetak ikke bør være underlagt regler for IKT-virksomheten utover det som følger av gjeldsinformasjonsforskriften § 8, med unntak av bestemmelsens siste punktum. Som alternativ vurderer Finanstilsynet at det kan utarbeides en veiledning med forventninger til foretakenes oppfølging av IKT-virksomheten. Som resultat av Finanstilsynets forslag foreslås det at gjeldsinformasjonsforskriften § 8 siste punktum oppheves.

2.1.3. Foretak unntatt i DORA artikkel 2 nr. 3

Ifølge DORA artikkel 2 nr. 3 er visse foretak innen forsikring, pensjon og AIF-forvaltere unntatt fra reglene i DORA. Unntaket gjelder følgende foretak:

a. forvaltere av alternative investeringsfond som nevnt i artikkel 3 nr. 2 i direktiv 2011/61/EF,
b. forsikrings- og gjenforsikringsforetak som nevnt i artikkel 4 i direktiv 2009/138/EF,
c. tjenestepensjonsforetak som forvalter pensjonsordninger som til sammen ikke har mer enn 15 medlemmer i alt,
d. fysiske eller juridiske personer som er unntatt i henhold til artikkel 2 og 3 i direktiv 2014/65/EU,
e. forsikringsformidlere, gjenforsikringsformidlere og forsikringsformidlere som har forsikringsformidling som tilleggsvirksomhet, som er svært små, små eller mellomstore bedrifter,
f. postgirokontorer som nevnt i artikkel 2 nr. 5 punkt (3) i direktiv 2013/36/EU.

Foretakene har ikke lovpålagte krav til IKT-virksomhet etter at de ble tatt ut fra IKT-forskriftens virkeområde den 1. juli 2025.

Formålet med DORA er styrke den digitale operasjonelle motstandsdyktigheten for foretak i finanssektoren. Kravene i regelverket skal bidra til finansiell stabilitet, økt tillitt til finansmarkedene og redusere risiko for og konsekvensene av IKT-hendelser. Selv om det digitale trusselbildet er i endring og det følgelig er viktig med sikker IKT-drift også i foretakstypene som nevnt i artikkel 2 nr. 3, bør lovpålagte krav rettet mot foretakenes IKT-virksomhet være proporsjonale sett opp mot foretakenes størrelse og betydning for finanssektoren.

Finanstilsynet vurderer at foretakene som er unntatt fra DORA i artikkel 2 nr. 3 ikke skal underlegges krav i DORA på nåværende tidspunkt. Vurderingen begrunnes i foretakenes betydning for finansiell stabilitet og hensyn til forenkling av reguleringskrav for finansnæringen. Foretakene er i dag blant annet underlagt regler om virksomhetsstyring og risikostyring i finansforetaksloven eller risikostyringsforskriften. Finanstilsynet ser likevel behovet for at foretakene veiledes om hvilke forventninger som stilles til foretakets IKT-virksomhet. Behovet for en forventningsavklaring har blant annet blitt synliggjort gjennom en henvendelse Finanstilsynet mottok fra et foretak som var blitt tatt ut fra IKT-forskriftens virkeområde og unntatt fra virkeområdet i DORA etter artikkel 2 nr. 3. I henvendelsen ble det stilt spørsmål om hvilke krav som gjaldt for deres IKT-virksomhet. Finanstilsynet foreslår derfor å publisere en veiledning som skal bidra til at foretakene opprettholder en forsvarlig IKT-virksomhet og er i stand til å møte endringer i det digitale trusselbildet. Veiledningen vil gi uttrykk for Finanstilsynets forventning til foretakets styring av og kontroll med IKT-virksomhet. Foretakene

kan bruke veiledningen som støtte for å vurdere sin operasjonelle risiko, i tråd med kravene som følger av finansforetaksloven og risikostyringsforskriften.

2.1.4. Foretak uten IKT-regulering

Hittil har hverken morselskap i konsern eller låneformidlere vært underlagt regler om IKT-virksomhet. I forbindelse med høringen knyttet til DORA-loven uttalte Finansforbundet at det var behov for å "avklare virkeområdet til DORA når det gjelder bl.a. morselskap i finanskonsern. Morselskap er å anse som finansforetak, men det fremgår ikke av listen i høringsnotatet […] om hvorvidt de også omfattes av virkeområdet for DORA". I tillegg til å vurdere behovet for å underlegge morselskap i konsern krav til IKT-virksomhet etter DORA, har Finanstilsynet også vurdert behovet for å omfatte låneformidlere av DORAs virkeområde.

