DET KONGELIGE
FINANSDEPARTEMENT

Prop. 54 LS

(2024–2025)

Proposisjon til Stortinget (forslag til lovvedtak og stortingsvedtak)

Lov om digital operasjonell motstandsdyktighet i finanssektoren, lov om endringer i hvitvaskingsloven (gjennomføring av forordning (EU) 2023/1113) og samtykke til godkjenning av to beslutninger i EØS-komiteen om innlemmelse i EØS-avtalen av forordning (EU) 2022/2554, direktiv (EU) 2022/2556 og forordning (EU) 2023/1113

DET KONGELIGE
FINANSDEPARTEMENT

Prop. 54 LS

(2024–2025)

Proposisjon til Stortinget (forslag til lovvedtak og stortingsvedtak)

Lov om digital operasjonell motstandsdyktighet i finanssektoren, lov om endringer i hvitvaskingsloven (gjennomføring av forordning (EU) 2023/1113) og samtykke til godkjenning av to beslutninger i EØS-komiteen om innlemmelse i EØS-avtalen av forordning (EU) 2022/2554, direktiv (EU) 2022/2556 og forordning (EU) 2023/1113

Innhold

DET KONGELIGE
FINANSDEPARTEMENT

Prop. 54 LS

(2024–2025)

Proposisjon til Stortinget (forslag til lovvedtak og stortingsvedtak)

Lov om digital operasjonell motstandsdyktighet i finanssektoren, lov om endringer i hvitvaskingsloven (gjennomføring av forordning (EU) 2023/1113) og samtykke til godkjenning av to beslutninger i EØS-komiteen om innlemmelse i EØS-avtalen av forordning (EU) 2022/2554, direktiv (EU) 2022/2556 og forordning (EU) 2023/1113

Tilråding fra Finansdepartementet 7. mars 2025, godkjent i statsråd samme dag.
(Regjeringen Støre)

1 Proposisjonens hovedinnhold

1.1 Lov om digital operasjonell motstandsdyktighet i finanssektoren (DORA)

Departementet fremmer i kapittel 2 forslag til ny lov om digital operasjonell motstandsdyktighet i finanssektoren (DORA-loven) som vil gjennomføre EØS-regler som svarer til Europaparlaments- og rådsforordning (EU) 2022/2554 av 14. desember 2022 og endringsdirektiv (EU) 2022/2556 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren («Digital Operational Resilience Act», DORA).

Lovforslaget innebærer nye 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.

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.

DORA-regelverket innebærer harmonisering av krav til IKT-sikkerhet i finansielle foretak i Europa. Gjennomføring av regelverket i norsk rett vil gjøre at kravene til foretakene i den norske finanssektoren styrkes, selv om dagens norske regelverk og tilsynsmessige oppfølging bygger på de samme prinsippene som de nye kravene.

I proposisjonen bes det også om samtykke til godkjenning av EØS-komiteens beslutning nr. 40/2025 av 20. februar 2025, jf. Grunnloven § 26 annet ledd, som innlemmer DORA-regelverket i EØS-avtalen.

1.2 Endringer i hvitvaskingsloven om opplysninger som skal følge overføringer av penger og visse kryptoeiendeler (TFR II)

Departementet fremmer i kapittel 3 forslag til endringer i *lov 1. juni 2018 nr. 23 om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsloven)* som vil gjennomføre EØS-regler som svarer til Europaparlaments- og rådsforordning (EU) 2023/1113 av 31. mai 2023 om opplysninger som skal følge overføringer av penger og visse kryptoeiendeler og om endringer i direktiv (EU) 2015/849 av 20. mai 2015 om forebyggende tiltak mot bruk av det finansielle systemet i forbindelse med hvitvasking av penger eller finansiering av terrorisme (fjerde hvitvaskingsdirektiv).

