Finansdepartementet

Høringsnotat

Nytt regelverk for digital operasjonell motstandsdyktighet i finanssektoren

Norsk gjennomføring av *Digital Operational Resilience Act (DORA)*

23. januar 2024

Innhold

1 Innledning og bakgrunn ... 3
2 Gjeldende rett ... 5
2.1 Lovregler og generelle forskriftskrav ... 5
2.1.1 Finansforetak og betalingssystemer ... 5
2.1.2 Verdipapirområdet ... 5
2.1.3 Finanstilsynsloven ... 6
2.2 IKT-forskriften ... 7
2.2.1 Virkeområde ... 7
2.2.2 Risikostyring ... 7
2.2.3 Hendelseshåndtering ... 8
2.2.4 IKT-leverandører ... 9
3 Forventet EØS-rett ... 10
3.1 Forordning (EU) 2022/2554 ... 10
3.1.1 Formål og virkeområde ... 10
3.1.2 Risikostyring ... 11
3.1.3 Hendelseshåndtering ... 13
3.1.4 Test av motstandsdyktighet ... 14
3.1.5 Avtaler om bruk av IKT-tjenester ... 16
3.1.6 Overvåking av IKT-leverandører ... 17
3.1.7 Informasjonsdeling mellom foretak ... 20
3.1.8 Tilsyn og myndighetssamarbeid ... 20
3.1.9 Endringer i andre forordninger ... 22
3.1.10 Avsluttende bestemmelser ... 23
3.2 Direktiv (EU) 2022/2556 ... 23
4 Departementets foreløpige vurdering ... 24
4.1 Behov god regulering av IKT-risiko ... 24
4.2 Gjennomføring og virkeområde mv. ... 25
4.2.1 Gjennomføring ... 25
4.2.2 Virkeområde og nasjonale krav ... 25
4.2.3 Forholdet til annen hendelsesrapportering ... 26
4.2.4 Forholdet til utkontraktering generelt ... 27
4.3 Tilsyn og sanksjoner ... 27
4.3.1 Tilsynsmyndighet ... 27
4.3.2 Sanksjoner ... 28
4.4 Tilpasninger i annet regelverk ... 29
5 Økonomiske og administrative konsekvenser ... 31
5.1 Innledning ... 31
5.2 Konsekvenser for foretak i finanssektoren ... 31
5.3 Konsekvenser for IKT-leverandører ... 32
5.4 Konsekvenser for kunder og norsk økonomi ... 32
5.5 Konsekvenser for myndigheter ... 32
6 Utkast til regelverksendringer ... 33
6.1 Utkast til lov om digital operasjonell motstandsdyktighet i finanssektoren ... 33
6.2 Utkast til lov om endringer i finanslovgivningen mv. ... 34
6.3 Utkast til forskrift om endring i finansforetaksforskriften og forskrift om pensjonsforetak ... 38

1 Innledning og bakgrunn

Finanssektoren er i stor grad avhengig av digitale løsninger, og benytter seg i økende grad av tredjepartsleverandører for IKT-tjenester og -utstyr. Kompleksiteten i tjenesteproduksjonen og kontraktsforholdene med IKT-leverandørene har økt betydelig over mange år. I tillegg opererer mange finansielle foretak i flere land, samtidig som markedet for IKT-tjenester til finanssektoren er preget av internasjonalisering og konsolidering. Den norske finanssektoren er blant de mest digitaliserte i verden, og tett integrert med finansmarkedene i Norden og Europa. Digitaliseringen gir store fordeler både for foretakene, kundene og samfunnet ellers, men innebærer også risikoer og sårbarheter. Alvorlig svikt i IKT-systemer kan i verste fall true den finansielle stabiliteten og påvirke samfunnssikkerheten, enten svikten forårsakes av operasjonelle avvik, vinningskriminalitet eller målrettede angrep.

Den finansielle infrastrukturen i Norge vurderes som robust, samtidig som endringer i det digitale trusselbildet, bl.a. som følge av Russlands angrep på Ukraina og økt digital kriminalitet, har bidratt til økt oppmerksomhet om faren for systemiske cyberhendelser og viktigheten av digital robusthet og motstandsdyktighet innen finanssektoren.[1] Totalberedskapskommisjonen har nylig anbefalt å forsterke arbeidet med infrastruktur og digital sikkerhet generelt, og bl.a. pekt på at det i lys av utviklingen i trussel- og risikobildet er «behov for å forbedre hvordan risikostyring utøves både på myndighets- og virksomhetssiden» og for «en vesentlig heving av innsatsen på forebygging og videreutvikling av våre teknologiske infrastrukturer og digitale tjenester».[2] For finansielle tjenester mener kommisjonen at «det er avgjørende å sikre et likt og samtidig regelverk i Europa som gir like krav til blant annet risikostyring, rapportering, informasjonsutveksling og krav til utkontraktering og oppfølging av tredjeparter».

Foretakene i den norske finanssektoren har i mange år vært underlagt regelverk og tilsyn som skal bidra til en høy grad av IKT-sikkerhet, enten foretakene drifter løsningene selv eller har utkontraktert dette til IKT-leverandører. Særlig stiller IKT-forskriften fra 2003 omfattende krav til foretakenes risikostyring, hendelseshåndtering og bruk av IKT-leverandører. Siden det til nå ikke har vært noe harmonisert, felleseuropeisk regelverk på dette området, har krav om digital motstandsdyktighet og IKT-sikkerhet i stor grad vært nasjonale, med betydelig variasjon mellom land. EØS-regelverk for ulike deler av finanssektoren har hatt krav om håndtering av IKT-risiko som en del av reglene om operasjonell risiko, bl.a. i form av krav til tapsabsorberende kapital for å dekke en gitt IKT-risiko, og indirekte i form av generelle krav til forsvarlig organisering og drift av virksomheten. I den grad det har vært konkrete krav til hvordan foretakene har innrettet IKT-virksomheten, styrt risiko og håndtert hendelser, har dette i hovedsak blitt gitt på nasjonalt nivå, selv om felleseuropeiske tilsynsstandarder har bidratt til konvergens på viktige områder.

For å samle og vesentlig bygge ut de felleseuropeiske reglene om håndtering av IKT-risiko i finanssektoren, ble forordning (EU) 2022/2554 om digital operasjonell motstandsdyktighet vedtatt i EU i desember 2022, sammen med et tilhørende direktiv.

[1] Se Finanstilsynets *Risiko- og sårbarhetsanalyse 2023*.
[2] Se NOU 2023: 17.

Det nye regelverket omtales som «Digital Operational Resilience Act» (DORA), og skal gjelde i EU fra januar 2025. DORA inneholder omfattende krav til foretakenes IKT-risikostyring, håndtering og rapportering av IKT-hendelser, testing av den digitale motstandsdyktigheten, bruk av IKT-leverandører og informasjonsdeling. Det er også rammeverk for myndighetsovervåking på europeisk nivå av kritiske IKT-leverandører og tilrettelegging for tettere samarbeid på tvers av land og myndigheter. Regelverket har få nasjonale valg, og skal dessuten utfylles med felles tekniske standarder på en rekke områder. Behovet for et heldekkende og harmonisert regelverk er bl.a. begrunnet slik i fortalen til forordningen:[3]

> *«Siden bestemmelser om IKT-risiko bare delvis er behandlet på EU-nivå, er det i dag hull eller overlapp på viktige områder, f.eks. IKT-hendelsesrapportering og testing av digital operasjonell motstandsdyktighet, og inkonsistens som følge av forskjellige nasjonale regler eller kostnadsineffektiv anvendelse av overlappende regler. Dette er spesielt skadelig for en IKT-intensiv bruker som finanssektoren, siden teknologirisiko er grenseoverskridende og finanssektoren leverer tjenester på bred, grensekryssende basis. Finansielle foretak som har grensekryssende virksomhet eller flere konsesjoner (f.eks. kan ett foretak ha konsesjoner som bank, verdipapirforetak og betalingsforetak fra forskjellige myndigheter i én eller flere medlemstater), står overfor operasjonelle utfordringer med å håndtere IKT-risiko og redusere negative virkninger av IKT-hendelser på egenhånd og på en sammenhengende, kostnadseffektiv måte. (…)*
>
> *Finansielle foretak bør ha samme tilnærming og følge de samme prinsippbaserte reglene ved håndtering av IKT-risiko, men ta hensyn til foretakets størrelse og overordnede risikoprofil, samt arten, omfanget og kompleksiteten til foretakets tjenester, aktiviteter og operasjoner. Konsistens bidrar til å øke tilliten til det finansielle systemet og opprettholde stabilitet, spesielt i tider med høy avhengighet av IKT-systemer, -plattformer og -infrastruktur, som innebærer økt digital risiko. Å ha grunnleggende cyberhygiene bidrar også til å unngå store kostnader for økonomien ved å minimere konsekvenser og kostnader ved IKT-forstyrrelser.»*

DORA-regelverket antas å være EØS-relevant, og Finanstilsynet har på oppdrag fra Finansdepartementet utredet behovet for endringer i norsk rett for å gjennomføre de forventede EØS-forpliktelsene. Dette høringsnotatet er utarbeidet av departementet på grunnlag av Finanstilsynets utredning og andre kilder. Etter gjennomgang av gjeldende rett i kapittel 2 og de forventede EØS-forpliktelsene i kapittel 3, følger departementets foreløpige vurdering i kapittel 4. De økonomiske og administrative konsekvensene er omtalt i kapittel 5. Departementets foreløpige utkast til regelverksendringer i kapittel 6 innebærer at DORA-forordningen gjennomføres i en ny lov om digital operasjonell motstandsdyktighet i finanssektoren, og at det foretas konsekvenstilpasninger i enkelte lover og forskrifter på finansmarkedsområdet.

[3] Punkt 10 og 13 i fortalen til forordning (EU) 2022/2554, oversatt fra dansk versjon.

2 Gjeldende rett

2.1 Lovregler og generelle forskriftskrav

2.1.1 Finansforetak og betalingssystemer

Etter lov 10. april 2015 nr. 17 om finansforetak og finanskonsern (finansforetaksloven) § 13-5 skal et finansforetak organiseres og drives på en forsvarlig måte, og ha en klar organisasjonsstruktur og ansvarsfordeling samt klare og hensiktsmessige styrings- og kontrollordninger. Foretaket skal ha hensiktsmessige retningslinjer og rutiner for å identifisere, styre, overvåke og rapportere risiko foretaket er, eller kan bli, eksponert for, samt uavhengige kontrollfunksjoner med ansvar for internrevisjon, risikostyring og etterlevelse av regelverk. Foretakets styrings- og kontrollordninger samt retningslinjer og rutiner skal være tilpasset risikoen ved og omfanget av virksomheten i foretaket. Departementet har gitt utfyllende regler i forskrift.

Betalingssystemer er systemer for overføring av midler med formelle og standardiserte ordninger og felles regler for behandling, avregning eller oppgjør av betalingstransaksjoner, jf. lov 17. desember 1999 nr. 95 om betalingssystemer m.v. (betalingssystemloven) § 1-1 første ledd. Systemer for betalingstjenester er i § 1-1 tredje ledd definert som systemer basert på standardvilkår for overføring av penger fra eller mellom kundekonti i banker mv. når overføringene bygger på bruk av betalingskort, tallkoder eller annen form for selvstendig brukerlegitimasjon utstedt til en ubestemt krets. Loven skal bl.a. bidra til at systemer for betalingstjenester innrettes og drives slik at hensynet til sikker og effektiv betaling og til rasjonell og samordnet utførelse av betalingstjenester ivaretas, jf. § 3-1. Systemer for betalingstjenester skal etter § 3-3 første ledd innrettes og drives i samsvar med formålet i § 3-1, og Finanstilsynet kan gi nærmere regler om standardisering av avtaler, vilkår, tekniske forhold mv. for systemer for betalingstjenester.

Forskrift 22. august 2014 nr. 1097 om kapitalkrav og nasjonal tilpasning av CRR/CRD IV (CRR/CRD IV-forskriften) del X har nærmere regler om risikostyring og internkontroll for bl.a. banker, kredittforetak og finansieringsforetak, samt verdipapirforetak og visse forvaltningsselskaper. Forskrift 9. desember 2016 nr. 1503 § 22 gir nærmere regler om risikostyring og internkontroll for pensjonsforetak. Forskrift 9. desember 2016 nr. 1502 om finansforetak og finanskonsern § 3-2 gir tilleggskrav til søknad om tillatelse som betalingsforetak og e-pengeforetak, herunder om IKT-drift og beredskap. Forskrift 15. februar 2019 nr. 152 om systemer for betalingstjenester er fastsatt i medhold av finansforetaksloven og betalingssystemloven, og gir nærmere regler bl.a. om risikovurdering og krav til sikker ytelse.

2.1.2 Verdipapirområdet

Etter lov 29. juni 2007 nr. 75 om verdipapirhandel (verdipapirhandelloven) § 9-16 er det bl.a. krav om at verdipapirforetak skal treffe tiltak som skal sikre kontinuitet og regelmessighet i investeringstjenestevirksomheten og tiltak som begrenser operasjonell risiko til et minimum når det benytter seg av en tredjepart til å utføre operasjonelle funksjoner, og det skal ha effektive kontroll- og sikkerhetsordninger for informasjons-

behandlingssystemer, gode administrasjons- og regnskapsrutiner og tilfredsstillende interne kontrollordninger. Etter § 11-11 skal markedsoperatører for regulerte markeder etablere og gjennomføre internkontroll i samsvar med relevant regelverk og retningslinjer, og etter § 11-18 ha interne regler og tiltak som bl.a. sikrer identifisering og håndtering av vesentlige risikoer som virksomheten utsettes for, at markedet har systemer for en forsvarlig drift av det tekniske systemet, herunder effektive ordninger i tilfelle teknisk avbrudd. Etter § 11-19 skal et regulert marked bl.a. ha effektive systemer, prosedyrer og ordninger som sikrer at handelssystemet er robust, samt beredskapsplaner og systemer som sikrer kontinuerlig drift ved svikt i handelssystemet. Departementet kan i forskrift gi utfyllende regler til de ulike bestemmelsene.

Etter lov 25. november 2011 nr. 44 om verdipapirfond (verdipapirfondloven) § 2-11 skal forvaltningsselskap for verdipapirfond innrette sin virksomhet slik at det bl.a. har gode administrasjons- og regnskapsrutiner og kontroll- og sikkerhetsordninger. Tilsvarende gjelder for forvaltere av alternative investeringsfond etter lov 20. juni 2014 nr. 28 om forvaltning av alternative investeringsfond § 3-1. Departementet kan i forskrift gi utfyllende regler til de ulike bestemmelsene.

I tillegg til det ovennevnte er det regler om håndtering av operasjonell risiko mv. i kredittvurderingsbyråforordningen (CRA), forordningen om OTC-derivater, sentrale motparter og transaksjonsregistre (EMIR), verdipapirsentralforordningen (CSDR), verdipapirmarkedsforordningen (MiFIR) og referanseverdiforordningen (BMR), som er gjennomført i henholdsvis lov 20. juni 2014 nr. 30 om kredittvurderingsbyråer § 1, verdipapirhandelloven § 17-1, lov 15. mars 2019 nr. 6 om verdipapirsentraler og verdipapiroppgjør mv. (verdipapirsentralloven) § 1-1, verdipapirhandelloven § 8-1 og lov 4. desember 2015 nr. 95 om fastsettelse av finansielle referanseverdier (referanseverdiloven) § 1.