Regulering av morselskap i konsern kan være hensiktsmessig for å oppnå formålet med DORA om å styrke den digitale operasjonelle motstandsdyktigheten i finanssektoren. En regulering av morselskapet i et konsern kunne gitt flere fordeler, for eksempel en bedre IKT-risikostyring for konsernet som helhet. Dersom et morselskap leverer IKT-tjenester til et eller flere datterselskaper som er underlagt DORA, vil morselskapet likevel indirekte berøres av kravene som stilles til IKT-virksomhet i regelverket. Hensynet til forenkling av reguleringskrav i finansnæringen trekker også i retning av at morselskap ikke bør omfattes av DORAs virkeområde.

Selv om digital motstandsdyktighet hos norske låneformidlere har en betydning for den finansielle stabiliteten og for forbrukervern, tilsier de norske låneformidlingsforetakenes størrelse at de ikke vil utgjøre en større risiko for stabiliteten i finanssektoren dersom alvorlige IKT-hendelser skulle oppstå. Hensynet til forenkling i reguleringskrav i finanssektoren gjør seg også gjeldende i vurderingen av om låneformidlere bør underlegges krav i DORA.

Finanstilsynet vurderer etter dette at morselskap i konsern og låneformidlere ikke skal underlegges krav i DORA på nåværende tidspunkt. I tillegg til hensynet til forenklinger for foretak i finansnæringen, er forslaget om ikke å underlegge foretakene krav i DORA begrunnet i hvilken risiko foretakene kan utgjøre for finansiell stabilitet. I likhet med foretak som er unntatt i DORA artikkel 2 nr. 3, er de underlagt regler om virksomhetsstyring i henholdsvis finansforetaksloven og risikostyringsforskriften. For morselskap i konsern og låneformidlere mener Finanstilsynet at det er hensiktsmessig å utarbeide en veiledning om forsvarlig IKT-virksomhet, tilsvarende forslaget i punkt 2.1.3.

2.2. Oppgavefordeling og ansvar for TLPT

Ifølge DORA-loven § 3 fjerde ledd kan departementet fastsette bestemmelser i forskrift om trusselbasert penetrasjonstesting (TLPT), herunder om fordeling av oppgaver og ansvar mellom norske myndighetsorgan i henhold til DORA artikkel 26.

Hittil har foretak i finanssektoren gjennomført frivillig TLPT-testing etter TIBER-NO-rammeverket. Med DORA er krav til TLPT-testing lovfestet. TIBER-rammeverket tilfredsstiller kravene til TLPT-testing etter DORA.

Den kompetente myndigheten er TLPT-myndighet etter DORA med mindre en annen myndighet blir utpekt, se artikkel 26 nr. 9 og 10. Det er ikke pekt ut en TLPT-myndighet. Finanstilsynet er den kompetente myndigheten etter DORA og er dermed TLPT-myndighet.

Norges Bank og Finanstilsynet har siden 2021 samarbeidet om TLPT-testing etter TIBER-rammeverket. Ifølge forarbeidene til DORA-loven er hjemmelen i DORA-loven § 3 fjerde ledd

innført for å legge til rette for at samarbeidet og oppgavefordelingen mellom Finanstilsynet og Norges Bank kan videreføres ved TLPT-testing under DORA.[23]

Norges Bank og Finanstilsynet har hatt god dialog om hvordan TLPT-testing etter DORA bør utføres. De to myndighetene har en felles oppfatning av at samarbeidet knyttet til TLPT-testing etter TIBER-NO-rammeverket har fungert godt, og at erfaringene og samarbeidet fra TIBER-NO-rammeverket bør videreføres i arbeidet med TLPT-testing etter DORA. Formålet med TLPT-testing er å øke foretakenes digitale operasjonelle motstandsdyktighet, som er viktig for å opprettholde finansiell stabilitet. Et godt samarbeid mellom myndighetene er en forutsetning for en helhetlig tilnærming i arbeidet med å fremme stabilitet i det finansielle systemet.