Forordning (EU) 2023/1113 («Transfer of Funds Regulation II», TFR II) inneholder krav til tjenesteytere om innhenting, bekreftelse, lagring og overføringer av opplysninger om avsendere og mottakere av pengeoverføringer og overføringer av kryptoeiendeler. Disse kravene eksisterte allerede for tradisjonelle pengeoverføringer gjennom forordning (EU) 2015/847 (TFR I), men utvides i TFR II til å gjelde også for tjenesteytere som sender og mottar kryptoeiendeler. I tillegg innfører forordningen rapporteringsplikt for kryptoeiendelstjenesteytere, hvilket betyr at disse underlegges plikter i hvitvaskingsregelverket på lik linje med tradisjonelle betalingstjenesteytere.

I proposisjonen bes det videre om samtykke til godkjenning av EØS-komitéens beslutning nr. 42/2025 av 20. februar 2025, jf. Grunnloven § 26 annet ledd, som innlemmer TFR II-regelverket i EØS-avtalen.

2 Lov om digital operasjonell motstandsdyktighet i finanssektoren (DORA-loven)

2.1 Innledning

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.

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.

Forordning (EU) 2022/2554 om digital operasjonell motstandsdyktighet i finanssektoren ble vedtatt i EU 14. desember 2022. Samtidig ble direktiv (EU) 2022/2556 vedtatt for å gjøre nødvendige tilpasninger i ulike direktiver på finansmarkedsområdet. Rettsaktene omtales samlet som DORA («Digital Operational Resilience Act»), og ble tatt inn i EØS-avtalen 20. februar 2025 ved EØS-komiteens beslutning nr. 40/2025, med forbehold om Stortingets samtykke, jf. Grunnloven § 26 annet ledd. Departementet foreslår i denne proposisjonen at DORA-rettsaktene gjennomføres i norsk rett, og at Stortinget gir sitt samtykke til innlemmelse av dem i EØS-avtalen.

DORA-regelverket innebærer harmonisering av krav til sikkerheten i nettverks- og informasjonssystemer som understøtter virksomheten i finansielle foretak i Europa. Gjennomføring av regelverket i norsk rett vil gjøre at kravene til foretakene i den norske finanssektoren styrkes, selv om dagens norske regelverk og tilsynsmessige oppfølging bygger på de samme prinsippene som de nye kravene.

2.2 Bakgrunn for forslaget

2.2.1 Forordning (EU) 2022/2554 (DORA-forordningen)

Forordning (EU) 2022/2554 om digital operasjonell motstandsdyktighet i finanssektoren (DORA-forordningen) ble vedtatt i EU 14. desember 2022 sammen med det tilhørende endringsdirektivet (EU) 2022/2556. DORA-forordningen inneholder omfattende krav til foretakenes IKT-risikostyring, håndtering og rapportering av IKT-hendelser, testing av den digitale motstandsdyktigheten, bruk av IKT-leverandører og informasjonsdeling. DORA-forordningen etablerer også et rammeverk for myndighetsovervåking på europeisk nivå av kritiske IKT-leverandører og legger til rette 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. Forordningen ble gitt anvendelse i EU 17. januar 2025.

2.2.2 Direktiv (EU) 2022/2556 (DORA-direktivet)

Direktiv (EU) 2022/2556 (DORA-direktivet) ble vedtatt i EU 14. desember 2022 sammen med DORA-forordningen og endrer en rekke direktiver 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 DORA-forordningen, i tillegg til endringer for å sikre konsistens med kravene og begrepsbruken i forordningen. DORA-direktivet endrer direktiv 2009/65/EF (direktivet om

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

2.2.3 Høring

På oppdrag fra Finansdepartementet utredet Finanstilsynet i 2023 behovet for endringer i norsk rett for å gjennomføre de forventede EØS-forpliktelsene som svarer til DORA-regelverket. Departementet utarbeidet så et høringsnotat på grunnlag av Finanstilsynets utredning og andre kilder. Departementet sendte 23. januar 2024 notatet på høring med frist 3. april 2024. Høringsnotatet ble sendt til følgende instanser:

Alle departementene

Akademikerne
Aksjonærforeningen i Norge
Arbeids- og velferdsdirektoratet
Arbeidsgiverforeningen Spekter
Bankenes sikringsfond
Brønnøysundregistrene
Datatilsynet
Deloitte AS
Den norske advokatforening
Den Norske Aktuarforening
Den norske Revisorforening
Direktoratet for forvaltning og økonomistyring
Econa
Eiendom Norge
EVRY
Finans Norge
Finansforbundet
Finansieringsselskapenes forening
Folketrygdfondet
Forbrukerrådet
Forbrukertilsynet
Forening for Finansfag Norge
Handelshøgskolen ved Nord universitet
Handelshøyskolen BI
Havtrygd Gjensidig Forsikring
Hovedorganisasjonen for universitets- og høyskoleutdannede
Hovedorganisasjonen Virke
Huseiernes landsforbund
Høgskulen på Vestlandet
Kommunalbanken AS
Konkurransetilsynet
Kpmg AS
KS
Landsorganisasjonen i Norge
Likestillings- og diskrimineringsombudet
Nasdaq OMX Oslo ASA
Nordic Trustee
Norges Bank
Norges eiendomsmeglerforbund
Norges handelshøyskole
Norges ingeniør- og teknologorganisasjon
Norges Juristforbund
Norges Kommunerevisorforbund
Norges Rederiforbund
Norsk Crowdfunding Forening
Norsk Kapitalforvalterforening
Norsk Venturekapitalforening
Norsk Økrimforening
Norske Boligbyggelags Landsforbund SA
Norske Finansanalytikeres Forening
Norske Forsikringsmegleres Forening
Næringslivets Hovedorganisasjon
Oslo Børs ASA
Pensjonskasseforeningen
Regelrådet
Regjeringsadvokaten
Regnskap Norge
Riksadvokaten
Riksrevisjonen
Sivilombudet
Skattebetalerforeningen
Skattedirektoratet
Skatterevisorenes Forening
SMB Norge
Sparebankforeningen i Norge
Statens pensjonskasse
Statistisk sentralbyrå
Stiftelsesforeningen
Storebrand ASA
The Nordic Association of Marine Insurers (CEFOR)
Tietoevry Norge
Tilsynsrådet for advokatvirksomhet
Universitetet i Agder
Universitetet i Bergen
Universitetet i Oslo
Universitetet i Sørøst-Norge
Universitetet i Tromsø – Norges arktiske universitet
Verdipapirfondenes forening
Verdipapirforetakenes Forbund
Verdipapirsentralen ASA
Yrkesorganisasjonenes Sentralforbund

ØKOKRIM
Økonomiforbundet

Følgende høringsinstanser har gitt merknader:

Advokatforeningen
Finansforbundet
Finans Norge
NHO
Nordic Financial CERT
Norges Bank
Oslo Børs ASA
Pensjonskasseforeningen
Regelrådet
Verdipapirfondenes forening
Verdipapirforetakenes Forbund

Følgende instanser har skrevet at de ikke vil inngi høringsuttalelse, eller at de ikke har merknader til forslaget:

Arbeids- og velferdsdirektoratet
Brønnøysundregistrene
Den Norske Aktuarforening
Forsvarsdepartementet
Justis- og beredskapsdepartementet
Landbruks- og matdepartementet
Statistisk sentralbyrå

2.3 Gjeldende rett

2.3.1 Innledning

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. Nedenfor gis en oversikt over relevante bestemmelser i lov- og forskriftsverket for finansforetak, betalingssystemer og på verdipapirområdet, samt de mer detaljerte kravene etter IKT-forskriften.

2.3.2 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, 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 gjennomføring av CRR/CRD-regelverket (CRR/CRD-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 om pensjonsforetak* § 22 gir nærmere regler om risikostyring og internkontroll for pensjonsforetak. *Forskrift 9. desember 2016 nr. 1502 om finansforetak og finanskonsern (finansforetaksforskriften)* § 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.

2.3.3 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 verdipapirforetak benytter seg av en tredjepart til å utføre operasjonelle funksjoner. Det stilles videre krav om at verdipapirforetaket skal ha effektive kontroll- og sikkerhetsordninger for informasjonsbehandlingssystemer, 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, og 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 om risikostyring og internkontroll 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.