Forskrift 22. september 2008 nr. 1080 gir nærmere regler om risikostyring og internkontroll for regulerte markeder, verdipapirforetak, forvaltningsselskaper for verdipapirfond, betalingsforetak og opplysningsfullmektiger, e-pengeforetak, forsikringsformidlingsvirksomhet, eiendomsmeglingsforetak, inkassoforetak, regnskapsforetak, gjeldsinformasjonsforetak, låneformidlingsvirksomhet (unntatt aksessorisk låneformidling) og revisjonsforetak.

2.1.3 Finanstilsynsloven

Etter lov 7. juli 1956 nr. 1 om tilsynet med finansforetak mv. (finanstilsynsloven) § 4 kan Finanstilsynet gi visse pålegg og bestemmelser som skal gjelde for foretak under tilsyn, bl.a. knyttet til innretningen av internkontrollen. Etter § 4 c skal foretakene melde fra til Finanstilsynet ved inngåelse av avtale om utkontraktering av virksomhet, ved senere endring av slik avtale og ved bytte av oppdragstaker. Meldingen skal gis minst 60 dager før iverksettelsen av avtalen, avtaleendringen eller byttet av oppdragstaker. Finanstilsynet kan sette vilkår for utkontrakteringen eller gi foretaket pålegg om ikke å iverksette eller om å avslutte oppdraget, dersom tilsynet finner at utkontraktering skjer i et omfang eller på en måte som ikke kan anses som forsvarlig, vanskeliggjør tilsynet med den utkontrakterte virksomhet eller med foretakets samlede virksomhet, eller er i strid med bestemmelser gitt i eller i medhold av lov. Finanstilsynet kan

ved forskrift eller enkeltvedtak fastsette krav til melding etter første ledd og kan gjøre unntak fra meldeplikten. I forskrift 15. september 2021 nr. 2777 om meldeplikt ved utkontraktering av virksomhet mv. er det bl.a. angitt at meldeplikten gjelder avtaler om utkontraktering av virksomhet som er kritisk eller viktig for foretaket, og at meldeplikten ikke gjelder for forvaltere for verdipapirfond og alternative investeringsfond, regnskapsførerforetak, revisjonsforetak, eiendomsmeglingsforetak, advokater som driver eiendomsmegling, inkassoforetak, låneformidlere og forsikringsformidlere.

Et utkast til ny finanstilsynslov var på høring i 2023.[4] Høringsutkastet viderefører i hovedsak gjeldende finanstilsynslov §§ 4 og 4 c.

2.2 IKT-forskriften

2.2.1 Virkeområde

Forskrift 21. mai 2003 nr. 630 om bruk av informasjons- og kommunikasjonsteknologi (IKT-forskriften) er fastsatt av Finanstilsynet i medhold av betalingssystemloven § 3-3 første ledd, finanstilsynsloven § 4 og verdipapirhandelloven § 11-11 (tidligere børsloven § 11). IKT-forskriften gjelder etter § 1 første ledd for norske

1) banker,
2) kredittforetak,
3) finansieringsforetak,
4) forsikringsforetak,
5) private, kommunale og fylkeskommunale pensjonskasser og pensjonsfond,
6) børser og autoriserte markedsplasser,
7) verdipapirforetak,
8) forvaltningsselskaper for verdipapirfond,
9) inkassoforetak,
10) eiendomsmeglerforetak,
11) betalingsforetak og opplysningsfullmektiger,
12) e-pengeforetak og
13) systemer for betalingstjenester.

Etter § 1 annet ledd omfatter forskriften IKT-systemer som er av betydning for foretakets virksomhet, og for eksterne brukere av foretakets IKT-systemer skal det foreligge avtaler som sikrer at forskriftens krav til sikkerhet og dokumentasjon ivaretas.

Etter forskrift 31. oktober 2017 nr. 1691 om virksomhet etter gjeldsinformasjonsloven (gjeldsinformasjonsforskriften) § 8 gjelder IKT-forskriften tilsvarende for gjeldsinformasjonsforetak og kredittopplysningsforetak.

2.2.2 Risikostyring

IKT-forskriften § 2 gjelder planlegging og organisering av IKT-virksomheten. Det skal fastsettes overordnede mål, strategier og sikkerhetskrav, og foreligge beskrivelse av den enkelte prosess og hvordan ansvaret for administrasjon, anskaffelse, utvikling,

[4] Se NOU 2023: 6, som Finansdepartementet hadde på høring til 2. juni 2023.

drift, systemvedlikehold, sikring av informasjon og avvikling utføres på en betryggende måte. For de ulike delene av IKT-virksomheten skal det oppnevnes ansvarlige funksjoner eller stillinger. Det er også regler om utkontraktering, se avsnitt 2.2.4.

Etter forskriften § 3 skal foretaket fastsette kriterier for akseptabel risiko og ha en dokumentert prosess for risikoanalyser av IKT-virksomheten. Foretaket skal minst årlig gjennomføre risikoanalyser for å påse at risiko styres innenfor akseptable grenser. Etter § 4 skal foretaket fastsette kvalitetsmål for de enkelte deler av IKT-virksomheten og ha dokumenterte prosedyrer for oppfølging av målene. Etter § 5 skal foretaket ha prosedyrer for beskyttelse av utstyr, systemer og informasjon mot skader, misbruk, uautorisert adgang og endring, samt hærverk. Prosedyrene skal omfatte tildeling, endring, sletting og kontroll med autorisasjon for tilgang til systemene.

Foretaket skal etter forskriften § 6 ha prosedyrer for anskaffelse, utvikling, videreutvikling og testing av IKT-systemer, og etter § 7 skal sikre at systemene vedlikeholdes og forvaltes på en måte som gir en stabil, planlagt og forutsigbar drift. Driften skal etter § 8 være basert på dokumenterte prosedyrer som sikrer fullstendig, rettidig og korrekt behandling og oppbevaring av data, og en tilgjengelighet i tråd med foretakets dokumenterte krav. Det skal gjennomføres regelmessige analyser og tiltak for å motvirke avvik, og foretaket skal teste og dokumentere at driften fungerer i henhold til foretakets dokumenterte krav.

Etter forskriften § 11 skal foretaket ha en dokumentert kriseplan som skal iverksettes dersom IKT-driften ikke kan opprettholdes som følge av en krise. Med krise menes hendelser som forårsaker driftsavbrudd slik at foretakets IKT-drift ikke kan fortsette med normalt tilgjengelige ressurser. Kriseplanen skal bl.a. omfatte beskrivelse og kriterier for oppstart av en kriseløsning, prosedyrer for å gjenopprette IKT-driften og informasjon til ansatte, leverandører, kunder, myndigheter og media. Det skal minst en gang årlig gjennomføres opplæring, øvelse og testing av at kriseløsningen virker som forutsatt, og resultatet av testen skal dokumenteres.

Etter forskriften § 13 skal det foreligge en samlet oppdatert oversikt over organisasjon, utstyr, IKT-systemer og vesentlige forhold i IKT-virksomheten. Det skal foreligge oppdatert dokumentasjon av det enkelte IKT-system som er av betydning for foretakets virksomhet og som dokumenterer at forskriftens krav er oppfylt til enhver tid.

2.2.3 Hendelseshåndtering

Etter IKT-forskriften § 9 skal foretaket ha prosedyrer for avviks- og endringshåndtering og sikre at disse følges. Prosedyrene for avvikshåndtering skal etter annet ledd omfatte alle avvik som oppstår i driften av IKT-systemene, og ha som formål å gjenopprette normal tilstand. De skal også inneholde retningslinjer for eskalering. Avviksbehandlingen skal identifisere årsak, hindre gjentagelser og sikre forsvarlig og formell behandling og dokumentering av avviket. Prosedyrene for endringshåndtering skal etter fjerde ledd omfatte alle endringer som kan påvirke IKT-systemene og skal sikre forsvarlig, formell behandling og dokumentering av endringene. Foretaket skal sikre at prosedyrene for endringshåndtering gir en stabil, planlagt og forutsigbar drift.

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, skal etter § 9 tredje ledd uten ugrunnet opphold rapporteres til Finanstilsynet.[5] Rapporteringen skal normalt omfatte hendelser som foretaket kategoriserer som svært alvorlig eller kritisk, men kan også omfatte andre avvik dersom disse avdekker spesielle sårbarheter i applikasjon, arkitektur, infrastruktur eller forsvarsverk.

2.2.4 IKT-leverandører

Etter IKT-forskriften § 12 har foretaket ansvar for at IKT-virksomheten oppfyller alle krav i forskriften, også når hele eller deler av IKT-virksomheten er utkontraktert, og det skal i tilfelle foreligge en skriftlig avtale som sikrer dette. Avtalen må sikre at foretak under tilsyn også gis rett til å kontrollere, herunder revidere, de av leverandørens aktiviteter som er knyttet til avtalen. Avtalen skal også sikre håndtering av taushetsbelagt informasjon. Avtalen skal videre sikre at Finanstilsynet gis tilgang til opplysninger fra og tilsyn hos IKT-leverandøren, der Finanstilsynet finner det nødvendig som et ledd i tilsynet med foretaket. Foretaket skal sikre, i egen regi eller gjennom et formalisert samarbeid med andre foretak enn IKT-leverandøren, at organisasjonen besitter tilstrekkelig kompetanse til å forvalte utkontrakteringsavtalen.

Etter § 2 fjerde ledd skal avtaler om utkontraktering av IKT-virksomhet behandles av styret, som skal forelegges planer for utkontrakteringen, med risikovurdering, og en beskrivelse av hvordan foretaket skal sikre leveransen. Foretaket skal også ha retningslinjer som skal sikre at utkontraktert IKT-virksomhet oppfyller forskriftens krav.

[5] Eiendomsmeglerforetak omfattes ikke av kravet til hendelsesrapportering.

3 Forventet EØS-rett

3.1 Forordning (EU) 2022/2554

3.1.1 Formål og virkeområde

Forordning (EU) 2022/2554 om digital operasjonell motstandsdyktighet i finanssektoren ble vedtatt i EU 14. desember 2022, og skal etter artikkel 64 gjelde der fra 17. januar 2025. Forordningen omtales som DORA («Digital Operational Resilience Act»). Samtidig med forordningen ble direktiv (EU) 2022/2556 vedtatt for å gjøre nødvendige tilpasninger i ulike direktiver på finansmarkedsområdet, se avsnitt 3.2. Begge rettsakter antas å være EØS-relevante.

Forordningen kapittel I omfatter generelle bestemmelser. Formålet er etter artikkel 1 å oppnå et høyt felles nivå av digital operasjonell motstandsdyktighet gjennom like krav til sikkerheten i nettverks- og informasjonssystemer som understøtter virksomheten i finansielle foretak. Det stilles krav til foretakene, utkontrakteringsavtaler, felleseuropeisk overvåking av kritiske IKT-leverandører og tilsyn og tilsynssamarbeid. Artikkel 1 sier også at forordningen skal regnes som et sektorspesifikt regelverk med krav som minst tilsvarer de generelle kravene til sikkerhet i nettverks- og informasjonssystemer i direktiv (EU) 2022/2555 (NIS2-direktivet), jf. boks 3.2. Det vil si at finansielle foretak unntas fra kravene i NIS2-direktivet, som i utgangspunktet gjelder alle tilbydere av samfunnsviktige tjenester.

Kravene i forordningen skal etter artikkel 2 nr. 1 gjelde følgende foretak:

a) kredittinstitusjoner,
b) betalingsforetak, inkludert betalingsforetak som er unntatt i henhold til direktiv (EU) 2015/2366,
c) opplysningsfullmektige,
d) e-pengeforetak, inkludert e-pengeforetak som er unntatt i henhold til direktiv 2009/110/EF,
e) verdipapirforetak,
f) tilbydere av tjenester knyttet til kryptoverdier,
g) verdipapirsentraler,
h) sentrale motparter,
i) handelsplasser,
j) transaksjonsregistre,
k) forvaltere av alternative investeringsfond,
l) forvaltningsselskaper,
m) leverandører av datarapporteringstjenester,
n) forsikrings- og gjenforsikringsforetak,
o) forsikringsformidlere, gjenforsikringsformidlere og tilknyttede forsikringsformidlere,
p) pensjonsforetak,
q) kredittvurderingsbyråer,
r) administratorer av kritiske referanseverdier,
s) tjenesteleverandører for folkefinansiering,

t) verdipapiriseringsregistre og
u) tredjepartstilbydere av IKT-tjenester.

Med unntak av tredjepartstilbydere av IKT-tjenester som nevnt i bokstav u, brukes samlebetegnelsen «finansielle foretak» om de som omfattes av forordningen. Etter artikkel 2 nr. 3 er følgende foretak unntatt fra forordningskravene:

a) forvaltere av alternative investeringsfond som nevnt i direktiv 2011/61/EU artikkel 3 nr. 2,
b) forsikrings- og gjenforsikringsforetak som nevnt i direktiv 2009/138/EF artikkel 4,
c) pensjonsforetak som forvalter ordninger som til sammen ikke har flere enn 15 medlemmer,
d) fysiske og juridiske personer som er unntatt i henhold til direktiv 2014/65/EU artikkel 2 og 3,
e) forsikringsformidlere, gjenforsikringsformidlere og tilknyttede forsikrings-formidlere som er mikroforetak eller små eller mellomstore foretak, og
f) postgiroinstitusjoner som nevnt i direktiv 2013/36/EU artikkel 2 nr. 5 (3).

Medlemsstatene kan dessuten etter artikkel 2 nr. 4 unnta foretak som nevnt i direktiv 2013/36/EU artikkel 2 nr. 5 punkt 4 til 23 (navngitte enkeltforetak i EU-land).

Forordningen artikkel 3 inneholder definisjoner.

Etter forordningen artikkel 4 skal foretakene gjennomføre forordningsreglene om risikostyring i samsvar med proporsjonalitetsprinsippet, og da ta hensyn til foretakets størrelse og samlede risikoprofil, samt virksomhetens type, omfang og kompleksitet. Anvendelsen av øvrige forordningsregler skal dessuten stå i et rimelig forhold til foretakets størrelse og samlede risikoprofil, samt virksomhetens type, omfang og kompleksitet, i tråd med spesifikke bestemmelser om dette i de ulike delene av forordningen. Tilsynsmyndigheten skal ta hensyn til proporsjonalitet i oppfølgingen av foretakene.