Med bakgrunn i dialogen mellom Norges Bank og Finanstilsynet innga Norges Bank høringssvar[24] til høring[25] av DORA-forskriften. I høringssvaret ble det foreslått å forskriftsfeste hovedtrekkene i oppgavefordelingen for TLPT-testing etter DORA på følgende måte:

- Utpeking av foretak og testfrekvens, jf. artikkel 26 nr. 1 og nr. 8

  Finanstilsynet skal ha endelig beslutningskompetanse for utpeking av foretak og testfrekvens, men Norges Banks vurderinger og innspill skal vektlegges.

- Godkjenning av funksjoner og omfang, jf. artikkel 26 nr. 2

  Norges Bank skal ha endelig beslutningskompetanse, men Finanstilsynets vurderinger og innspill skal vektlegges.

- Oppgaver knyttet til gjennomføring av tester, jf. artikkel 26 og 27 samt delegert kommisjonsforordning (EU) 2025/1190

  Norges Bank skal ha ansvaret for oppgavene knyttet til rådgivning, overvåkning og koordinering gjennom hele testprosessen, inkludert attestering og samarbeid med andre lands TCT-er (teamene som gjennomfører testene fra myndighetssiden).

- Oppfølging av funn

  Finanstilsynet skal ha ansvaret for oppfølgingen av funn og tiltak etter gjennomført testing.

Finanstilsynet var kjent med og enig i hovedtrekkene i forslaget før Norges Bank sendte høringssvaret.

For at samarbeidet om TLPT-testing etter DORA skal kunne videreføres og samtidig være i tråd med DORA artikkel 26 nr. 10, er det nødvendig å ha en tydelig fordeling av myndighetenes oppgaver relatert til TLPT-testing. Dette sikrer også forutsigbarhet og klarere rammer for foretakene. Oppgavefordelingen må derfor tydelig framgå av forskriftsreglene.

Med bakgrunn i det ovennevnte foreslår Finanstilsynet et nytt kapittel om TLPT i DORA-forskriften som tydeliggjør fordelingen av ansvaret for oppgavene knyttet til gjennomføringen av slik testing. Kapittelet inneholder bestemmelser om hvilke oppgaver Norges Bank og Finanstilsynet har i forbindelse med utpeking og gjennomføring av TLPT-tester.

TLPT-testing er et tilsynsverktøy og Finanstilsynet er tilsynsmyndighet for foretakene som skal testes. Det foreslås derfor at Finanstilsynet skal ha ansvaret for å peke ut foretak som skal testes og å avgjøre testfrekvensen, jf. artikkel 26 nr. 1. Ved beslutning om utpeking av foretak og om testfrekvensfrekvens vil Finanstilsynet samarbeide med Norges Bank. Videre foreslås

[23] Se Prop. 54 LS (2024–2025), punkt 2.5.7.3

[24] Norges Banks høringssvar

[25] Høring - forskrift til DORA-loven

det en videreføring av Norges Banks rolle som TLPT cyber team (TCT). Rollen innebærer å ha ansvaret for å koordinere tester og attestere på at foretakene har gjennomført test. Norges Bank skal også godkjenne funksjonene foretaket foreslår skal testes. Ved godkjenning av foretakenes forslag til funksjoner som skal testes vil Norges Bank samarbeide med Finanstilsynet. Endelig skal Finanstilsynet ha ansvaret for å følge opp testfunn og tiltaksplan hos foretaket, siden dette ligger nærmere den tilsynsmessige oppfølgingen.

For å legge til rette for videreføring av det gode samarbeid mellom myndighetene ved gjennomføringen av TLPT-tester, foreslås det å forskriftsfeste at Norges Bank skal ha anledning til å uttale seg om hvilke foretak Finanstilsynet beslutter at skal gjennomføre test og hvilken testfrekvens foretakene skal ha. Tilsvarende foreslås det å forskriftsfeste at Finanstilsynet skal ha anledning til å uttale seg før Norges Bank godkjenner foretakets forslag til funksjoner som skal testes.

2.3. Endringer i andre forskrifter

Forskrift om systemer for betalingstjenester § 2 annet ledd omhandler krav til betalingstjenestetilbyderes risikovurdering og etterlevelse av regelverk. Bestemmelsen krever at foretaket skal ha "effektive fremgangsmåter for å håndtere hendelser, inkludert alvorlige operasjonelle hendelser og sikkerhetshendelser", se første punktum, siste del. For å harmonisere hendelsesrapportering, er det innført en bestemmelse i DORA artikkel 23 der det stilles krav til at betalingsrelaterte operasjonelle hendelser og sikkerhetshendelser hos kredittinstitusjoner, betalingsforetak, opplysningsfullmektiger og e-pengeforetak skal vurderes og rapporteres etter reglene i DORA kapittel III. Finanstilsynet foreslår derfor å fjerne § 2 annet ledd, første punktum, siste del i forskrift om systemer for betalingstjenester.