2.3.4 Finanstilsynsloven

Etter *lov 7. desember 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 første ledd 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 etter § 4 c annet ledd 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. Det følger av § 4 c tredje ledd at 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.

Lov 21. juni 2024 nr. 41 om Finanstilsynet (den nye finanstilsynsloven) har ennå ikke blitt satt i kraft, men det tas sikte på ikrafttredelse våren 2025. Loven vil da erstatte gjeldende finanstilsynslov. Den nye loven viderefører i hovedsak gjeldende finanstilsynslov §§ 4 og 4 c, herunder i den nye lovens § 4-6 om utkontraktering.

2.3.5 IKT-forskriften

2.3.5.1 Virkeområde

Forskrift 21. mai 2003 nr. 630 om bruk av informasjons- og kommunikasjonsteknologi (IKT) (IKT-forskriften) er fastsatt av Finanstilsynet i medhold

av betalingssystemloven § 3-3, 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.

2.3.5.2 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, 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 punkt 2.3.5.4.

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 skal etter § 7 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, samt 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 én 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.

2.3.5.3 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 doku-

mentering 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. 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. Eiendomsmeglingsforetak omfattes ikke av kravet til hendelsesrapportering.

2.3.5.4 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.

2.4 EØS-rett

2.4.1 Innledning

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. Samtidig med forordningen ble direktiv (EU) 2022/2556 vedtatt for å gjøre nødvendige tilpasninger i ulike direktiver på finansmarkedsområdet. Rettsaktene omtales samlet som DORA («Digital Operational Resilience Act») og ble tatt inn i EØS-avtalen 20. februar 2025 ved EØS-komiteens beslutning nr. 40/2025, med forbehold om Stortingets samtykke, jf. Grunnloven § 26 annet ledd. Innholdet i forordningen og direktivet omtales nærmere nedenfor. De EØS-tilpasningene som er gjort til innholdet i forordningen ved EØS-komiteens beslutning, bl.a. når det gjelder ordningen med hovedovervåker, er beskrevet i punkt 2.6.3.

2.4.2 Forordning (EU) 2022/2554

2.4.2.1 Formål og virkeområde

Forordning (EU) 2022/2554 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). 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. opplysningsfullmektiger,
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, se artikkel 2 nr. 2. 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 forsikringsformidlere 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).

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.

2.4.2.2 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. Dette vil i norsk sammenheng være styret. Enkelte plikter som pålegges «ledelsesorganet» etter DORA-forordningen er imidlertid av en slik art at de etter norsk rett vil falle inn under det som vanligvis er daglig leders plikter. Den nærmere grensedragningen mellom styret og daglig leder omtales i punkt 2.5.4.3. Her fremgår det at departementet mener at det ved eventuell uklarhet om hvilket selskapsorgan som skal anses som ansvarlig etter DORA-regelverket, påhviler styret i norske foretak å avklare ansvarsfordelingen mellom styret og daglig leder.

Ledelsesorganet skal 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. Ledelsesorganet 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 av leveranser fra IKT-leverandører, alternativt utpeke et medlem av ledelsen som skal ha ansvar for å følge opp risikoeksponering og dokumentasjon forbundet med leveransen. Medlemmene av ledelsesorganet 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 virk-

somheten, være 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 raskt å oppdage unormal aktivitet, herunder ytelsesproblemer og IKT-hendelser, samt avdekke vesentlige kritiske punkter («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 konsekvensanalyse for virksomheten 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 andre læringspunkter skal inntas i foretakets risikovurderingsprosess, og IKT-ledelsen skal minst årlig rapportere til ledelsesorganet 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, med rutiner for hvordan kommunikasjonen skal foregå, både internt og eksternt.

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.