3.1.2 Risikostyring

Forordningen kapittel II inneholder krav til risikostyring. Etter artikkel 5 nr. 1 skal foretakene ha et overordnet rammeverk for styring og kontroll som sikrer en effektiv og forsvarlig styring av IKT-risiko for å oppnå et høyt nivå av digital operasjonell motstandsdyktighet. Rammeverket for IKT-risikostyringen skal etter nr. 2 fastsettes, godkjennes og overvåkes av foretakets ledelsesorgan. Ledelsesorganet er definert i artikkel 3 nr. 30 ved henvisninger til annet regelverk, hovedsakelig slik at det vises til organet som har ansvaret for å utarbeide foretakets strategi og overordnede mål og overvåke ledelsens beslutninger, som i norsk kontekst vil være styret. Styret skal videre bl.a. innføre retningslinjer for beskyttelse og tilgjengelighet av data, fastsette roller og ansvarsområder, fastsette en overordnet strategi og nivå for risikotoleranse, godkjenne ulike planverk, fastsette et passende budsjett og godkjenne og jevnlig revidere retningslinjer for bruk av IKT-leverandører. Styret skal også etablere rapporteringskanaler for å holde seg orientert om bruken av IKT-leverandører, planlagte endringer og den potensielle innvirkningen av disse på foretakets kritiske og viktige funksjoner. Med unntak av mikroforetak skal foretakene etter artikkel 5 nr. 3

også ha en funksjon for overvåking leveranser fra IKT-leverandører, alternativt utpeke et medlem av ledelsen som skal ha ansvar for å følge opp risikoeksponering og dokumentasjon forbundet med leveransen. Styremedlemmene skal dessuten etter nr. 4 holde seg oppdatert med tilstrekkelig kunnskap og ferdigheter for å kunne forstå og vurdere IKT-risikoen og dens betydning for virksomheten, herunder gjennom jevnlig deltakelse på kurs.

Artikkel 6 stiller nærmere krav til rammeverket for IKT-risikostyringen, som skal sette foretaket i stand til å håndtere IKT-risiko raskt, effektivt og helhetlig. Det stilles bl.a. krav til strategier, retningslinjer og prosedyrer foretakene skal ha for forskjellige deler av IKT-virksomheten, hvor ofte rammeverket skal gjennomgås og krav til internrevisjon. Artikkel 7 stiller krav til IKT-systemer og verktøy foretaket skal bruke for å håndtere risiko, bl.a. at de skal være tilpasset virksomheten, pålitelige og ha tilstrekkelig kapasitet. Artikkel 8 gir regler om hvordan foretaket skal identifisere, klassifisere og dokumentere IKT-relaterte funksjoner og avhengigheter, og løpende identifisere alle kilder til IKT-risiko. Etter artikkel 9 skal foretaket løpende overvåke sikkerheten og virkemåten til IKT-systemene, og ha på plass passende sikkerhetsverktøy, retningslinjer og prosedyrer for å beskytte systemene og kunne respondere med nødvendige tiltak. Etter artikkel 10 skal foretaket ha mekanismer for rask deteksjon av unormal aktivitet, herunder ytelsesproblemer og IKT-hendelser, samt avdekke vesentlige «single points of failure».

Etter artikkel 11 skal foretaket ha helhetlige retningslinjer for IKT-driftsstabilitet, og i tråd med disse ha passende og veldokumenterte ordninger, planer, prosedyrer og mekanismer. Herunder skal foretaket ha, vedlikeholde og jevnlig teste kontinuitetsplaner for IKT-virksomheten, særlig for kritiske eller viktige funksjoner som er utkontraktert til IKT-leverandører. Det skal foretas en forretningskonsekvensanalyse av alvorlige driftsforstyrrelser på basis av relevante data og scenarioanalyser, og denne skal ligge til grunn bl.a. for sikring av redundans i alle kritiske komponenter. Verdipapirsentraler skal oversende resultatene av kontinuitetstesting til tilsynsmyndigheten. Alle foretak (bortsett fra mikroforetak) skal på forespørsel fra tilsynsmyndigheten innrapportere et anslag på årlige kostnader og tap som følge av alvorlige IKT-hendelser.

Etter artikkel 12 skal foretaket ha retningslinjer, prosedyrer og metoder for gjenoppretting av IKT-systemer og data etter en hendelse. Gjenopprettingen skal skje med minimal nedetid og begrensede forstyrrelser og tap. Det er nærmere bestemmelser om prosedyrer for hvordan gjenoppretting skal skje og hvilke krav som stilles til løsninger, og for verdipapirsentraler stilles det bl.a. krav til minst ett sekundært datasenter som må tilfredsstille flere kriterier.

Etter artikkel 13 skal foretaket ha ressurser og ansatte for å samle informasjon om sårbarheter, cybertrusler og IKT-hendelser, og analysere hvordan de kan påvirke foretakets digitale operasjonelle motstandsdyktighet. Videre skal foretakene evaluere større IKT-hendelser ved å analysere årsaker og identifisere nødvendige forbedringer i IKT-driften eller kontinuitetsplaner, og på forespørsel fra tilsynsmyndigheten skal foretakene (bortsett fra mikroforetak) innrapportere gjennomførte endringer. Erfaringer fra tester, virkelige hendelser og annet skal inntas i foretakets risiko-

vurderingsprosess, og IKT-ledelsen skal minst årlig rapportere til styret om funn og anbefalinger. Det er også krav om overvåking av effektiviteten til strategien for digital motstandsdyktighet, intern opplæring for ansatte og vurdering av teknologiutviklingen.

Etter artikkel 14 skal foretaket ha planer for krisekommunikasjon, både internt og eksternt, med rutiner for hvordan kommunikasjonen skal foregå.

Artikkel 15 gir hjemler for EU-kommisjonen til å fastsette tekniske standarder for å harmonisere verktøy, metoder, prosesser og retningslinjer for IKT-risikostyring.

Etter artikkel 16 gjelder ikke reglene om risikostyring i artikkel 5 til 15 for:

a) små og ikke-sammenkoblede verdipapirforetak,
b) betalingsforetak som er unntatt i henhold til direktiv (EU) 2015/2366,
c) foretak som nevnt i direktiv 2013/36/EU artikkel 2 nr. 5 punkt 4 til 23 og som medlemsstatene ikke har unntatt etter forordningen artikkel 2 nr. 4,
d) e-pengeforetak som er unntatt i henhold til direktiv 2009/110/EF, og
e) små pensjonsforetak.

Disse foretakene skal isteden følge regler i artikkel 16 om et forenklet rammeverk for IKT-risikostyring.

3.1.3 Hendelseshåndtering

Forordningen kapittel III inneholder krav til håndtering, klassifisering og rapportering av IKT-hendelser. Etter artikkel 17 skal foretakene etablere en prosess for å avdekke, håndtere og varsle om IKT-hendelser. Foretakene skal loggføre alle IKT-hendelser og alvorlige cybertrusler, samt ha prosedyrer for overvåkning, håndtering og oppfølging, slik at rotårsaken identifiseres, dokumenteres og håndteres for å forhindre at det gjentar seg. Det er nærmere regler om håndteringsprosessen, bl.a. om å ha tidligvarslingsindikatorer, kommunikasjonsplaner og tiltak for å dempe virkninger og sikre rask gjenoppretting. Hendelser skal klassifiseres etter nærmere kriterier i artikkel 18, bl.a. basert på antall berørte kunder mv., varighet, datatap, kritikaliteten til berørte tjenester og økonomiske konsekvenser.

Artikkel 19 nr. 1 til 5 gjelder foretakets rapportering og informasjon om hendelser. Foretaket skal etter nr. 1 rapportere til tilsynsmyndigheten om alle alvorlige IKT-hendelser, som i artikkel 3 nr. 10 er definert som hendelser med stor negativ innvirkning på nettverks- og informasjonssystemer som understøtter foretakets kritiske eller viktige funksjoner. Foretaket skal i henhold til artikkel 19 nr. 4 først gi en innledende rapport, så én eller flere foreløpige rapporter når hendelsen eller håndteringen av den endrer seg vesentlig eller tilsynsmyndigheten ber om en oppdatering, og til slutt en endelig rapport når rotårsaksanalysen og data for faktiske virkninger foreligger. Rapportene skal inneholde alle opplysninger som er nødvendige for at tilsynsmyndigheten skal kunne vurdere betydningen av hendelsen og mulige grenseoverskridende virkninger. Når det oppstår alvorlige hendelser som påvirker kundenes finansielle interesser, skal foretaket uten unødig opphold dessuten informere kundene om hendelsen og iverksatte tiltak, jf. artikkelen nr. 3. Etter nr. 5 kan foretakene innenfor relevant EØS-regelverk og nasjonal lovgivning utkontraktere rapporteringsforpliktelsene til en tjenesteleverandør, men foretaket vil likevel være ansvarlig for etterlevelsen av forpliktelsene.

Etter artikkel 19 nr. 1 sjette ledd kan medlemsstatene fastsette at noen eller alle finansielle foretak også skal rapportere til nasjonale tilsynsmyndigheter eller responsmiljøer utpekt etter NIS2-direktivet (se boks 3.2 under). Etter nr. 2 kan dessuten foretakene på frivillig basis innrapportere til finanstilsynsmyndigheten vesentlige cybertrusler som foretaket mener er relevante for finanssystemet, tjenestebrukere eller kunder, og medlemsstatene kan fastsette slik rapportering også skal gå til responsmiljøer utpekt etter NIS2-direktivet.

Når finanstilsynsmyndigheten mottar rapporter om alvorlige IKT-hendelser, skal den informere relevante europeiske myndigheter, jf. artikkel 19 nr. 6, herunder den relevante felleseuropeiske finanstilsynsmyndigheten, nasjonale tilsynsmyndigheter eller responsmiljøer utpekt etter NIS2-direktivet, og ev. nasjonale krisehåndteringsmyndigheter. Myndighetene skal deretter etter nr. 7 vurdere om hendelsen er relevant for tilsynsmyndigheter i andre medlemsstater, og i tilfelle informere de aktuelle myndighetene slik at de kan treffe nødvendige tiltak for å beskytte den finansielle stabiliteten. For hendelser i verdipapirsentraler skal tilsynsmyndigheten umiddelbart informere tilsynsmyndigheter bl.a. i land der sentralen har vesentlig aktivitet, jf. nr. 8.

Artikkel 20 gir hjemler for EU-kommisjonen til å fastsette tekniske standarder for å harmonisere rapporteringen av IKT-hendelser. Etter artikkel 21 skal de felleseuropeiske finanstilsynsmyndighetene m.fl. utarbeide en rapport med vurdering av mulighetene for ytterligere sentralisering av foretakenes hendelsesrapportering gjennom opprettelse av et felleseuropeisk innsamlingspunkt.

Etter artikkel 22 skal tilsynsmyndigheten følge opp innrapporterte hendelser med mottaksbekreftelse, samt gi forholdsmessig tilbakemelding og ev. veiledning om relevante tiltak og hvordan virkningene i resten av sektoren kan minimeres.

Etter artikkel 23 gjelder forordningen kapittel III om hendelsesrapportering også for betalingsrelaterte operasjonelle eller sikkerhetsmessige hendelser hos kredittinstitusjoner, betalingsforetak, opplysningsfullmektiger og e-pengeforetak.

3.1.4 Test av motstandsdyktighet

Forordningen kapittel IV inneholder krav til testing av den digitale operasjonelle motstandsdyktigheten i foretakene. Etter artikkel 24 skal foretakene (bortsett fra mikroforetak) ha et helhetlig program for risikobaserte tester som en del av rammeverket for IKT-risikostyringen. Formålet er å vurdere beredskapen for håndtering av IKT-hendelser og avdekke svakheter, mangler og avvik i den digitale motstandsdyktigheten, samt gi grunnlag for raskt å gjennomføre forbedringstiltak. Testene skal gjennomføres av uavhengige parter, enten interne eller eksterne, og foretaket skal ha prosedyrer og rutiner for å prioritere, klassifisere og rette avdekkede feil, samt metoder for intern validering for å sikre at alle avdekkede svakheter, mangler og avvik følges opp. IKT-systemer og applikasjoner som understøtter kritiske eller viktige funksjoner, skal testes minst årlig.

Etter artikkel 25 skal testprogrammet legge til rette for hensiktsmessige tester, så som sårbarhetsvurderinger og -skanninger, «open source»-analyser, nettverkssikkerhetsvurderinger, mangelanalyser, fysiske sikkerhetsgjennomganger, spørreskjemaer og skanningsprogramvareløsninger, gjennomgang av kildekode, scenariobaserte tester,

kompatibilitetstester, ytelsestester, ende-til-ende-tester og penetrasjonstester. For verdipapirsentraler og sentrale motparter er det et eget krav om å gjennomføre sårbarhetsvurderinger før applikasjoner og infrastrukturkomponenter tas i bruk, samt før bruk av IKT-tjenester som understøtter kritiske eller viktige funksjoner. Mikroforetak skal også gjennomføre hensiktsmessige tester, og da ved å kombinere en risikobasert tilnærming med strategisk planlegging av IKT-tester, samt balansere ressursbruken mot risikobildet.

Etter artikkel 26 nr. 8 tredje ledd skal tilsynsmyndigheten identifisere hvilke foretak som skal ha krav om å gjennomføre mer avansert testing i form av trusselbasert penetrasjonstesting («threat-led penetration test», TLPT). I tillegg til å ta hensyn til proporsjonalitet, skal tilsynsmyndigheten basere sin vurdering på foretakets betydning for finanssektoren og finansiell stabilitet på nasjonalt og europeisk nivå, samt foretakets IKT-risikoprofil. Foretakene som identifiseres, skal gjennomføre TLPT minst hvert tredje år, eller oftere hvis tilsynsmyndigheten vurderer det som nødvendig, jf. artikkel 26 nr. 1. Hver TLPT skal etter nr. 2 dekke flere eller alle kritiske eller viktige funksjoner, og foretaket skal gjøre en kartlegging for å fastsette det konkrete omfanget, som skal valideres av tilsynsmyndigheten. Nr. 3 og 4 gir nærmere regler om IKT-leverandørers deltakelse i testingen, og åpner også for at IKT-leverandøren etter avtale gjennomfører en samlet TLPT for leveranser til flere foretak. Testingen skal uansett skje med tilstrekkelige risikostyringstiltak for å dempe risikoen for skadevirkninger, jf. nr. 5. Når en TLPT er gjennomført, skal foretaket oversende sammendrag av funn, forbedringsplaner og dokumentasjon til den ansvarlige myndigheten, som deretter skal gi en attest på at testen er korrekt gjennomført, jf. nr. 6 og 7. Attesten skal gi grunnlag for gjensidig anerkjennelse av testen mellom ulike tilsynsmyndigheter. Den ansvarlige myndigheten for TLPT er tilsynsmyndigheten, med mindre det bestemmes noe annet nasjonalt, jf. nr. 9 og 10. Nr. 11 gir hjemler for EU-kommisjonen til å fastsette tekniske standarder for TLPT i samsvar med TIBER-rammeverket fra Den europeiske sentralbanken (ESB), se boks 3.1.