Ifølge forskriftens § 2 annet ledd, siste punktum, skal datatrafikk i elektroniske betalingstjenester overvåkes for å sikre tilstrekkelig sikkerhetsnivå og kunne avdekke og hindre uautorisert bruk av tjenesten. Finanstilsynet vurderer at bestemmelsen bør tilpasses til å være rettet mot tjenesten og ikke det IKT-spesifikke, siden DORA også inneholder regler om overvåkning for å hindre uautorisert bruk og krav til sikkerhet, se blant annet artikkel 6, 9 og 10. Finanstilsynet foreslår derfor at § 2 annet ledd, siste punktum endres til å kun gjelde overvåkning for å avdekke og hindre uautorisert bruk av tjenesten. Endringen samsvarer også med EUs forslag til ny forordning om betalingstjenester (PSR)[26] artikkel 83 nr. 1 bokstav c, som stiller krav til at betalingstjenesteytere skal ha transaksjonsovervåkning for å beskytte mot og avdekke svindel.

Finansforetaksforskriften § 3-2 og forskrift om systemer for betalingstjenester § 3 henviser til IKT-forskriften § 9 om hendelsesrapportering. Bestemmelsene i finansforetaksforskriften og forskrift om systemer for betalingstjenester er inntatt som en del av implementeringen av EUs andre betalingstjenestedirektiv PSD2 ((EU) 2015/2366). Henvisningene til IKT-forskriften i finansforetaksforskriften og i forskrift om systemer for betalingstjenester må rettes til tilsvarende bestemmelser i DORA. Finanstilsynet foreslår derfor at henvisningen i finansforetaksforskriften § 3-2 endres til DORA kapittel III og henvisningen i forskrift om systemer for betalingstjenester § 3 rettes til DORA artikkel 23.

3. Økonomiske og administrative konsekvenser

3.1. Innledning

DORA innebærer en harmonisering av krav til sikkerheten i nettverks- og informasjonssystemer som understøtter virksomheten i foretak i finanssektoren. Regelverket

[26] EUs forslag til forordning om betalingstjenester

skal øke tilliten til det finansielle systemet, opprettholde stabilitet og unngå store kostnader for økonomien ved å minimere konsekvenser og kostnader ved IKT-forstyrrelser. Krav etter IKT-forskriften og annet sektorregelverk tilsvarer langt på vei kravene som følger av DORA. Selv om dagens IKT-regelverk bygger på de samme prinsippene, følger det mer detaljerte krav til foretak i finanssektoren sin IKT-virksomhet etter DORA.

3.2. Konsekvenser for foretak

Foretakene som i dag skal etterleve IKT-forskriften, men som Finanstilsynet foreslår skal bli omfattet av krav i DORA, må etterleve mer detaljerte krav til blant annet styring av og kontroll med IKT-virksomhet, rammeverk for risikostyring, testing og styring av IKT-tredjepartsrisiko. Foretakene vil for eksempel ha behov for å oppdatere sine leverandøravtaler og interne prosesser, prosedyrer og rutiner for IKT-risikostyring i samsvar med de nye kravene. Likevel anses kravene i DORA å innebære mindre økonomiske og administrative konsekvenser for foretakene på nevnte områder. Eventuelle konsekvenser vil være mest fremtredende hos de mindre foretakene, og blant annet avhenge av om de blir underlagt krav om fullt eller forenklet rammeverket for IKT-risikostyring.

Når det gjelder krav til hendelseshåndtering og -rapportering, medfører de nye kravene at finansieringsforetak og inkassoforetak må innrette sine prosedyrer og rapportering til Finanstilsynet i samsvar med de mer detaljerte reglene som følger av DORA. Finanstilsynets vurdering er likevel at finansieringsforetak og inkassoforetak i hovedtrekk er underlagt tilsvarende krav etter dagens regelverk. Eiendomsmeglerforetak er underlagt krav om hendelseshåndtering, men ikke hendelsesrapportering etter IKT-forskriften. Gjennom forslaget om å bli underlagt krav om hendelsesrapportering for oppgjørsfunksjonen, må foretakene innrette seg etter nye krav og vil ha behov for å oppdatere prosesser for håndtering og rapportering av IKT-hendelser. Finanstilsynet vurderer likevel at de økonomiske og administrative konsekvensene vil være av mindre karakter.