2.4.2.3 IKT-relatert hendelseshåndtering, klassifisering og rapportering

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 av om hendelser. Foretaket skal etter nr. 1 rapportere til tilsynsmyndigheten om alle alvorlige IKT-hendelser, som i artikkel 3 nr. 10 er defi-

nert 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 (CSIRT-enheter) utpekt etter NIS2-direktivet. 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 at 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, etter konsultasjon med Den europeiske sentralbanken (ESB) og Det europeiske byrået for nettverks- og informasjonssikkerhet (ENISA), utarbeide en rapport med vurdering av mulighetene for ytterligere sentralisering av foretakenes hendelsesrapportering gjennom å opprette 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.

2.4.2.4 Testing av digital operasjonell 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. Artikkel 26 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. Artikkel 26 nr. 11 gir hjemler for EU-kommisjonen til å fastsette tekniske standarder for TLPT i samsvar med TIBER-rammeverket fra Den europeiske sentralbanken (ESB).

2.4.2.5 Håndtering av tredjeparts IKT-risiko

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. Artikkel 28 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 fordels- og 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.

2.4.2.6 Overvåkning 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 artikkel 31 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 artikkel 31 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 artikkel 31 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 artikkel 31 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 artikkel 31 nr. 11 søke om å bli det. Etter artikkel 31 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 artikkel 31 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 artikkel 32 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 artikkel 32 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. Artikkel 32 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 artikkel 35 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 artikkel 42 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 artikkel 42 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 artikkel 42 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.

Ordningen med hovedovervåker er tilpasset EFTA-pilaren gjennom EØS-komiteens beslutning, slik at EFTAs overvåkningsorgan fungerer som hovedovervåker overfor fysiske og juridiske personer når disse er etablert i en EØS/EFTA-stat eller i et tredjeland, men med et datterforetak i en EØS/EFTA-stat, se nærmere omtale i punkt 2.6.3.

2.4.2.7 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.

2.4.2.8 Tilsyn, myndighetssamarbeid og sanksjoner

Forordningen kapittel VII gjelder nasjonale tilsynsmyndigheter på finansmarkedsområdet, samt samarbeid mellom myndigheter på europeisk nivå.

Artikkel 46 angir hvilke tilsynsmyndigheter som i samsvar med annet EU/EØS-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 gjenopprettende 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, ilegge 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 alvorlighetsgrad, 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. Tilsynsmyndigheten 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.

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. 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. 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).

2.4.2.9 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).

2.4.2.10 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 forsikringsformidlere 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, PSDII) skal EU-kommisjonen også vurdere om flere av foretakene som er omfattet av det direktivet, bør omfattes av forordningen, jf. artikkel 58 nr. 2. Etter artikkel 58 nr. 3 skal EU-kommisjonen innen januar 2026 vurdere om revisorer og revisjonsselskaper bør omfattes av forordningen eller tilsvarende krav i direktiv 2006/43/EF (revisjonsdirektivet).

Forordningen skal etter artikkel 64 gjelde fra 17. januar 2025 i EU.

2.4.3 Direktiv (EU) 2022/2556

Direktiv (EU) 2022/2556 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-forordningen), i tillegg til endringer for å sikre konsistens med kravene og begrepsbruken i DORA-forordningen. Endringene gjelder virksomhetskravene for kredittinstitusjoner, betalingsforetak, verdipapirforetak, regulerte markeder og forvaltere av verdipapirfond og alternative investeringsfond, samt justeringer i kravene til innhold i gjenopprettings- og krisehåndteringsplaner for kredittinstitusjoner mv. Direktivendringene innebærer i seg selv ingen nye materielle forpliktelser utover de som vil følge av forordningen.

Ovennevnte direktiver er gjennomført i sektorlovgivningen og forutsetter endringer i finansforetaksloven, verdipapirhandelloven, verdipapirfondloven, lov om forvaltning av alternative investeringsfond, pensjonsforetaksforskriften og finansforetaksforskriften.

Endringene som følge av DORA-direktivet er av teknisk karakter. Endringsbestemmelsene innebærer at forpliktelsene etter DORA-forordningen også forankres i sektorlovgivningen. Endringene i sektorlovgivningen innebærer, som nevnt, i seg selv ingen nye materielle forpliktelser

for de foretakene det gjelder. De konkrete forpliktelsene fremgår av DORA-forordningen.