Boks 3.1: TIBER-rammeverket

Den europeiske sentralbanken (ESB) fastsatte i 2018 et rammeverk for å teste finansielle foretaks evne til å oppdage, beskytte seg mot og reagere på avanserte cyberangrep, kalt TIBER-EU («threat intelligence-based ethical red teaming»). TIBER-EU er en form for trusselbasert penetrasjonstesting (TLPT), jf. at noen foretak etter DORA vil få krav om å gjennomføre TLPT jevnlig. Noen av de nærmere reglene om TLPT skal utarbeides i samsvar TIBER-EU.

Nasjonale versjoner av TIBER-EU er innført i flere europeiske land, også i Norge. TIBER-NO er utarbeidet av Finanstilsynet og Norges Bank i dialog med finansnæringen og andre relevante myndigheter, og de første testene startet høsten 2022. TIBER-tester skal etterligne reelle angrep og gi innsikt om sårbarheter for det enkelte foretak og sårbarheter som kan få systemiske konsekvenser og betydning for finansiell stabilitet. Et standardisert oppsett for testingen skal bidra til kvalitet og til at testresultatene kan sammenlignes, også på tvers av land.

Artikkel 27 stiller krav til testerne som skal gjennomføre TLPT, bl.a. knyttet til egnethet, kapasitet, ekspertise, sertifisering og forsikringsdekning. For bruk av interne testere er det i tillegg krav om myndighetsgodkjenning og at leverandøren av etterretningsinformasjon er ekstern, mens det for bruk av eksterne testere er krav om forsvarlig forvaltning av testresultatene mv. Etter artikkel 26 nr. 8 første ledd er det dessuten krav om at foretak som bruker interne testere skal bruke eksterne testere til hver tredje test.

3.1.5 Avtaler om bruk av IKT-tjenester

Forordningen kapittel V del I inneholder regler om foretakenes håndtering av risiko forbundet med bruk av tjenester fra IKT-leverandører. Etter artikkel 28 nr. 1 skal slik leverandørstyring inngå som en del av rammeverket for IKT-risikostyring, basert på prinsipper om proporsjonalitet og foretakets ansvar uavhengig av utkontraktering. Bortsett fra mikroforetak, skal alle foretak ha en strategi for leverandørrisiko som oppfyller nærmere krav, jf. nr. 2. Etter nr. 3 skal alle foretak ha et register med oversikt over bruk av tjenester fra IKT-leverandører og hvilke av tjenestene som understøtter kritiske eller viktige funksjoner, og på forespørsel gjøre registeret tilgjengelig for tilsynsmyndigheten. Foretakene skal minst årlig rapportere til tilsynsmyndigheten om nye avtaler som er inngått, og i tillegg informere myndigheten i rimelig tid om planlagte avtaler om IKT-tjenester som vil understøtte kritiske eller viktige funksjoner, samt når en funksjon har blitt kritisk eller viktig.

Før et foretak inngår avtale med en IKT-leverandør, må foretaket ha gjort en rekke vurderinger og undersøkelser knyttet til leverandøren, og det kan bare inngås avtaler med leverandører som etterlever hensiktsmessige informasjonssikkerhetsstandarder, jf. artikkel 28 nr. 4 og 5. Foretakene skal ha en risikobasert tilnærming til bruk av tilgang, inspeksjon og revisjon hos leverandøren, hvor hyppigheten av revisjoner og inspeksjoner, samt hvilke områder som skal revideres, skal være forhåndsdefinert, jf. nr. 6. Når avtalen innebærer en høy teknisk kompleksitet, er det særlige krav til revisjonen. Foretaket skal i visse definerte tilfeller kunne si opp avtalen med leverandøren, og for avtaler om tjenester som understøtter kritiske eller viktige funksjoner skal foretaket ha en uttredelsesstrategi som sikrer at det kan si opp avtalen uten at det gir forstyrrelser i virksomheten, jf. nr. 7 og 8. Nr. 9 og 10 gir hjemler for EU-kommisjonen til å fastsette tekniske standarder med nærmere krav.

Før et foretak inngår en avtale om IKT-tjenester som vil understøtte kritiske eller viktige funksjoner, skal foretaket etter artikkel 29 vurdere om IKT-leverandøren vil være vanskelig å erstatte eller om flere av leveransene til foretaket vil bli konsentrert hos samme leverandør (eller samarbeidende leverandører). Foretakene skal også gjøre en kost-nytte-vurdering av alternative løsninger, så som bruk av andre leverandører. Dersom det er mulig at leverandøren videreutkontrakterer leveranser, skal foretaket gjøre en kost-risiko-vurdering, særlig når det gjelder underleverandører i tredjeland, samt ta stilling til om avtalen innebærer lange eller komplekse verdikjeder som kan svekke mulighetene for overvåking og tilsyn. Foretaket skal også vurdere betydningen av regelverk for insolvens og databeskyttelse som gjelder for leverandøren.

Artikkel 30 stiller krav til utforming av avtaler med IKT-leverandører, bl.a. knyttet til fullstendige beskrivelser av leveransene, krav til tjenestekvalitet, samarbeid med tilsynsmyndigheten, overvåking, oppsigelse og rapporteringskrav. For tjenester som vil understøtte kritiske eller viktige funksjoner, er det særlige krav til utforming av avtalen. I kontraktsforhandlingene skal foretaket vurdere bruk av standard kontraktsbestemmelser utarbeidet av offentlige myndigheter. EU-kommisjonen har hjemler til å fastsette tekniske standarder med nærmere krav til avtalene.

3.1.6 Overvåking av IKT-leverandører

Forordningen kapittel V del II inneholder regler om myndighetsovervåking av kritiske IKT-leverandører. Etter artikkel 31 nr. 1 skal de tre felleseuropeiske tilsynsmyndighetene (EBA, EIOPA og ESMA) sammen utpeke IKT-leverandører som er kritiske for finansielle foretak, og for hver av dem oppnevne en av de felleseuropeiske tilsynsmyndighetene som hovedovervåker, basert på hvilken finanssektor som i størst grad benytter seg av leverandørens tjenester. Kritiske IKT-leverandører skal utpekes på grunnlag av anbefalinger fra et overvåkingsforum som skal etableres etter artikkel 32 (se nedenfor), og i tråd med følgende kriterier i artikkel 31 nr. 2:

a) de systemiske konsekvensene for stabilitet, kontinuitet eller kvalitet i den finansielle tjenesteytingen ved en større operasjonell svikt hos IKT-leverandøren,

b) den systemiske karakteren eller viktigheten av de finansielle foretakene som er avhengige av IKT-leverandøren, vurdert bl.a. ut fra antall systemviktige finansforetak som er avhengig av leveransene,

c) finansielle foretaks avhengighet av IKT-leverandøren i produksjonen av kritiske eller viktige funksjoner, og

d) i hvilken grad IKT-leverandøren kan erstattes, herunder som følge av mangel på reelle alternativer og vanskeligheter med å flytte data og produksjon til en ny IKT-leverandør.

IKT-leverandører som inngår i konsern, skal vurderes ut fra konsernets betydning, og slike ev. kritiske leverandører skal ha ett kontaktpunkt for kommunikasjonen med hovedovervåkeren, jf. nr. 3 og 4. Etter nr. 5 skal hovedovervåkeren varsle en IKT-leverandør som vurderes som kritisk, og leverandøren kan innen seks uker oversende en erklæring med alle relevante opplysninger for vurderingen. Hovedovervåkeren kan deretter be om ytterligere opplysninger innen 30 dager. Når en kritisk IKT-leverandør er utpekt, skal de felleseuropeiske tilsynsmyndighetene varsle leverandøren om utpekingen og virkningsdatoen for overvåkingen, mens leverandøren skal varsle de aktuelle foretakene. EU-kommisjonen skal etter nr. 6 fastsette nærmere kriterier for utpeking av kritiske IKT-leverandører innen 17. juli 2024, og etter nr. 7 skal ingen utpekes før dette er gjort. Etter nr. 8 kan visse IKT-leverandører ikke utpekes som kritiske, bl.a. konserninterne IKT-leverandører og IKT-leverandører som bare leverer tjenester til foretak i én medlemsstat. De felleseuropeiske tilsynsmyndighetene skal etter nr. 9 årlig publisere en liste over kritiske IKT-leverandører, mens nasjonale tilsynsmyndigheter etter nr. 10 skal avgi en årlig rapport til overvåkingsforumet om foretakenes IKT-avhengigheter. IKT-leverandører som ikke utpekes som kritiske, kan

imidlertid etter nr. 11 søke om å bli det. Etter nr. 12 kan foretak bare fortsette å bruke kritiske IKT-leverandører etablert i tredjeland hvis leverandøren innen 12 måneder etablerer et datterforetak i EU, og slike leverandører skal dessuten etter nr. 13 varsle hovedovervåkeren om ev. endringer i ledelsesstrukturen i datterforetaket.

Overvåkingsforumet skal etter artikkel 32 nr. 1 etableres av de felleseuropeiske tilsynsmyndighetene for å støtte arbeidet med IKT-leverandørrisiko på tvers av finanssektorer, og ha i oppgave å forberede vedtak og drøfte utviklingstrekk. Forumet skal etter nr. 2 også gjøre en felles årlig vurdering av overvåkingsaktivitetene, bidra til koordinering, god håndtering av konsentrasjonsrisiko og utforsking av tiltak mot risikosmitte på tvers av sektorer, samt etter nr. 3 foreslå helhetlige referanseverdier for kritiske IKT-leverandører. Overvåkingsforumet skal etter nr. 4 bestå av styrelederne for de tre felleseuropeiske tilsynsmyndighetene og en representant på høyt nivå fra hver av de nasjonale tilsynsmyndighetene. Direktørene for de tre felleseuropeiske tilsynsmyndighetene, samt representanter fra EU-kommisjonen, Det europeiske systemrisikorådet (ESRB), ESB og Det europeiske byrået for nettverks- og informasjonssikkerhet (ENISA), skal være observatører. Nr. 5 til 9 omhandler oppnevninger, bruk av eksperter, arbeidsdeling mellom myndigheter mv.

Etter artikkel 33 skal hovedovervåkeren vurdere om den kritiske IKT-leverandøren har helhetlige, forsvarlige og effektive regler, prosedyrer, mekanismer og ordninger for å håndtere IKT-risikoen som de kan utsette finansielle foretak for. Hovedovervåkeren skal på grunnlag av denne vurderingen fastsette en klar, detaljert og begrunnet individuell overvåkingsplan, som beskriver årlige mål og planlagte tiltak. Når IKT-leverandøren har mottatt utkast til en slik plan, kan den innen 15 dager sende inn en erklæring som dokumenterer forventet virkning på ikke-finansielle kunder, og ev. utarbeide løsninger for å dempe risikoen. Etter artikkel 34 skal de felleseuropeiske tilsynsmyndighetene samarbeide og koordinere utøvelsen av rollen som hovedovervåker.

Etter artikkel 35 nr. 1 skal hovedovervåkeren ha myndighet til å:

a) kreve at IKT-leverandøren legger frem all informasjon som er nødvendig for at hovedovervåkeren skal kunne ivareta sine oppgaver etter forordningen, herunder forretningsdokumenter eller operasjonelle dokumenter, kontrakter, retningslinjer, dokumentasjon, revisjonsrapporter, hendelsesrapporter og informasjon knyttet til parter som IKT-leverandøren har utkontraktert funksjoner eller aktiviteter til, jf. nærmere regler i artikkel 37,

b) gjennomføre generelle undersøkelser og inspeksjoner hos IKT-leverandøren etter nærmere regler i artikkel 38 til 40,

c) kreve rapporter fra IKT-leverandøren om oppfølging av anbefalinger, jf. under, og

d) gi anbefalinger til IKT-leverandøren, særlig om sikkerhetskrav og -prosesser, betingelser og vilkår for leveransen av tjenester til finansielle foretak, planlagt utkontraktering og ev. anbefaling om å avstå fra utkontraktering i visse tilfeller.

Artikkel 35 nr. 2 til 5 gjelder koordinering og informasjon mellom myndigheter, IKT-leverandørens rett til å legge frem en konsekvensanalyse for ikke-finansielle kunder

og IKT-leverandørens plikt til å samarbeide med hovedovervåkeren. Etter nr. 6 til 11 skal hovedovervåkeren gi IKT-leverandøren dagbøter ved manglende eller delvis manglende etterlevelse av krav om informasjon, rapporter eller tilrettelegging for undersøkelser og inspeksjoner, dersom forholdene ikke er rettet innen 30 dager etter at det er gitt pålegg om retting. Nivået på dagbøtene skal fastsettes ut fra alvorlighetsgrad og opptil et beløp tilsvarende 1 pst. av gjennomsnittlig daglig omsetning i foregående år, og kan kreves i opptil seks måneder. Artikkel 36 gjelder de felleseuropeiske tilsynsmyndighetenes mulighet for å utøve myndighet i tredjeland, i den grad en kritisk IKT-leverandør har virksomhet der for å levere tjenester i EU.

De nærmere reglene om undersøkelser og inspeksjoner i artikkel 38 til 40 angir bl.a. hva og hvem hovedovervåkeren skal ha tilgang til hos IKT-leverandøren, herunder informasjon, representanter og lokaler, samt krav om at hovedovervåkeren skal varsle IKT-leverandøren og relevante tilsynsmyndigheter. Ved undersøkelser og inspeksjoner skal hovedovervåkeren bistås av en felles undersøkelsesgruppe som skal opprettes for hver kritiske IKT-leverandør. Gruppen skal bestå av medarbeidere fra de felleseuropeiske tilsynsmyndighetene og de nasjonale tilsynsmyndighetene som fører tilsyn med finansielle foretak som benytter seg av leverandøren. I tillegg kan en nasjonal finanstilsynsmyndighet i landet der IKT-leverandøren er etablert, samt den nasjonale tilsynsmyndigheten etablert etter NIS2-direktivet i samme land, delta på frivillig basis. Hovedovervåkeren skal innen tre måneder etter en undersøkelse eller inspeksjon gi anbefalinger til IKT-leverandøren. Artikkel 41 gir hjemmel for EU-kommisjonen til å fastsette tekniske standarder for informasjon fra IKT-leverandører, sammensetning av felles undersøkelsesgrupper og nasjonale tilsynsmyndigheters vurdering av IKT-leverandørers oppfølging av anbefalinger, jf. artikkel 42.

Artikkel 42 gjelder i hovedsak de nasjonale tilsynsmyndighetenes oppfølging av finansielle foretak. Innen 60 dager etter å ha mottatt anbefalinger fra hovedovervåkeren skal IKT-leverandøren etter artikkelen nr. 1 bekrefte at den vil følge anbefalingene eller forklare hvorfor den ikke vil følge dem, og hovedovervåkeren skal videreformidle denne informasjonen til de nasjonale tilsynsmyndighetene for de berørte finansielle foretakene. Dersom tilsynsmyndigheten i sin løpende oppfølging av et foretak vurderer at det ikke i tilstrekkelig grad håndterer risikoen som er identifisert i anbefalinger til IKT-leverandøren, skal tilsynsmyndigheten varsle foretaket om det. Dersom foretaket ikke treffer nødvendige tiltak innen 60 dager, kan tilsynsmyndigheten etter nr. 6 pålegge foretaket å suspendere eller si opp hele eller deler av avtalen med IKT-leverandøren, men skal etter nr. 8 gi foretaket nok tid til å tilpasse avtalen eller iverksette uttredelsesstrategien eller overgangsplaner. Etter nr. 2 skal hovedovervåkeren offentliggjøre informasjon om IKT-leverandører med mangelfulle svar på anbefalinger, og dersom en IKT-leverandør avviker fra anbefalingene på en måte som kan ha betydelige skadevirkninger for finansiell stabilitet, kan hovedovervåkeren etter nr. 7 gi ikke-bindende og ikke-offentlige uttalelser til nasjonale tilsynsmyndigheter for å bidra til konsistente og konvergerende tiltak overfor foretakene.