For finansieringsforetak vil krav til rapportering og registerføring av IKT-tjenesteavtaler være tilsvarende som etter dagens regelverk. For eiendomsmeglerforetak (med egen oppgjørsfunksjon) og inkassoforetak, som hittil har vært unntatt meldeplikt, vil en underleggelse av krav i DORA med en eventuell meldeplikt for IKT-tjenesteavtaler medføre at foretaket må opprette prosedyrer for dette. Heller ikke krav til melding må anses å føre til en betydelig økonomisk eller administrativ belastning for foretakene det gjelder.

De økonomiske og administrative konsekvensene for Norsk naturskadepool ved underleggelse av krav til IKT-virksomheten ble i høringsnotat for ny naturskadeforsikringslov vurdert til å være av begrenset karakter.[27] En underleggelse av krav etter DORA vil medføre at Norsk naturskadepool blant annet må etterleve mer detaljerte krav til styring av og kontroll med IKT-virksomheten, herunder rammeverk for risikostyring, enn ved underleggelse av IKT-forskriften. En underleggelse av krav i DORA vil etter Finanstilsynets vurdering derfor medføre noe økt arbeidsbyrde og følgelig økte økonomiske konsekvenser på kort sikt. På lengre sikt vil foretaket derimot kunne oppnå en høyere grad av digital operasjonell motstandsdyktighet som kan begrense de mulige økonomiske og administrative konsekvensene som kan følge av en IKT-hendelse.

Finanstilsynet har adgang til å gi bøter til foretak som ikke overholder bestemte krav i DORA. På tilsvarende måte som ved pålegg og tvangsmulkt etter dagens regelverk[28], vil hensynet til proporsjonalitet vektlegges ved en eventuell vurdering av om et foretak skal ilegges bøter ved brudd på lovpålagte krav etter DORA. Med hensyn til de økonomiske konsekvensene som kan følge ved brudd på etterlevelse av krav for finansieringsforetak, eiendomsmeglerforetak, inkassoforetak og Norsk naturskadepool, vurderer Finanstilsynet at konsekvensene likevel

[27] Se Justis- og beredskapsdepartementets høringsnotat, punkt 7

[28] Se finanstilsynsloven § 4-1 og § 4-3

ikke vil bli betydelige. Dette begrunnes blant annet i hensynet til proporsjonalitet som følger av DORA.

Gjeldsinformasjonsforetak og kredittopplysningsforetak, som til nå har hatt krav til sin IKT-virksomhet gjennom gjeldsinformasjonsforskriften med videre henvisning til IKT-forskriften, vil etter forslaget kun være omfattet av gjeldsinformasjonsforskriftens krav til å sikre nødvendig konfidensialitet, integritet og tilgjengelighet for deres tjenester etter gjeldsinformasjonsloven. Ettersom forslaget innebærer at deler av de regulatoriske kravene faller bort, vil dette kunne lette den administrative og økonomiske byrden for foretakene. For gjeldsinformasjonsforetak har det blitt vist til at en veileder som inneholder forventninger til IKT-virksomhet kan være aktuelt.

Finanstilsynet vurderer at forslaget om å ikke underlegge foretakene i DORA artikkel 2 nr. 3 krav i forordningen, men heller stille forventninger til IKT-virksomheten gjennom en veiledning, ikke vil medføre negative økonomiske eller administrative konsekvenser for foretakene. Finanstilsynet vurderer derimot at en veiledning med klare forventninger til styring av og kontroll med IKT-virksomheten vil kunne bidra positivt til foretakenes identifisering og håndtering av IKT-risikoer, som en del av etterlevelsen av de generelle kravene til risikostyring og internkontroll i finansforetaksloven og risikostyringsforskriften. En veiledning kan derfor bidra til å redusere risikoen for omdømmetap og sanksjoner ved manglende styring av og kontroll med IKT-virksomheten. En veiledning vil etter Finanstilsynets syn også bidra til at foretakene i DORA artikkel 2 nr. 3 vil styrke sin digitale operasjonelle motstandsdyktighet.