2.5 Gjennomføring i norsk rett

2.5.1 Oversikt

Utkastet til norsk gjennomføring av forordning (EU) 2022/2554 og direktiv (EU) 2022/2556 (DORA-forordningen og -direktivet) fikk generelt støtte i høringen, samtidig som høringsinstansene ønsket alternative løsninger og avklaringer på en del områder. Departementet vil i det følgende presentere høringsutkastet og høringsinstansenes merknader, og foreslår en ny lov som gjennomfører DORA-forordningen, samt konsekvenstilpasninger i annet lovverk.

2.5.2 Regelverksstruktur

2.5.2.1 Høringsutkastet

I høringsnotatet foreslo departementet at DORA-forordningen gjennomføres ved inkorporasjon i en ny lov om digital operasjonell motstandsdyktighet i finanssektoren. Det vil si at forordningen skal gjelde i sin helhet som norsk lov. Denne gjennomføringsmåten er benyttet for flere andre EØS-regelverk, bl.a. kredittvurderingsbyråforordningen, verdipapirsentralforordningen og referanseverdiforordningen. Utkastet i høringsnotatet til ny lov inneholdt i § 1 første ledd inkorporasjonsbestemmelsen, mens § 1 annet ledd gir departementet hjemmel for å fastsette utfyllende forskrifter.

2.5.2.2 Høringsinstansenes syn

Norges Bank uttaler at «en innføring av regelverket vil styrke den digitale motstandskraften i finanssektoren», og at nye regler for oppfølging av IKT-leverandører som er sentrale på europeisk nivå «vil være et viktig bidrag til oppfølging av IKT-risiko på tvers av landegrenser».

Finans Norge uttrykker også støtte til «departementets forslag om å implementere de felleseuropeiske reglene som følger av DORA gjennom en ny lov om digital operasjonell motstandsdyktighet i finanssektoren».

Oslo Børs ASA støtter «Finansdepartementets forslag til og begrunnelse for gjennomføring av DORA-regelverket i ny lov om digital operasjonell motstandsdyktighet i finanssektoren, samt ved endringer i verdipapirhandelloven og enkelte andre relevante lover».

2.5.2.3 Departementets vurdering

Departementet foreslår at DORA-forordningen inkorporeres i norsk lov, i tråd med høringsutkastet. Gjennomføringen 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. Dette kan bidra til å fremme robusthet, finansiell stabilitet, trygghet for kundene og ivaretakelse av kritiske samfunnsfunksjoner. Gjennomføring av godt kjente, felleseuropeiske krav kan også ha betydning for tilliten i internasjonale markeder til norske foretaks risikostyring og norske myndigheters oppfølging av finanssektoren.

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 tjenester til foretak under tilsyn i flere europeiske land. Felleseuropeiske krav til bl.a. foretakenes oppfølging av og kontroll med IKT-leverandører, kan bidra til økt sikkerhet i viktige betalingssystemer og gjennom det bidra til finansiell stabilitet. Forordningen legger også til rette for tettere samarbeid mellom myndighetene, både strategisk og 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.

Forordningen foreslås gjennomført i Norge i en ny lov om digital operasjonell motstandsdyktighet i finanssektoren (DORA-loven). Etter lovforslaget § 1 første ledd skal forordningen gjelde som norsk lov med de tilpasninger som følger av EØS-avtalen, se punkt 2.6.

Lovforslaget § 1 annet ledd viser til at med DORA-forordningen menes forordningen slik den er gjennomført i første ledd, det vil si i EØS-tilpasset form, og med eventuelle endringer gjennomført eller henvist til i første ledd, eller gjennomført i forskrift med hjemmel i fjerde ledd.