Etter artikkel 43 skal hovedovervåkeren innkreve en overvåkingsavgift fra kritiske IKT-leverandører. Avgiften skal dekke alle utgifter knyttet til overvåkingen, og EU-

kommisjonen skal fastsette nærmere regler om størrelsen på avgiften og hvordan den skal betales.

Etter artikkel 44 kan de felleseuropeiske tilsynsmyndighetene etablere samarbeid med myndigheter i tredjeland, bl.a. om praksis for IKT-risikohåndtering, tiltak og hendelseshåndtering.

3.1.7 Informasjonsdeling mellom foretak

Etter forordningen kapittel VI (artikkel 45) kan finansielle foretak utveksle informasjon og etterretning om cybertrusler, forutsatt at utvekslingen:

a) har som mål å forbedre foretakenes motstandsdyktighet, særlig ved å øke bevisstheten om cybertrusler, begrense eller hindre spredning av trusler og understøtte forsvarskapasitet, deteksjonsteknikker, tiltaksstrategier eller innsats- og gjenoppretningsfaser,

b) foregår innenfor et betrodd fellesskap av finansielle foretak, og

c) gjennomføres i ordninger som beskytter potensielt sensitiv informasjon og er omfattet av regler om forretningsmessig konfidensialitet, beskyttelse av personopplysninger og retningslinjer for konkurransepolitikk.

Slike informasjonsutvekslingsordninger skal ha bestemmelser om deltakelse fra finansielle foretak og ev. også fra myndigheter og IKT-leverandører mv. Finansielle foretak skal informere tilsynsmyndigheten om deltakelse i slike ordninger.

3.1.8 Tilsyn og myndighetssamarbeid

Forordningen kapittel VII gjelder nasjonale tilsynsmyndigheter på finansmarkeds-området, samt samarbeid mellom myndigheter på europeisk nivå.

Artikkel 46 angir hvilke tilsynsmyndigheter som i samsvar med annet EU-regelverk skal ha ansvar for tilsynet med de ulike foretakstypenes etterlevelse av forordningen. Etter artikkel 50 skal tilsynsmyndigheten ha alle nødvendige hjemler for å kunne føre tilsyn med foretakenes etterlevelse av forordningen, herunder myndighet til å få utlevert dokumentasjon, foreta stedlig tilsyn og kreve korrigerende og gjenopp-rettende tiltak for avdekkede regelbrudd. Tilsynsmyndigheten skal også kunne ilegge administrative sanksjoner, som skal være effektive, proporsjonale og avskrekkende. Som et minimum skal tilsynsmyndigheten kunne gi pålegg om retting eller stans av atferd eller praksis, overtredelsesgebyr, kreve utlevering av datatrafikklogger og publisere vedtak der identiteten til foretaket og regelbruddets karakter fremgår. Etter artikkel 51 skal tilsynsmyndigheten ilegge administrative sanksjoner i henhold til nasjonal lovgivning, og i valget av type og nivå ta hensyn til om bruddet var forsettlig eller skyldes uaktsomhet. Det skal også legges vekt på bl.a. bruddets alvorlighets-grad, graden av ansvar for bruddet, foretakets finansielle styrke, gevinster og tap hos foretaket og tredjeparter, graden av samarbeid med tilsynsmyndigheten og tidligere brudd. Etter artikkel 52 kan medlemsstatene velge å ikke ha regler om administrative sanksjoner for regelverksbrudd som er gjenstand for straffesanksjoner. Tilsyns-myndigheten skal etter artikkel 54 publisere vedtak om administrative reaksjoner, inkludert identiteten til foretaket og informasjon om regelbruddet. Dersom publisering

av identiteten vil være uforholdsmessig og ha skadevirkninger, kan myndigheten utsette publisering, anonymisere eller avstå fra å publisere (på visse vilkår). Artikkel 55 og 56 gjelder taushetsplikt og behandling av persondata. Nasjonalt regelverk som gjennomfører forordningen kapittel VII, skal etter artikkel 53 notifiseres til EU-kommisjonen og de felleseuropeiske tilsynsmyndighetene.

Boks 3.2: Digitalsikkerhetsloven og NIS2-direktivet

Stortinget vedtok i desember 2023 en ny lov om digital sikkerhet (digitalsikkerhetsloven), jf. Innst. 78 L (2023-2024) og Prop. 109 LS (2022–2023). Loven legger til rette for gjennomføring av direktiv (EU) 2016/1148 om sikkerhet i nettverks- og informasjonssystemer (NIS-direktivet). Loven forplikter virksomheter som har en særlig viktig rolle for å opprettholde kritisk samfunnsmessig og økonomisk aktivitet til å overholde sikkerhetskrav etter § 7, og etter § 8 varsle om alvorlige hendelser til det organet Kongen utpeker. Justis- og beredskapsdepartementet viser i proposisjonen til at det er etablert flere nasjonale responsmiljøer, og legger opp til å utpeke det organ som anses som mest hensiktsmessig til å motta varselet. Også når det gjelder tilsyn legges det opp til at eksisterende struktur benyttes i størst mulig grad, jf. at Kongen etter loven § 13 utpeker én eller flere tilsynsmyndigheter som skal føre tilsyn med tilbydere som omfattes av loven.

Direktiv (EU) 2022/2555 (NIS2-direktivet) ble vedtatt 14. desember 2022, og skal fra oktober 2024 erstatte NIS1-direktivet i EU. Formålet er å øke motstandsdyktigheten i nettverks- og informasjonssystemer hos private og offentlige aktører. Direktivet gjelder i utgangspunktet alle tilbydere av samfunnsviktige tjenester, inkludert bank og finansmarkedsinfrastrukturer, men det er unntak for foretak som omfattes av sektorspesifikke regelverk som DORA.

Etter NIS2-direktivet skal medlemsstatene utpeke en eller flere *tilsynsmyndigheter* som skal ha ansvar for cybersikkerhet og tilsyn med etterlevelsen av regelverket. Hvis det utpekes mer enn én myndighet, skal en av dem utpekes som et *nasjonalt kontaktpunkt* for grensekryssende samarbeid. Medlemsstatene skal også utpeke eller etablere ett eller flere *responsmiljø* («computer security incident response teams», CSIRT) for hendelseshåndtering i sektorene, enten i eller utenfor tilsynsmyndigheten(e).

For å legge til rette for strategisk samarbeid og informasjonsutveksling mellom medlemsstatene videreføres og styrkes en *samarbeidsgruppe* på europeisk nivå, først etablert etter NIS1-direktivet. Gruppen skal bestå av representanter for medlemsstatene, EU-kommisjonen og ENISA, i tillegg til at finanstilsynsmyndighetene etter DORA kan delta i visse aktiviteter. Et europeisk nettverk for de nasjonale responsmiljøene videreføres også, samtidig som det skal etableres et myndighetsnettverk for å understøtte koordinert håndtering av større IKT-hendelser («European cyber crisis liaison organisation network», EU-CyCLONe).

For å fremme samarbeid og muliggjøre tilsynsmessig utveksling med myndigheter på nettverks- og informasjonssikkerhetsområdet kan de felleseuropeiske og nasjonale finanstilsynsmyndighetene etter artikkel 47 delta i den såkalte samarbeidsgruppen etablert etter NIS2-direktivet, se boks 3.2. Finanstilsynsmyndighetene skal kunne delta i gruppens aktiviteter som berører spørsmål av relevans for tilsynet med finansielle foretak, og kan også be om å få delta i aktiviteter relatert til kritiske IKT-

leverandører. Nasjonale finanstilsynsmyndigheter kan dessuten rådføre seg og dele informasjon med sentrale kontaktpunkter og responsmiljøer etablert etter NIS2-direktivet, samt be om tekniske råd og bistand fra tilsynsmyndigheter utpekt etter det direktivet, se boksen. Disse tilsynsmyndighetene kan også etablere samarbeidsordninger seg imellom for å legge til rette for rask og effektiv koordinering.

Nasjonale finanstilsynsmyndigheter skal etter artikkel 48 samarbeide tett med hverandre og hovedovervåkeren (når det er relevant), herunder ved å utveksle all relevant informasjon om kritiske IKT-leverandører. Etter artikkel 49 kan de felleseuropeiske tilsynsmyndighetene, nasjonale tilsynsmyndigheter og krisehåndteringsmyndigheter, ESB, krisehåndteringsmyndigheten i eurosonen (SRB), ESRB og ENISA etablere ordninger for erfaringsutveksling for å forbedre situasjonsbevisstheten og identifisere felles cybersårbarheter og risiko. De skal også kunne utvikle kriseøvelser som omfatter cyberangrep, med sikte på å utvikle kommunikasjonskanaler og evne til koordinert innsats ved en grensekryssende IKT-hendelse eller -trussel som kan ha systemiske virkninger i den europeiske finanssektoren. I tråd med dette har ESRB anbefalt å etablere et europeisk rammeverk for koordinering ved systemiske cyberhendelser (EU-SCICF), se boks 3.3.

Boks 3.3: Europeisk rammeverk for koordinering ved systemiske cyberhendelser

Det europeiske systemrisikorådet (ESRB) utstedte i desember 2021 anbefaling ESRB/2021/17 om etablering av et europeisk rammeverk for koordinering ved systemiske cyberhendelser («pan-European systemic cyber incident coordination framework», EU-SCICF). Etter anbefalingen bør de felleseuropeiske tilsynsmyndighetene, ESB, ESRB og relevante nasjonale myndigheter forberede en gradvis utvikling av rammeverket i tråd med (de da forventede) kravene i DORA, herunder gjennom en analyse av legale og operasjonelle barrierer for etablering av et slikt samarbeid. Det er også anbefalt å utpeke kontaktpunkter i hvert land og for de felleseuropeiske myndighetene for utviklingsfasen og senere bruk av rammeverket. Finanstilsynet er meldt inn som kontaktpunkt for Norge.

I innledningen til anbefalingen peker ESRB bl.a. på trusselen fra cyberhendelser og at det er risiko for koordineringssvikt og inkonsistente tiltak mellom myndigheter på tvers av land og sektorer. EU-SCICF er ment å tette hull og supplere andre koordineringsordninger, slik som samarbeidsgruppen etter NIS2-direktivet. ESRB viser til at det er behov for å spesifisere hva slags informasjon som skal deles i EU-SCICF, hvilke kanaler som skal brukes og hvem som skal motta informasjonen, i tillegg til at øvelser kan bidra til utvikling av rammeverket og til at myndighetene er bedre forberedt på systemiske cyberkriser.

3.1.9 Endringer i andre forordninger

Forordningen artikkel 59 til 63 endrer en rekke andre forordninger på finansmarkedsområdet, i hovedsak ved at det tas inn henvisninger til at ulike typer foretak skal etterleve krav til risikostyring mv. i forordningen. Endringene gjøres i:

a) forordning (EF) 1060/2009 (kredittvurderingsbyråforordningen, CRA),
b) forordning (EU) 648/2012 (forordningen om OTC-derivater, sentrale motparter og transaksjonsregistre, EMIR),
c) forordning (EU) 909/2014 (verdipapirsentralforordningen, CSDR),

d) forordning (EU) 600/2014 (verdipapirmarkedsforordningen, MiFIR) og
e) forordning (EU) 2016/1011 (referanseverdiforordningen, BMR).

I tillegg endres flere direktiver, se avsnitt 3.2.

3.1.10 Avsluttende bestemmelser

Forordningen artikkel 57 gjelder EU-kommisjonens myndighet til å fastsette utfyllende regelverk. Etter artikkel 58 nr. 1 skal EU-kommisjonen innen 17. januar 2028 avgi en rapport til Parlamentet og Rådet med en revisjon av forordningen, ev. ledsaget av forslag til regelverksendringer. Kommisjonen skal herunder vurdere om forsikrings-formidlere som er unntatt etter artikkel 2 nr. 3 bokstav e, og som benytter automatiske salgssystemer, bør omfattes av forordningen. Som et ledd i revisjonen av direktiv (EU) 2015/2366 (betalingstjenestedirektivet) skal Kommisjonen også vurdere om flere av foretakene som er omfattet av det direktivet, bør omfattes av forordningen, jf. artikkel 58 nr. 2. Etter nr. 3 skal Kommisjonen innen januar 2026 vurdere om revisorer og revisjonsselskaper bør omfattes av forordningen eller tilsvarende krav i direktiv 2006/43/EF (revisjonsdirektivet).

Forordningen skal artikkel 64 gjelde fra 17. januar 2025.

3.2 Direktiv (EU) 2022/2556

Direktiv (EU) 2022/2556 ble vedtatt i EU 14. desember 2022, og skal gjelde der fra 17. januar 2025. Direktivet endrer følgende direktiver på finansmarkedsområdet:

a) direktiv 2009/65/EF (direktivet om kollektive investeringsfond, UCITS),
b) direktiv 2009/138/EF (forsikringsdirektivet, Solvens II),
c) direktiv 2011/61/EU (direktivet om forvaltning av alternative investeringsfond, AIFMD),
d) direktiv 2013/36/EU (kapitalkravsdirektivet, CRD),
e) direktiv 2014/59/EU (krisehåndteringsdirektivet, BRRD),
f) direktiv 2014/65/EU (verdipapirmarkedsdirektivet, MiFID II),
g) direktiv (EU) 2015/2366 (betalingstjenestedirektivet, PSD II) og
h) direktiv (EU) 2016/2341 (tjenestepensjonsdirektivet, IORP).

Endringene innebærer i hovedsak at det i bestemmelser om forsvarlig organisering og drift av virksomheten tas inn henvisninger til IKT-risikostyring og kravene som vil gjelde etter forordning (EU) 2022/2554 (DORA), i tillegg til endringer for å sikre konsistens med kravene og begrepsbruken i forordningen. Endringene gjelder virksomhetskravene for finansforetak, betalingsforetak, verdipapirforetak, regulerte markeder og forvaltere av verdipapirfond og alternative investeringsfond, samt justeringer i kravene til innhold i gjenopprettings- og krisehåndteringsplaner for kreditt-institusjoner mv. Direktivendringene innebærer i seg selv ingen nye materielle forpliktelser utover de som vil følge av forordningen.