3.3. Konsekvenser for myndigheter

Finanstilsynets forslag om å oppheve IKT-forskriften og heller underlegge foretak krav til IKT-virksomhet etter DORA, vil medføre en forenkling ved at Finanstilsynet får ett IKT-regelverk å forvalte og å føre tilsyn etter, selv om kravene etter DORA er mer detaljerte.

Forslaget om å innføre en rapporteringsplikt for eiendomsmeglerforetak for hendelser knyttet til oppgjørsfunksjonen i eiendomsmeglerforetak vil derimot kunne medføre en økt oppfølging fra Finanstilsynets side. Tilsvarende gjelder ved en innføring av meldeplikt for IKT-tjenesteavtaler som støtter kritiske eller viktige funksjoner for større inkassoforetak. Det samme gjelder for slike IKT-tjenesteavtaler knyttet til oppgjørsfunksjonen hos eiendomsmeglerforetak. Finanstilsynet vurderer likevel at de økonomiske og administrative konsekvensene som følger av de nevnte forslagene ikke vil være betydelige.

Forslaget om å underlegge Norsk naturskadepool krav i DORA i stedet for IKT-forskriften vil medføre noe økte, men begrensede økonomiske og administrative konsekvenser. Det vises også til at oppfølgingen her kun gjelder ett foretak.

Den foreslåtte endringen om å oppheve henvisningen til IKT-forskriften i gjeldsinformasjonsforskriften § 8 siste punktum vil kunne lette den tilsynsmessige oppfølgingen av gjeldsinformasjonsforetak for Finanstilsynet. Årsaken er at de gjenstående kravene i gjeldsinformasjonsforskriften er mindre omfattende enn de som følger av IKT-forskriften.

Når det gjelder de foreslåtte reglene knyttet til oppgavefordeling og ansvar for TLPT mellom Finanstilsynet og Norges Bank, vil oppgavene for begge myndighetene langt på vei tilsvare de samme som ved TLPT-testing under TIBER-NO. De foreslåtte reglene vil gi myndighetene klarere rammer og større forutsigbarhet. Norges Bank pekte i sitt høringssvar til DORA-forskriften på at TLPT vil medføre flere tester enn dagens TIBER-tester. Av den grunn vil begge myndigheter derfor kunne oppleve økt arbeidsmengde og følgelig en økt administrativ og økonomisk belastning. Finanstilsynet vurderer derfor de økonomiske og administrative konsekvensene samlet sett som moderat for norske myndigheter på dette området.

3.4. Konsekvenser for kunder og norsk økonomi

Finanstilsynet foreslår at flere foretak i finanssektoren skal underlegges krav i DORA. Som nevnt foreslås det at foretakene skal underlegges mer detaljerte regler, blant annet knyttet til styring av IKT-risiko, der formålet er å redusere sannsynligheten for hendelser og konsekvensene dersom hendelser oppstår. Det kan gi grunnlag for trygghet og tillit til den norske finanssektoren, i en situasjon der trusselbildet har blitt mer alvorlig. Siden IKT-hendelser som forstyrrer ytelsen av finansielle tjenester 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. At noen flere foretak i finanssektoren underlegges krav i DORA antas ikke å ha vesentlig betydning for prisingen av finansielle tjenester.

Utkast til lov om endring i DORA-loven

Endringer i følgende lover:

Lov 27. mai 2025 nr. 18 om digital operasjonell motstandsdyktighet i finanssektoren (DORA-loven)

I

I lov 27. mai 2025 nr. 18 om digital operasjonell motstandsdyktighet i finanssektoren (DORA-loven gjøres følgende endring:

§ 2 første ledd bokstav f og ny bokstav g skal lyde:

f. morselskap i finanskonsern,

g. Norsk naturskadepool.

II

Loven trer i kraft fra den tid Kongen bestemmer.

Utkast til forskrift om endring i DORA-forskriften mv.

Hjemmel: Lov 27. mai 2025 om digital operasjonell motstandsdyktighet i finanssektoren (DORA-loven) § 1 fjerde ledd, § 2 og § 3 fjerde ledd, lov 17. desember 1999 nr. 95 om betalingssystemer m.v. § 3-3 første ledd annet punktum og § 6-2 og lov 10. april 2015 nr. 17 om finansforetak og finanskonsern (finansforetaksloven) § 2-10 femte ledd, § 2-10a femte ledd og § 2-11 tredje ledd.