Videre foreslås det en hjemmel for departementet til å kunne fastsette utfyllende regler i forskrift, se lovforslaget § 1 tredje ledd. Forslaget skal for det første gi departementet hjemmel til å gjennomføre utfyllende kommisjonsrettsakter fastsatt med hjemmel i DORA-forordningen, så som tekniske standarder og andre utfyllende regler. Forslaget skal også legge til rette for at departementet midlertidig kan fastsette denne

typen utfyllende regler før de er tatt inn i EØS-avtalen, slik at norsk regelverk kan holdes oppdatert med det som gjelder i EU. EU-kommisjonen har fastsatt kommisjonsrettsakter med utfyllende regler til DORA, men enkelte regler er fortsatt under utarbeidelse. Generelt vil en måtte påregne at utfyllende kommisjonsrettsakter vedtas og trer i kraft i EU før de innlemmes i EØS-avtalen. Det vil kunne være uheldig for norske foretak og vil kunne svekke effekten av DORA-regelverket dersom disse får virkning i Norge vesentlig senere enn i EU på grunn av forsinkelser i EØS-prosessen, da de utfyllende kommisjonsrettsaktene regulerer den praktiske gjennomføringen av bestemmelser i forordningen. Eksempler på dette er rettsaktene knyttet til rapportering av IKT-hendelser og rapportering av register over IKT-tjenesteavtaler.

Etter lovforslaget § 1 fjerde ledd kan departementet i forskrift gjøre endringer i, herunder fastsette unntak fra, bestemmelsene gjennomført i § 1 første ledd til gjennomføring av Norges forpliktelser etter EØS-avtalen. Hjemmelen skal sikre at departementet kan gjennomføre mindre endringer i DORA-forordningen i forskrifts form, selv om forordningen er gjennomført i lov. Dette er samme type derogasjonshjemmel som er gitt i annen lovgivning på finansmarkedsområdet som gjennomfører EØS-regler som svarer til EU-forordninger. Se for eksempel lov om EØS-finanstilsyn § 6 annet ledd og verdipapirhandelloven § 7-1 tredje ledd.

2.5.3 Virkeområde, nasjonale krav og proporsjonalitet

2.5.3.1 Høringsutkastet

Departementet viste i høringsnotatet til at kravene i forordningen vil gjelde de aller fleste foretakstypene i finanssektoren, dog ikke forvaltere av 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, eiendomsmeglingsforetak 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.

Departementet la 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. Departementet påpekte at kravene i så fall bør gjennomgås for å sikre konsistens med de mer omfattende forordningskravene, og uttalte at det alternativt kunne vurderes å fastsette at forordningskravene skal gjelde helt eller delvis for de unntatte foretakene. Departementet antok at slike forenklede krav kunne være aktuelt bl.a. for små forsikrings- og pensjonsforetak samt inkassoforetak og eiendomsmeglingsforetak, siden disse i dag følger IKT-forskriften. I utkastet til lov om digital operasjonell motstandsdyktighet i finanssektoren § 2 var 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 eiendomsmeglingsforetak, og herunder fastsette forenklede krav for slike foretak i samsvar med relevante bestemmelser i forordningen. Departementet antok at også gjeldsinformasjonsforetak og kredittopplysningsforetak fortsatt skal ha krav om IKT-risikostyring mv., noe som ev. kan kreve tilpasning av gjeldsinformasjonsforskriften.

I høringsnotatet uttrykte departementet at den foreløpige vurderingen var at det ikke er annet regelverk enn IKT-forskriften (og ev. deler av finanstilsynsloven § 4 c, jf. omtalen av forholdet til utkontraktering generelt nedenfor) som kan overlappe eller være i strid med forordningen, og dermed må endres eller oppheves for de som omfattes av forordningen. Departementet bemerket også at det ikke syntes å være behov for å gi utfyllende regler på områder som ikke er dekket av forordningen, annet enn hjemmelen for forenklede krav for unntatte foretak etter lovutkastet § 2.

Departementet pekte dessuten på at foretakenes anvendelse av kravene i forordningen skal være proporsjonale, og at dette særlig gjelder reglene om risikostyring, men i noen grad også for andre deler av forordningen. Videre ble det bemerket at det er strengere krav til de mest betydningsfulle foretakene, bl.a. krav om mer avansert testing, og at tilsynsmyndigheten skal ta hensyn til proporsjonalitet i oppfølgingen av foretakene.