4 Departementets foreløpige vurdering

4.1 Behov god regulering av IKT-risiko

Finanssektoren er i stor grad avhengig av digitale løsninger, og benytter seg i økende grad av IKT-leverandører. Større IKT-hendelser kan medføre store kostnader for det enkelte foretak og deres kunder. Dersom kritiske funksjoner rammes, kan kostnadene for andre foretak, deres kunder og samfunnet som helhet bli store. Norske foretak har over tid trappet opp sitt arbeid med IKT-sikkerhet, bl.a. for å kunne møte endringer i det digitale trusselbildet og større sårbarhetsflater. Fremover er det trolig behov for å trappe opp innsatsen ytterligere, slik også Totalberedskapskommisjonen peker på. IKT-driften blir stadig mer kompleks og konsentrert hos få leverandører, og finanssektoren er et attraktivt mål for vinningskriminalitet og cyberangrep, samtidig som nær kontinuerlig tilgang til finansielle tjenester blir viktigere for kundene. Siden de samfunnsøkonomiske konsekvensene av forstyrrelser i finanssektoren ofte er større enn de bedriftsøkonomiske kostnadene, bør en god regulering generelt føre til at foretakene har et høyere sikkerhetsnivå enn de ville valgt selv.

Norsk gjennomføring av forordning (EU) 2022/2554 (DORA) vil innebære at kravene til foretakene i den norske finanssektoren styrkes. Selv om dagens IKT-forskrift og Finanstilsynets oppfølging bygger på felleseuropeiske retningslinjer som også gjenspeiles i DORA, vil det nye regelverket gi vesentlig mer omfattende og detaljerte krav til norske foretaks risikostyring, hendelseshåndtering og bruk av IKT-leverandører. Det kan bidra til å fremme robusthet, finansiell stabilitet, trygghet for kundene og ivaretakelse av kritiske samfunnsfunksjoner. Gjennomføring av godt kjente, felleseuropeiske krav kan ha betydning for tilliten i internasjonale markeder til norske foretaks risikostyring og norske myndigheters oppfølging av finanssektoren. Regelverket legger dessuten til rette for at foretakene kan fortsette å dele informasjon og etterretning knyttet til cybertrusler og sårbarheter, slik mange norske foretak allerede gjør gjennom samhandlingen med Nordic Financial CERT.

Finansmarkedene er internasjonale, og markedene er særlig tett integrert i Norden og Europa. Den finansielle infrastrukturen og IKT-leverandørmarkedet er preget av internasjonalisering og konsolidering. En uønsket IKT-hendelse i ett foretak eller én sektor kan smitte raskt mellom foretak, sektorer og land. Den digitale motstandsdyktigheten i andre lands finanssektorer og hos internasjonalt aktive IKT-leverandører kan derfor ha stor betydning for sikkerheten og stabiliteten i det norske finanssystemet. Innføringen av DORA i Europa er et viktig tiltak for å styrke IKT-sikkerheten i et internasjonalt marked der ulike leverandører av IKT-tjenester leverer til foretak under tilsyn i flere europeiske land. Felleseuropeiske krav bl.a. til foretakenes oppfølging og kontroll med IKT-leverandører, kan bidra til økt sikkerhet i viktige betalingssystemer og gjennom det bidra til finansiell stabilitet. DORA legger også legger til rette for tettere samarbeid mellom myndighetene, både strategisk og mer operativt, som kan ha stor betydning for foretakenes evne til å forsvare seg. Myndighetene skal bl.a. bidra til identifisering av felles cybersårbarheter og rask informasjonsutveksling og koordinering ved alvorlige IKT-hendelser.

4.2 Gjennomføring og virkeområde mv.

4.2.1 Gjennomføring

EØS-relevante forordninger gjøres generelt til en del av norsk rett ved inkorporasjon, det vil si at forordningen skal gjelde i sin helhet som norsk lov eller forskrift. I tillegg må eventuelle eksisterende regler som er i strid med forordningen endres eller oppheves, og det må vurderes om det er behov for å gi utfyllende regler på områder som ikke er dekket av forordningen. Etter departementets foreløpige vurdering bør forordning (EU) 2022/2554 (DORA) inkorporeres i norsk lov, i tråd med praksis for denne typen forordninger.[6] Departementets foreløpige regelverksutkast i kapittel 6 innebærer at forordningen gjennomføres i en ny lov om digital operasjonell motstandsdyktighet i finanssektoren, og at det foretas konsekvenstilpasninger i flere lover og forskrifter.

Etter utkast til lov om digital operasjonell motstandsdyktighet i finanssektoren § 1 første ledd skal forordningen gjelde som norsk lov med de tilpasninger som følger av EØS-avtalen, se avsnitt 6.1. Departementet vil gjennom 2024 samarbeide med de andre EØS/EFTA-landene og EU om innlemmelsen av forordningen i EØS-avtalen, og herunder ta stilling til hvilke tilpasninger som bør gjelde. Et av prinsippene for EØS-tilpasning er at bindende vedtak som de felleseuropeiske tilsynsmyndighetene etter regelverket skal kunne fatte i EU, skal fattes av EFTAs overvåkingsorgan i EØS/EFTA-landene. Etter lovutkastet § 1 annet ledd kan departementet fastsette utfyllende forskrifter til første ledd og i forskrift gjøre endringer i, herunder fastsette unntak fra, bestemmelsene gjennomført i første ledd til gjennomføring av Norges forpliktelser etter EØS-avtalen. Departementet vil med en slik hjemmel bl.a. kunne gjennomføre tekniske standarder og andre utfyllende regler som EU-kommisjonen skal fastsette etter forordningen.

4.2.2 Virkeområde og nasjonale krav

Kravene i forordningen vil gjelde de aller fleste foretakstypene i finanssektoren, jf. omtalen i avsnitt 3.1.1. Kravene gjelder dog ikke forvaltere som forvalter alternative investeringsfond med forvaltningskapital under visse terskler, små forsikrings- og pensjonsforetak, fysiske og juridiske personer som er unntatt fra virkeområdet til verdipapirmarkedsdirektivet, forsikringsformidlere, gjenforsikringsformidlere og tilknyttede forsikringsformidlere som er mikroforetak eller små eller mellomstore foretak, og såkalte postgiroinstitusjoner. Inkassoforetak, eiendomsmeglerforetak og systemer for betalingstjenester er ikke nevnt i forordningen, men omfattes i dag av IKT-forskriftens virkeområde. Systemer for betalingstjenester kan imidlertid bare tilbys av foretak som omfattes av forordningen, og vil derfor måtte omfattes av forordningskravene.

[6] Såkalte nivå 1-forordninger (forordninger som er vedtatt av Europarlamentet og Rådet) som er innlemmet i EØS-avtalen, er i stor grad gjennomført i Norge ved inkorporasjon i lov. Dette gjelder bl.a. kredittvurderingsbyråforordningen, verdipapirsentralforordningen og referanseverdiforordningen, jf. avsnitt 2.1.1.

Departementet legger til grunn at det er rom for å ha nasjonale regler om IKT-risikostyring mv. for foretak som er unntatt fra eller ikke omfattes av forordningen, f.eks. ved at IKT-forskriften videreføres som forenklede krav for foretak som i dag er omfattet av forskriften. I så fall bør kravene gjennomgås for å sikre konsistens med de mer omfattende forordningskravene, og alternativt kan det vurderes å fastsette at forordningskravene skal gjelde helt eller delvis for de unntatte foretakene. Departementet antar at slike forenklede krav er aktuelt bl.a. for små forsikrings- og pensjonsforetak samt inkassoforetak og eiendomsmeglerforetak, siden det ellers vil kunne bli en svekkelse av reguleringen for foretak som i dag følger IKT-forskriften. I utkastet til lov om digital operasjonell motstandsdyktighet i finanssektoren § 2 er det derfor tatt inn en hjemmel for departementet til å fastsette at bestemmelsene i forordningen helt eller delvis skal gjelde for unntatte foretak, inkassoforetak og eiendomsmeglerforetak, og herunder fastsette forenklede krav for slike foretak i samsvar med relevante bestemmelser i forordningen.

Departementet antar at også gjeldsinformasjonsforetak og kredittopplysningsforetak fortsatt skal ha krav om IKT-risikostyring mv., noe som ev. kan kreve tilpasning av gjeldsinformasjonsforskriften, jf. avsnitt 2.2.1.

Som omtalt i avsnitt 3.1.1, skal foretakenes anvendelse av kravene i forordningen være proporsjonal. Dette gjelder særlig reglene om risikostyring, men også for andre deler av forordningen skal dette i noen grad ligge til grunn. Videre er det strengere krav til de mest betydningsfulle foretakene, bl.a. krav om mer avansert testing, jf. avsnitt 3.1.4.

Etter departementets foreløpige vurdering er det ikke annet regelverk enn IKT-forskriften (og ev. deler av finanstilsynsloven § 4 c, jf. avsnitt 4.2.4) som kan overlappe eller være i strid med forordningen, og dermed må endres eller oppheves for de som omfattes av forordningen. Det synes heller ikke nå å være behov for å gi utfyllende regler på områder som ikke er dekket av forordningen, annet enn hjemmel for forenklede krav for unntatte foretak etter lovutkastet § 2.

4.2.3 Forholdet til annen hendelsesrapportering

Etter forordningen artikkel 19 kan nasjonale myndigheter fastsette at foretakenes hendelsesrapportering (og ev. frivillig innrapportering av vesentlige cybertrusler) også skal gå til tilsynsmyndigheter eller responsmiljøer utpekt etter NIS2-direktivet, jf. avsnitt 3.1.3. Som nevnt i boks 3.2 legges det i gjennomføringen av NIS1-direktivet opp til å benytte eksisterende strukturer i størst mulig grad, og Finansdepartementet legger til grunn at Finanstilsynet uansett skal være mottaker av rapporteringen fra foretakene i finanssektoren, jf. avsnitt 4.3.1. Dersom det i NIS1-gjennomføringen eller den senere NIS2-gjennomføringen utpekes andre tilsynsmyndigheter eller responsmiljøer som det vil være hensiktsmessig at foretakene i finanssektoren rapporterer direkte til, bør det gjøres en ny vurdering av disse foretakenes plikter. For foretakene i finanssektoren bør ev. plikter etter den nye digitalsikkerhetsloven uansett samordnes med pliktene etter forordningen.

4.2.4 Forholdet til utkontraktering generelt

I forordningen artikkel 28 er det bl.a. krav om at foretakene skal ha et register over bruk av tjenester fra IKT-leverandører og minst årlig rapportere til tilsynsmyndigheten, jf. avsnitt 3.1.5. Dersom den avtalte tjenesteleveransen ikke møter kravene i forordningen, skal foretaket stanse den på ordnet måte, jf. også omtalen av artikkel 29 og 30 i avsnitt 3.1.5, og tilsynsmyndigheten skal om nødvendig gi pålegg om retting eller stans, jf. omtalen av artikkel 50 i avsnitt 3.1.8.

Etter finanstilsynsloven § 4 c er det krav om melding om utkontraktering generelt, og Finanstilsynet kan gripe inn med pålegg, jf. omtalen i avsnitt 2.1.3. Denne meldeplikten er ikke begrenset til avtaler om IKT-tjenester, og bør derfor i utgangspunktet kunne videreføres. Det er imidlertid et spørsmål om finanstilsynsloven § 4 c bør endres slik at bestemmelsen bare gjelder annen utkontraktering enn det som omfattes av utkastet til lov om digital operasjonell motstandsdyktighet i finanssektoren, siden bestemmelsen ellers kan tenkes å være i strid med forordningsreglene og skape uklarhet for foretakene. Departementet har foreløpig ikke inntatt dette i lovutkastet i avsnitt 6.2, men vil vurdere det i lys av høringssvarene.

4.3 Tilsyn og sanksjoner

4.3.1 Tilsynsmyndighet

Finanstilsynet er tilsynsmyndighet for foretakene som omfattes av forordningen (unntatt IKT-leverandører), og i utkastet til lov om digital operasjonell motstandsdyktighet i finanssektoren § 3 er det skissert en bestemmelse som slår fast at Finanstilsynet er nasjonal tilsynsmyndighet etter forordningen og skal føre tilsyn med overholdelse av bestemmelser gitt i eller i medhold av den nye loven. Dette samsvarer med Finanstilsynets rolle i de regelverkene som er nevnt i forordningen artikkel 46, jf. avsnitt 3.1.8. Departementet legger til grunn at finanstilsynsloven dekker de hjemlene tilsynsmyndigheten skal ha etter forordningen artikkel 50, herunder opplysningsplikt, stedlige tilsyn og pålegg om retting.

For IKT-leverandører innfører forordningen et rammeverk for overvåking på europeisk nivå, der de felleseuropeiske tilsynsmyndighetene (EBA, EIOPA og ESMA) skal utpeke IKT-leverandører som er kritiske for finanssektoren i EU, jf. avsnitt 3.1.6. Avhengig av hvilken del av finanssektoren IKT-leverandøren har størst betydning for, skal en av de felleseuropeiske tilsynsmyndighetene følge opp leverandøren gjennom rollen som hovedovervåker. Etter innlemmelse av forordningen i EØS-avtalen kan det antas at det er IKT-leverandører som er kritiske for finanssektoren også i resten av EØS, som skal utpekes, og at det vil være et EØS/EFTA-organ som skal ha rollen som hovedovervåker overfor ev. kritiske IKT-leverandører som er etablert i et EØS/EFTA-land. Som nevnt over er et av prinsippene for EØS-tilpasning at bindende vedtak som de felleseuropeiske tilsynsmyndighetene etter regelverket skal kunne fatte i EU, skal fattes av EFTAs overvåkingsorgan i EØS/EFTA-landene. Finanstilsynets rolle som nasjonal tilsynsmyndighet vil være å delta i det generelle overvåkingsforumet som skal etableres etter forordningen artikkel 32, og ev. også i undersøkelsesgrupper som etableres for undersøkelser og inspeksjoner hos den

enkelte IKT-leverandør. Finanstilsynet vil også ha i oppgave å følge opp de norske finansielle foretakenes håndtering av risiko som identifiseres i anbefalinger til IKT-leverandører.

4.3.2 Sanksjoner

Finanstilsynet vil videre måtte kunne ilegge administrative sanksjoner, jf. omtalen av forordningen artikkel 51 i avsnitt 3.1.8. Departementet legger foreløpig til grunn at det bare vil være aktuelt med overtredelsesgebyr, og at andre sanksjoner som f.eks. ledelseskarantene ikke vil være relevant ved brudd på forordningskravene. Norske myndigheters adgang til å ilegge overtredelsesgebyr er utvidet de siste årene, både på Finanstilsynets område og andre forvaltningsområder. Frem til nå har Finanstilsynets bruk av gebyr i stor grad vært knyttet til overtredelse av regelverk på verdipapirområdet og overtredelse av foretakenes plikter etter hvitvaskingsreglene.