EØS-henvisninger: EØS-avtalen vedlegg IX nr. 31 q, forordning (EU) 2022/2554) og Kommisjonens gjennomføringsforordning (EU) 2024/2956.

I

I forskrift 24. juni 2025 nr. 1296 gjøres følgende endringer:

Nytt kapittel 1 skal bestå av nåværende § 1 - § 2 og skal ha følgende tittel:

Kapittel 1. Formål og virkeområde

§ 2 nytt annet ledd skal lyde:

Forskriftens kapittel 2 gjelder for finansieringsforetak, eiendomsmeglingsforetak, inkassoforetak og Norsk naturskadepool. Forskriftens § 3 gjelder også så langt det passer og med de tilpasninger som framgår av forskriftens kapittel 2.

Nytt kapittel 2 skal inneholde § 3 og overskriften skal lyde:

Kapittel 2. Utfyllende regelverk under forordning (EU) 2022/2554 (DORA)

Nytt kapittel 3 skal lyde:

Kapittel 3. DORA-forordningens anvendelse på andre foretak

§ 4. *Forordning om digital operasjonell motstandsdyktighet*

Forordning (EU) 2022/2554 gjelder slik det framgår av bestemmelsene i dette kapittelet og med de tilpasninger som framgår av EØS-avtalen vedlegg IX.

§ 5. *Definisjoner og proporsjonalitet*

Forordning (EU) 2022/2554 artikkel 3 og 4 gjelder tilsvarende.

§ 6. *Virksomhetsstyring og rammeverk for risikostyring*

Forordning (EU) 2022/2554 artikkel 5 til 15 gjelder tilsvarende for følgende foretak:

1. finansieringsforetak,
2. eiendomsmeglerforetak som er mellomstore eller større,
3. inkassoforetak som er mellomstore eller større.

Forordning (EU) 2022/2554 artikkel 16 gjelder for følgende foretak:

1. eiendomsmeglerforetak som er små eller mindre,

2. inkassoforetak som er små eller mindre og
3. Norsk naturskadepool.

§ 7. *Hendelseshåndtering og -rapportering*

Forordning (EU) 2022/2554 kapittel III gjelder tilsvarende for følgende foretak:

1. finansieringsforetak,
2. hendelser som er relatert til oppgjørsfunksjonen i eiendomsmeglerforetak
3. inkassoforetak og
4. Norsk naturskadepool.

§ 8. *Testing av digital operasjonell motstandsdyktighet*

Forordning (EU) 2022/2554 artikkel 24 og 25 gjelder tilsvarende.

§ 9. *Styring av IKT-tredjepartsrisiko*

Forordning (EU) 2022/2554 kapittel V, del I gjelder tilsvarende, med de tilpasninger som framgår av denne forskriftens § 10 og § 11. Artikkel 42 gjelder også tilsvarende.

§ 10. *Melding om inngått IKT-tjenesteavtale*

Forordning (EU) 2022/2554 artikkel 28 nr. 3 femte avsnitt gjelder for følgende foretak:

1. finansieringsforetak,
2. eiendomsmeglerforetak som inngår IKT-tjenesteavtale relatert til oppgjørsfunksjonen,
3. inkassoforetak som er underlagt det fulle rammeverket for risikostyring og
4. Norsk naturskadepool.

§ 11. *Krav til register over IKT-tjenesteavtaler*

Forordning (EU) 2022/2554 artikkel 28 nr. 3 første avsnitt gjelder tilsvarende, men foretaket skal kun ha register på foretaksnivå. Kommisjonens gjennomføringsforordning (EU) 2024/2956 gjelder ikke.

Registeret over IKT-tjenesteavtaler skal minst inneholde følgende opplysninger:

1. leverandørens navn og organisasjonsnummer, LEI-nummer og EUID. Dersom leverandøren har både LEI-nummer og EUID, skal begge oppgis,
2. en beskrivelse av typen IKT-tjenesteavtale,
3. landet leverandøren har hovedkontor i,
4. underleverandørers navn og organisasjonsnummer, samt lanet underleverandøren har hovedkontor i,
5. avtalens oppstarts og opphørsdato eller opplysning om at avtalen er rullerende og
6. dato for siste risikovurdering av IKT-tjenesteavtalen.

§ 12. *Informasjonsdeling*

Forordning (EU) 2022/2554 kapittel VI gjelder tilsvarende.

§ 13. *Overtredelsesgebyr*

Forordning (EU) 2022/2554 artikkel 50, 51 og 54 gjelder tilsvarende, med de begrensinger som framgår av DORA-loven § 4.

§ 14. *Vern av personopplysninger og taushetsplikt*

Forordning (EU) 2022/2554 artikkel 55 og 56 gjelder tilsvarende.

Nytt kapittel 4 skal lyde:

Kapittel 4. Trusselbasert penetrasjonstesting (TLPT)

§ 15. *Utpeking av foretak som skal gjennomføre TLPT*

Finanstilsynet skal beslutte hvilke foretak som skal gjennomføre TLPT-tester i henhold til forordning (EU) 2022/2554 artikkel 26. Finanstilsynet skal også beslutte hvor ofte et foretak skal gjennomføre slike tester. Før Finanstilsynet treffer en beslutning om utpeking av foretak eller testfrekvens, skal Norges Bank gis anledning til å uttale seg.

§ 16. *Godkjenning av funksjoner som skal testes*

Norges Bank skal godkjenne det utpekte foretakets forslag til hvilke funksjoner som skal omfattes av TLPT-testen. Før Norges Bank godkjenner forslag til testing av funksjoner, skal Finanstilsynet gis anledning til å uttale seg.

§ 17. *TLPT cyber team og koordinering av TLPT*

Norges Bank skal ha rollen som TLPT cyber team (TCT) ved gjennomføring av TLPT-tester og være ansvarlig for å koordinere testgjennomføringen.

§ 18. *Attest og oppfølging etter gjennomført TLPT*

Norges Bank skal utstede en attest som bekrefter foretakets gjennomføring av en TLPT-test. Attesten skal være i tråd med forordning (EU) 2022/2554 artikkel 26 nr. 7.

Finanstilsynet er ansvarlig for å følge opp testfunnene og tiltaksplanen.

Nytt kapittel 5 skal inneholde nåværende § 4 og ha overskriften:

Kapittel 5. Ikrafttredelse

Nåværende § 4 skal være § 19.

II

I forskrift 31. oktober 2017 nr. 1691 om virksomhet etter gjeldsinformasjonsloven (gjeldsinformasjonsforskriften) gjøres følgende endringer:

§ 8 siste punktum oppheves.

III

I forskrift 9. desember 2016 nr. 1502 om finansforetak og finanskonsern (finansforetaksforskriften) gjøres følgende endringer:

§ 3-2 bokstav a skal lyde:

En beskrivelse av foretakets rutiner for å overvåke, håndtere og følge opp sikkerhetshendelser og sikkerhetsrelaterte kundeklager, samt rutine for rapportering av alvorlige operasjonelle hendelser og sikkerhetshendelser *jf. forordning (EU) 2022/2554 om digital operasjonell motstandsdyktighet i finanssektoren, kapittel III.*

IV

I forskrift 15. februar 2019 nr. 152 om systemer for betalingstjenester gjøres følgende endringer:

§ 2 annet ledd skal lyde:

Betalingstjenestetilbydere skal ha systemer og kontrollmekanismer for operasjonell og sikkerhetsmessig risiko knyttet til ytelsen av betalingstjenester. Systemene skal sikre etterlevelse av regelverk, avtaler og interne rutiner. Elektroniske betalingstjenester skal overvåkes for å kunne avdekke og hindre uautorisert bruk av tjenesten.

§ 3 skal lyde:

Dersom hendelse som angitt i *forordning (EU) 2022/2554 om digital operasjonell motstandsdyktighet i finanssektoren artikkel 23* påvirker eller kan påvirke betalingstjenestebrukernes økonomiske interesser, skal betalingstjenestetilbyderen uten ugrunnet opphold underrette brukerne om hendelsen. Meldingen skal omtale tiltak brukeren kan iverksette

V

Forskrift 21. mai 2003 nr. 630 om bruk av informasjons- og kommunikasjonsteknologi (IKT) oppheves.

VI

Forskriften trer i kraft fra den tid departementet bestemmer.

Finanstilsynet
Revierstredet 3
P.O. Box 1187 Sentrum
NO-0107 Oslo

Tel. +47 22 93 98 00
post@finanstilsynet.no
finanstilsynet.no