I et høringsnotat av 19. desember 2019 (som er til behandling i departementet) har Finanstilsynet foreslått en utvidet adgang til å benytte overtredelsesgebyr på finansmarkedsområdet, herunder ved brudd på krav til forsvarlig virksomhet, styring og kontroll mv. i finansforetaksloven § 13-5. Tilsynets forslag samsvarer med verdipapirhandelloven § 21-5 første ledd, som gir tilsynet adgang til å ilegge overtredelsesgebyr ved overtredelse av bl.a. de generelle kravene til organisering av verdipapirforetakenes virksomhet. Innretningen på forordningskravene, bl.a. kravene til foretakenes styring og kontroll av IKT-risiko og håndtering og rapportering av IKT-hendelser, kan tilsi at overtredelser sanksjoneres på samme måte. I utkast til lov om digital operasjonell motstandsdyktighet i finanssektoren § 4 første ledd foreslås det en bestemmelse om at Finanstilsynet kan ilegge overtredelsesgebyr ved overtredelse av bestemmelser i loven, jf. at forvaltningsorganer etter forvaltningsloven § 44 første ledd kan ilegge overtredelsesgebyr når det er fastsatt i lov. I utkastet § 4 fjerde ledd foreslås en forskriftshjemmel til å fastsette at overtredelse av regler gitt i medhold av loven også kan medføre ileggelse av overtredelsesgebyr.

Etter forvaltningsloven § 44 annet ledd kan overtredelsesgebyr ilegges etter faste satser eller utmåles i det enkelte tilfelle (individuell utmåling) innenfor en øvre ramme som må fastsettes i eller i medhold av lov. Forordningen har ikke bestemmelser om størrelsen på overtredelsesgebyr. Finanstilsynets forslag fra 2019 innebærer bl.a. at det kan ilegges overtredelsesgebyr på inntil 50 millioner kroner både for foretak og enkeltpersoner. Departementet har foreløpig inntatt en slik grense i utkastet til den nye loven, jf. § 4 første ledd. Utmålingen av gebyrer innenfor en slik ev. grense må baseres på relevante kriterier i forvaltningsloven og forordningen, samt andre norske myndigheters praksis for bruk av overtredelsesgebyr.

Etter forvaltningsloven § 46 annet ledd skal det ved avgjørelsen av om et foretak skal ilegges administrativ sanksjon, og ved individuell utmåling av sanksjonen, bl.a. tas hensyn til sanksjonens preventive virkning, overtredelsens grovhet, om foretaket kunne ha forebygget overtredelsen, om overtredelsen er begått for å fremme foretakets interesser, om foretaket har hatt eller kunne oppnådd noen fordel ved overtredelsen, om det foreligger gjentakelse, foretakets økonomiske evne, om andre reaksjoner som følge av lovbruddet blir ilagt foretaket eller noen som har handlet på

vegne av det, og om overenskomst med fremmed stat eller internasjonal organisasjon forutsetter bruk av administrativ foretakssanksjon eller foretaksstraff. Disse kriteriene samsvarer i stor grad med forordningen artikkel 51.

Når det er fastsatt i lov at det kan ilegges administrativ sanksjon overfor et foretak, er skyldkravet uaktsomhet med mindre noe annet er bestemt, jf. forvaltningsloven § 46 første ledd. Skyldkravet for overtredelse av forordningen fremgår av utkast til § 4 tredje ledd. Det foreslås videre at medvirkning til overtredelser kan sanksjoneres på samme måte, jf. annet ledd.

Det bør fremgå tilstrekkelig tydelig i loven hvilke handlinger eller unnlatelser som kan føre til ileggelse av overtredelsesgebyr. Siden bestemmelsene om sanksjoner i forordningen artikkel 50 og 51 er nokså generelt utformet uten konkret angivelse av hva slags overtredelser som skal kunne sanksjoneres med administrative sanksjoner, er det ikke gitt hvordan og i hvilken grad dette bør konkretiseres i norsk lov. Forordningen inneholder både overordnede krav til forsvarlig virksomhet og mer tekniske og detaljerte krav. Hvilke handlingsnormer som vil være egnet for håndtering av overtredelser, vil kunne komme klarere frem etter hvert som myndigheter og foretak får erfaring med det nye regelverket, samtidig som rammene for dette i utgangspunktet må være konkrete og fremgå av regelverket. Departementet vil vurdere nærmere hvilke bestemmelser i forordningen som det særlig bør være aktuelt å sanksjonere med overtredelsesgebyr, samt hvilken beløpsgrense som bør gjelde for konkrete overtredelser. I lovutkastet er det foreløpig foreslått at overtredelse av følgende bestemmelser i forordningen kan medføre overtredelsesgebyr: artikkel 5 om forvaltning og organisasjon, artikkel 6 om rammeverk for IKT-risikohåndtering, artikkel 11 om respons og gjenoppretting, artikkel 12 om retningslinjer og prosedyrer for sikkerhetskopiering og gjenoppretting, artikkel 17 om prosess for håndtering av IKT-relaterte hendelser, artikkel 19 nr. 1, 3 og 4 om rapportering av større IKT-relaterte hendelser, artikkel 24 om generelle krav til gjennomføringen av testing av digital operasjonell motstandsdyktighet, og artikkel 28 om generelle prinsipper for forsvarlig styring av IKT-tredjepartsrisiko. Flere av handlingsnormene som foreslås at kan medføre ileggelse av overtredelsesgebyr ved overtredelser, inneholder generelle krav som konkretiseres i andre bestemmelser. Eksempelvis utdypes kravene i forordningen artikkel 6 av mer detaljerte krav i artikkel 7-10. Hensynet til klarhet og forutberegnelighet kan tilsi at også de bestemmelsene som utdyper de overordnede bestemmelsene angis særskilt i loven. Departementet ønsker innspill fra høringsinstansene til disse vurderingene.

4.4 Tilpasninger i annet regelverk

Forordnings- og direktivendringene som er omtalt i henholdsvis avsnitt 3.1.9 og 3.2, krever endringer i flere lover på finansmarkedsområdet. Endringene innebærer i hovedsak at det i bestemmelser om forsvarlig organisering og drift av virksomheten tas inn henvisninger til IKT-risikostyring og kravene som vil gjelde etter forordning (EU) 2022/2554 (DORA), i tillegg til endringer for å sikre konsistens med kravene og begrepsbruken i forordningen. Departementets foreløpige utkast til endringslov innebærer slike tilpasninger i verdipapirhandelloven, verdipapirfondloven, lov om

forvaltning av alternative investeringsfond, lov om kredittvurderingsbyråer, finansforetaksloven, referanseverdiloven og verdipapirsentralloven, se avsnitt 6.2.

Endringer i betalingstjenestedirektivet og tjenestepensjonsdirektivet (jf. avsnitt 3.2) krever tilsvarende tilpasninger i finansforetaksforskriften og forskrift om pensjonsforetak, se avsnitt 6.3.

5 Økonomiske og administrative konsekvenser

5.1 Innledning

Forordningen (EU) 2022/2554 (DORA) innebærer harmonisering av krav til sikkerheten i nettverks- og informasjonssystemer som understøtter virksomheten i foretak i finanssektoren. Det stilles krav til foretakenes risikostyring, avtaler om bruk av IKT-tjenester, felleseuropeisk overvåking av kritiske IKT-leverandører og tilsyn og tilsynssamarbeid. Regelverket skal øke tilliten til det finansielle systemet, opprettholde stabilitet og unngå store kostnader for økonomien ved å minimere konsekvenser og kostnader ved IKT-forstyrrelser. EØS-avtalen innebærer at Norge har plikt til å gjennomføre forordningen når den er innlemmet i EØS-avtalen. Det er derfor ikke grunnlag for å vurdere alternative løsninger.

5.2 Konsekvenser for foretak i finanssektoren

Forordningen 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. Det samme kan ev. lavere risiko for hendelser hos IKT-leverandører som foretakene direkte eller indirekte benytter seg av, samt hos utenlandske finansielle foretak som norske foretak samhandler med eller kan bli påvirket av. Mer analyse og informasjonsutveksling på tvers av foretak, myndigheter og land kan gjøre det lettere for foretakene å forsvare seg mot trusler. I EU-kommisjonens konsekvensanalyse er det anslått at økt digital motstandsdyktighet som følge av det nye regelverket kan redusere kostnadene forbundet med IKT-hendelser i finanssektoren i EU med 10 pst.[7] Dagens kostnader forbundet med hendelser er en usikker størrelse, og Kommisjonen anslo i 2020 årlige besparelser i sektoren på mellom 0,2 og 2,7 mrd. euro. Kommisjonen anslo også at tilpasning til nye IKT-risikostyringskrav kunne kreve en økning av EU-foretakenes cybersikkerhetsbudsjett med om lag 10 pst.

Siden norske foretak lenge har vært underlagt krav som langt på vei tilsvarer forordningen, kan det antas 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. Forordningen vil imidlertid gi et mer detaljert regelverk, også i form av tekniske standarder som skal fastsettes av EU-kommisjonen. Videre vil rapporteringskrav, både internt og eksternt, bli mer omfattende enn i dag, og det blir krav til oppfølging av rapporteringen. Foretakene må påregne vesentlig innsats særlig i overgangen til nytt regelverk, bl.a. knyttet til gjennomgang av systemer, avtaler og dokumentasjon, opplæring av ansatte mv. Kravene til trusselbasert penetrasjonstesting vil medføre egne behov for administrasjon og oppfølging i foretakene som omfattes. På den annen side kan den europeiske harmoniseringen av regelverk og rapportering gi forenklinger og besparelser, spesielt for foretak som har virksomhet i flere land. For mindre foretak kan anvendelsen av proporsjonalitetsprinsippet få

[7] Se vedlegg 5 i EU-kommisjonens konsekvensanalyse 24. september 2020, SWD(2020) 198.

vesentlig betydning, samtidig som de fleste generelt må forholde seg til forordningens konkrete minstekrav på forskjellige områder. Reglene for avtaler om IKT-tjenester kan styrke foretakenes posisjon overfor IKT-leverandører, både gjennom reguleringen av avtaler og myndighetsovervåking av kritiske leverandører.

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, bl.a. til oppfølging og innholdet i avtaler, jf. avsnitt 3.1.5. Dette antas likevel ikke å ha større økonomiske eller administrative konsekvenser for IKT-leverandørene, jf. dagens krav i IKT-forskriften. IKT-leverandører som utpekes som kritiske for finanssektoren i EU/EØS vil bli gjenstand for myndighetsovervåking, herunder undersøkelser og inspeksjoner, og kan måtte tilpasse seg myndighetsanbefalinger for å kunne opprettholde leveranser til finansielle foretak. Dette kan ha vesentlig betydning for IKT-leverandørenes drift og kostnader, herunder administrative kostnader forbundet med etterlevelse av regelverket og oppfølging av overvåkingen. I tillegg skal de kritiske IKT-leverandørene betale en overvåkingsavgift. Finanstilsynet har opplyst at det legger til grunn at det ikke er norske tjenestetilbydere som i dag har virksomhet som tilsier at de kan bli utpekt som kritiske IKT-leverandører.

5.4 Konsekvenser for kunder og norsk økonomi

Formålet med forordningen er å redusere sannsynligheten for skadelige IKT-hendelser i den europeiske finanssektoren. 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

I tillegg til tilsyn med etterlevelsen av et mer omfattende regelverk, innebærer forordningen enkelte nye oppgaver som trolig vil kreve noe økt ressursbruk i Finanstilsynet. Finanstilsynet skal bl.a. informere relevante europeiske myndigheter om IKT-hendelser i Norge og håndtere tilsvarende informasjon fra andre land (jf. avsnitt 3.1.3), identifisere og følge opp foretak som skal foreta trusselbasert penetrasjonstesting (jf. avsnitt 3.1.5) og delta i IKT-overvåkingsforumet og ev. undersøkelsesgrupper og følge opp anbefalinger til IKT-leverandører (jf. avsnitt 3.1.6). Det kan også bli behov for økt samhandling med andre norske myndigheter, som Nasjonal sikkerhetsmyndighet og Datatilsynet. Siden Finanstilsynet fører risikobasert tilsyn, er dagens oppfølging av IKT-risikostyring mv. i tråd med proporsjonalitetsprinsippet.

6 Utkast til regelverksendringer

6.1 Utkast til lov om digital operasjonell motstandsdyktighet i finanssektoren

§ 1. *Forordningen om digital operasjonell motstandsdyktighet i finanssektoren*

(1) EØS-avtalen vedlegg IX nr. […] (forordning (EU) 2022/2554 om digital operasjonell motstandsdyktighet i finanssektoren) gjelder som lov med de tilpasninger som følger av vedlegg IX, protokoll 1 til avtalen og avtalen for øvrig.

(2) Departementet kan fastsette utfyllende forskrifter til bestemmelsen her og i forskrift gjøre endringer i, herunder fastsette unntak fra, bestemmelsene gjennomført i første ledd til gjennomføring av Norges forpliktelser etter EØS-avtalen.

§ 2. *Forenklede krav for andre foretak*

(1) Departementet kan i forskrift fastsette at bestemmelsene i § 1 helt eller delvis skal gjelde for foretak nevnt i forordning (EU) 2022/2554 artikkel 2 nr. 3, inkassoforetak og eiendomsmeglerforetak. Departementet kan herunder fastsette forenklede krav for slike foretak i samsvar med relevante bestemmelser i forordning (EU) 2022/2554.

§ 3. *Tilsyn*

(1) Finanstilsynet er nasjonal tilsynsmyndighet etter forordningen om digital operasjonell motstandsdyktighet i finanssektoren og fører tilsyn med overholdelse av bestemmelser gitt i eller i medhold av denne loven.

§ 4. *Overtredelsesgebyr*

(1) Finanstilsynet kan ilegge fysiske personer eller foretak overtredelsesgebyr på inntil 50 millioner kroner ved overtredelse av forordning (EU) 2022/2554 artikkel 5 om forvaltning og organisasjon, artikkel 6 om rammeverk for IKT-risikohåndtering, artikkel 11 om respons og gjenoppretting, artikkel 12 om retningslinjer og prosedyrer for sikkerhetskopiering og gjenoppretting, artikkel 17 om prosess for håndtering av IKT-relaterte hendelser, artikkel 19 nr. 1, 3 og 4 om rapportering av større IKT-relaterte hendelser, artikkel 24 om generelle krav til gjennomføringen av testing av digital operasjonell motstandsdyktighet, og artikkel 28 om generelle prinsipper for forsvarlig styring av IKT-tredjepartsrisiko.

(2) Medvirkning til overtredelse som nevnt i første ledd, kan sanksjoneres på samme måte.

(3) Fysiske personer kan ilegges overtredelsesgebyr for forsettlige eller uaktsomme overtredelser. Foretak kan ilegges overtredelsesgebyr når foretaket eller noen som har handlet på foretakets vegne, forsettlig eller uaktsomt har begått en overtredelse som nevnt i første eller annet ledd.

(4) Departementet kan i forskrift gitt i medhold av loven fastsette at den som forsettlig eller uaktsomt overtrer forskriften, kan ilegges overtredelsesgebyr.

§ 5. *Ikrafttredelse*

(1) Loven gjelder fra den tid Kongen bestemmer. Kongen kan sette i kraft de enkelte bestemmelser til forskjellig tid.

(2) Departementet kan fastsette overgangsregler.

6.2 Utkast til lov om endringer i finanslovgivningen mv.

I

I lov 29. juni 2007 nr. 75 om verdipapirhandel gjøres følgende endringer:

§ 8-1 første ledd skal lyde:

EØS-avtalen vedlegg IX forordning (EU) nr. 600/2014 (om markeder for finansielle instrumenter (verdipapirmarkedsforordningen)) som endret ved forordning (EU) nr. 1033/2016 *og forordning (EU) 2022/2554* gjelder som lov med de tilpasninger som følger av vedlegg IX, protokoll 1 til avtalen og avtalen for øvrig.

§ 9-16 første ledd skal lyde:

Verdipapirforetak skal innrette sin virksomhet på følgende måte:

1. Foretaket skal ha tilstrekkelige og betryggende retningslinjer, rutiner og kontrollmetoder som skal sikre at foretaket, dets ledere, ansatte og tilknyttede agenter etterlever sine forpliktelser etter lov og forskrifter.
2. Foretaket skal være oppbygd og organisert på en slik måte at risikoen for interessekonflikter mellom foretaket og dets kunder, eller foretakets kunder seg imellom, begrenses til et minimum, jf. § 10-2.
3. Foretaket skal treffe rimelige tiltak som skal sikre kontinuitet og regelmessighet i investeringstjenestevirksomheten, herunder ha nødvendige systemer, ressurser og prosedyrer, *inkludert IKT-systemer satt opp og håndtert i henhold til forordning (EU) 2022/2554 artikkel 7.*
4. Foretaket skal treffe betryggende tiltak slik at operasjonell risiko begrenses til et minimum når det benytter seg av en tredjepart til å utføre operasjonelle funksjoner, jf. annet ledd.
5. Foretaket skal *ha gode* administrasjons- og regnskapsrutiner, tilfredsstillende interne kontrollordninger og effektive prosedyrer for risikovurdering, samt stillingsinstrukser som særskilt regulerer ansvarsfordelingen mellom daglig leder og andre ledere av virksomheten.
6. Foretaket skal ha tilfredsstillende interne retningslinjer, rutiner og kontrollmetoder for personlige transaksjoner som foretas av foretakets ledere, ansatte og tilknyttede agenter.
7. Foretaket skal ha systemer som sikrer pålitelig og korrekt informasjonsoverføring, og som sikrer at opplysningene til enhver tid behandles fortrolig, samt reduserer risikoen for dataforfalskning, informasjonslekkasje og annen ulovlig tilgang til informasjonen *i henhold til kravene i forordning (EU) 2022/2554.*

8. Foretaket skal sørge for dokumentasjon av alle investeringstjenester og all investeringsvirksomhet, herunder alle utførte transaksjoner, som skal være minst så fyllestgjørende at Finanstilsynet kan kontrollere om de regler Finanstilsynet har ansvar for, er overholdt. Slik dokumentasjon skal oppbevares i minst fem år, eller lengre tid dersom Finanstilsynet bestemmer det.
9. Foretaket skal ha interne instrukser for de ansattes adgang til å være medlem av styre, bedriftsforsamling eller foretaksforsamling eller ha slik innflytelse som nevnt i aksjeloven § 1-3 annet ledd i selskaper. Slike instrukser skal også omfatte styremedlemmer som har slik innflytelse i verdipapirforetaket som nevnt i aksjeloven § 1-3 annet ledd. Tilsvarende instrukser skal utarbeides for tilfeller der det er gitt unntak etter § 10-4 annet ledd.
10. Foretaket skal ha retningslinjer og rutiner for beregning og utbetaling av resultatavhengig godtgjørelse.

§ 9-23 første og andre ledd skal lyde:

(1) Verdipapirforetak som utfører algoritmehandel, skal ha effektive systemer og risikokontroller som er egnet for virksomheten, for å sikre at foretakets handelssystemer er robuste og har tilstrekkelig kapasitet *i henhold til kravene i forordning (EU) 2022/2554 kapittel II* og er underlagt hensiktsmessige terskler og grenser for handler. Slike systemer og kontroller skal også hindre at det sendes uriktige ordrer eller at systemene skaper eller bidrar til uro i markedet. Verdipapirforetaket skal også ha effektive systemer og risikokontroller som sikrer at handelssystemene ikke kan brukes til formål som er i strid med reglene i kapittel 3 eller med reglene til en handelsplass som foretaket er tilknyttet.

(2) Verdipapirforetak som utfører algoritmehandel, skal ha effektive beredskapsplaner og -systemer *i henhold til kravene i forordning (EU) 2022/2554 artikkel 11* for å håndtere en eventuell svikt i dets handelssystemer og skal påse at systemet er fullt testet og tilfredsstillende overvåket slik at det oppfyller kravene i bestemmelsen her *og krav i henhold til forordning (EU) 2022/2554 kapittel II og IV.*

§ 11-18 første ledd nr. 2 skal lyde:

identifisering og håndtering av vesentlige risikoer som virksomheten utsettes for, *herunder håndtering av risiko knyttet til IKT-systemer i henhold til forordning (EU) 2022/2554 kapittel II,*

§ 11-19 første og andre ledd skal lyde:

(1) Et regulert marked skal ha effektive systemer, prosedyrer og ordninger *for operasjonell motstandsdyktighet i henhold til forordning (EU) 2022/2554 kapittel II* som til enhver tid sikrer at handelssystemet:

1. er robust og har tilstrekkelig kapasitet for å kunne håndtere høye ordre- og meldingsvolum,
2. sikrer velordnet handel ved alvorlig markedsuro,
3. er fullt gjennomtestet.

(2) Et regulert marked skal ha beredskapsplaner og systemer *i henhold til forordning (EU) 2022/2554 artikkel 11* som sikrer kontinuerlig drift ved svikt i handelssystemet.

§ 11-21 fjerde ledd skal lyde:

Et regulert marked skal kreve at medlemmene gjør hensiktsmessige tester av sine algoritmer, og skal stille testmiljøer tilgjengelig for slik testing *i henhold til kravene i forordning (EU) 2022/2554 kapittel II og IV.*

§ 17-1 første ledd skal lyde:

EØS-avtalen vedlegg IX nr. 31bc (forordning (EU) nr. 648/2012) om OTC-derivater, sentrale motparter og transaksjonsregistre (EMIR), som endret ved direktiv (EU) 2015/849 *og forordning (EU) 2022/2554,* gjelder som lov med de tilpasninger som følger av vedlegg IX, protokoll 1 til avtalen og avtalen for øvrig.

§ 19-2 første ledd skal lyde:

Verdipapirforetak, sentrale motparter, datarapporteringsforetak og markeds-operatører, *samt IKT tredjeparts tjenesteleverandører som referert til i kapittel V i forordning (EU) 2022/2554*, plikter å gi Finanstilsynet de opplysninger som kreves om forhold som angår foretakets forretning og virksomhet. Tilsvarende gjelder foretak i samme konsern. Tilsvarende gjelder også for verdipapirforetaks tilknyttede agenter. Foretaket plikter å fremvise, og i tilfelle utlevere til kontroll, dokumentasjon etter § 9-16 første ledd nr. 8, herunder lydopptak og elektronisk kommunikasjon etter § 9-17, og øvrig fysisk og elektronisk dokumentasjon som angår virksomheten.

II

I lov 25. november 2011 nr. 44 om verdipapirfond skal § 2-11 første ledd nr. 1 lyde:

gode administrasjons- og regnskapsrutiner og kontroll- og sikkerhetsordninger *for elektronisk databehandling, herunder for nettverk og systemer som er etablert og håndtert etter forordning (EU) 2022/2554.*

III

I lov 20. juni 2014 nr. 28 om forvaltning av alternative investeringsfond skal § 3-1 første ledd bokstav b lyde:

gode administrasjons- og regnskapsrutiner, kontroll- og sikkerhetsordninger *for elektronisk databehandling, herunder for nettverk og systemer som er etablert og håndtert etter forordning (EU) 2022/2554,* og regler for ansattes personlige transaksjoner,

IV

I lov 20. juni 2014 nr. 30 om kredittvurderingsbyråer skal § 1 lyde:

EØS-avtalen vedlegg IX nr. 31eb (forordning (EF) nr. 1060/2009) om kredittvurderingsbyråer (kredittvurderingsbyråforordningen) som endret ved forordning (EU) nr. 513/2011, direktiv 2011/61/EU, forordning (EU) nr. 462/2013 *og forordning (EU) 2022/2554*, gjelder som lov med de tilpasninger som følger av vedlegg IX, protokoll 1 til avtalen og avtalen for øvrig.

V

I lov 10. april 2015 nr. 17 om finansforetak og finanskonsern gjøres følgende endringer:

§ 13-5 første ledd skal lyde:

Et finansforetak skal organiseres og drives på en forsvarlig måte. Foretaket skal ha en klar organisasjonsstruktur og ansvarsfordeling samt klare og hensiktsmessige styrings- og kontrollordninger. Foretaket skal ha hensiktsmessige retningslinjer og rutiner for å identifisere, styre, overvåke og rapportere risiko foretaket er, eller kan bli, eksponert for. *Foretaket skal ha nettverks- og informasjonssystemer i samsvar med forordning (EU) 2022/2554.* Foretaket skal også ha hensiktsmessige retningslinjer og rutiner for gjennomføring, overvåkning og regelmessig vurdering av godtgjørelses-ordninger.

§ 20-6 a tredje ledd bokstav g skal lyde:

å forenkle strukturen i foretaket eller konsernet for å sikre at kritiske funksjoner kan skilles ut juridisk og operasjonelt fra øvrig virksomhet *for å sikre kontinuitet og digital operasjonell motstandsdyktighet.*

VI

I lov 4. desember 2015 nr. 95 om fastsettelse av finansielle referanseverdier skal § 1 første ledd lyde:

EØS-avtalen vedlegg IX forordning (EU) 2016/1011 (om indekser brukt som referanseverdier i finansielle instrumenter og finansielle kontrakter eller for å måle resultatet i investeringsfond (referanseverdiforordningen)) *som endret ved forordning (EU) 2022/2554* gjelder som lov med de tilpasninger som følger av vedlegg IX, protokoll 1 til avtalen og avtalen for øvrig.

VII

I lov 15. mars 2019 nr. 6 om verdipapirsentraler og verdipapiroppgjør mv. § 1-1 skal første ledd lyde:

EØS-avtalen vedlegg IX forordning (EU) nr. 909/2014 (om forbedring av verdipapir-oppgjør i Den europeiske union og om verdipapirsentraler samt om endring av direktiv 98/26/EF og 2014/65/EU og forordning (EU) nr. 236/2012 (verdipapirsentral-forordningen)) *som endret ved forordning (EU) 2022/2554* gjelder som lov med de tilpasninger som følger av vedlegg IX til avtalen, protokoll 1 til avtalen og avtalen for øvrig.

VIII

Loven gjelder fra den tid Kongen bestemmer. Kongen kan sette i kraft de enkelte bestemmelsene til forskjellig tid.

Departementet kan fastsette overgangsregler

6.3 Utkast til forskrift om endring i finansforetaksforskriften og forskrift om pensjonsforetak

Fastsatt av Finansdepartementet [dato] med hjemmel i lov 10. juni 2005 nr. 44 om forsikringsvirksomhet §§ 3-1 femte ledd og 13-5 sjette ledd.

I

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

§ 1-7 bokstav j skal lyde:

tjenester levert av ytere av tekniske tjenester som støtter tilbudet av betalingstjenester uten på noe tidspunkt å komme i besittelse av midlene som overføres, *inkludert behandling og lagring av data, tillits- og personverntjenester, data- og enhets-autentisering, informasjons- og kommunikasjonsteknologi (IKT) og kommunikasjons-nettverk, levering og vedlikehold av terminaler og enheter som brukes til betaling-stjenester,* med unntak av betalingsfullmakttjenester og kontoinformasjonstjenester.

§ 3-2 skal lyde:

§ 3-2. ***Tilleggskrav til søknad om tillatelse som betalingsforetak og e-pengeforetak***

Søknad om tillatelse til å drive virksomhet som betalingsforetak, e-pengeforetak eller opplysningsfullmektig skal i tillegg til kravene i finansforetaksloven § 3-1 også inneholde følgende dokumentasjon:

a. 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 *i henhold til kapittel III i forordning (EU) 2022/2554.*
b. Rutiner om lagring og overvåkning av sensitiv betalingsinformasjon, samt begrensninger i og oversikt over adgang til denne informasjonen.
c. En beskrivelse av foretakets forretningsmessige kontinuitetsplan som identifiserer kritiske deler av virksomheten, *effektive retningslinjer og planer for forretningsmessig IKT-kontinuitet-, respons- og gjenoppretting, samt prosedyrer for å teste om planene er effektive og tilstrekkelige i henhold til forordning (EU) 2022/2554.*
d. Prinsipper og definisjoner som foretaket bruker i innsamlingen av statistiske opplysninger om drift, transaksjoner og svindel.
e. Foretakets retningslinjer knyttet til sikkerhet, inkludert en detaljert risiko-vurdering av betalingstjenestevirksomheten og en beskrivelse av kontrollen med sikkerheten og tiltak for å beskytte brukerne av betalingstjenestene mot risikoene som er identifisert, inkludert svindel og ulovlig bruk av sensitive opplysninger og personopplysninger, *samt angi hvordan de sikrer et høyt nivå av digital operasjonell motstandskraft i samsvar med kapittel II i forordning (EU) 2022/2554.*
f. En beskrivelse av foretakets kontroll med eventuelle agenter og filialer, jf. finansforetaksforskriften § 13-4, en beskrivelse av foretakets utkontraktering

og deltakelse i nasjonalt eller internasjonalt betalingssystem, *samt ordninger for bruk av IKT-tjenester i henhold til forordning (EU) 2022/2554.*

Første ledd bokstav a berører ikke anvendelsen av kapittel II i forordning (EU) 2022/2554 for:

a. betalingstjenesteytere nevnt i bokstav a), b) og d) i artikkel 1 nr. 1 i Europaparlaments- og Rådsdirektiv (EU) 2015/2366.
b. leverandører av kontoinformasjonstjenester nevnt i artikkel 33 nr. 1 i Europaparlaments- og Rådsdirektiv (EU) 2015/2366.
c. betalingsinstitusjoner som er unntatt i henhold til artikkel 32 nr. 1 i Europaparlaments- og Rådsdirektiv (EU) 2015/2366.
d. elektroniske pengeinstitusjoner med dispensasjon som nevnt i artikkel 9 nr. 1 i direktiv 2009/110/EF.

Denne bestemmelsen gjelder ikke for søknad om begrenset tillatelse som betalingsforetak

II

I forskrift 9. desember 2016 nr. 1503 om pensjonsforetak skal § 22 tredje ledd lyde:

Systemet for risikostyring og internkontroll skal omfatte tiltak for å sikre kontinuitet i utøvelsen av virksomheten, herunder beredskapsplaner. *For dette formål skal pensjonsforetaket benytte hensiktsmessige og forholdsmessige systemer, ressurser og prosedyrer, og skal særlig sette opp og administrere nettverks- og informasjonssystemer i samsvar med Europaparlamentets og rådets forordning (EU) 2022/2554, der det er aktuelt.*

III

Forskriften trer i kraft […].