2.5.3.2 Høringsinstansenes syn

Finans Norge forstår høringsnotatet «dithen at IKT-forskriften skal videreføres, og at både DORA

og IKT-forskriften skal være gjeldende samtidig i Norge». Finans Norge uttaler videre:

> «DORA vil i denne sammenheng erstatte IKT-forskriften for de finansforetakene som er omfattet av DORA. Selv om DORA bygger på et proporsjonalitetsprinsipp, er det ikke redegjort for hvilke deler av DORA som skal gjelde for de ulike finansforetakene. Det er ikke klargjort hvilke finansforetak som vil få minimumskrav, og hvilke som eventuelt vil få utvidede krav.
>
> Vedrørende IKT-forskriften, ser det ut som (…) at departementet foreslår at IKT-forskriften fortsatt skal være gjeldende overfor enkelte kategorier av finansforetak som er unntatt fra DORA etter art. 2 nr. 3. Det fremgår ikke nærmere hvilke finansforetak dette er ment å gjelde.
>
> Flere av finansforetakene som er unntatt fra DORA, er i dag også unntatt fra IKT-forskriften. Å innta nye finansforetak i virkeområdet for IKT-forskriften, forutsetter en vurdering av hvorvidt IKT-forskriften er et egnet rammeverk for slik virksomhet. Etter Finans Norges syn, er for eksempel IKT-forskriften lite egnet for forsikringsformidlingsforetak med lav omsetning. Slike forsikringsformidlingsforetak er unntatt fra DORA etter art. 2 nr. 3 og etter art. 3 nr. 64. Det kreves en nærmere begrunnelse for å tilordne denne kategorien av finansforetak til virkeområdet for IKT-forskriften. Dette er ofte finansforetak som i liten grad er tilpasset standardene som IKT-forskriften legger opp til. Proporsjonalitetsprinsippet tilsier derfor at slike finansforetak bør holdes utenfor IKT-forskriften.
>
> Finans Norge vil påpeke behovet for en redaksjonell opprydning, med hensikt om å avklare virkeområdet til både DORA og IKT-forskriften.»

Advokatforeningen mener at det bør «tydeliggjøres hva som skal gjelde for finansieringsforetak, som ikke synes å være omfattet av forslagene i høringsnotatet», mens *Finansforbundet* uttaler at det er behov for å «avklare virkeområdet til DORA når det gjelder bl.a. morselskap i finanskonsern. Morselskap er å anse som finansforetak, men det fremgår ikke av listen i høringsnotatet (…) om hvorvidt de også omfattes av virkeområdet for DORA».

Pensjonskasseforeningen uttaler bl.a. følgende om behovet for proporsjonal anvendelse av regelverket:

> «Forordningen unntar små pensjonsforetak med mindre enn 15 medlemmer fra regelverket, og det gjør også et skille ved at små pensjonsforetak med mindre enn 100 medlemmer har betydelig forenklede krav. Finansdepartementet skriver i høringsnotatet at det for disse kan være aktuelt og enten opprettholde dagens IKT-forskrift som et styrket, forenklet krav for disse, men at denne gjennomgås for å sikre konsistens med det mer omfattende regelverket. Alternativt vises det til muligheten at det ved innføringen av forordningen i det norske regelverket uten unntak [sic]. I begge tilfellene vil dette bety betydelig økte krav for de minste pensjonskassene sammenlignet med kravene i forordningen og i strid med dens bakenforliggende intensjon. De økte kravene vil pålegge de minste pensjonskassene økte kostnader i utførelsen av kravene, som igjen kan være vanskelig å forsvare. Alle pensjonskassene, også de minste følger i dag IKT-forskriften. Pensjonskasseforeningen stiller spørsmål ved hva som er hensikten med å pålegge også de minste foretakene et så omfattende regelverk som kommer i tillegg til andre særnorske regelverk for disse pensjonskassene.
>
> I Norge er det Finanstilsynet som fører tilsyn med norske pensjonskasser, og med det er ansvarlige for å kontrollere at pensjonskassene etterlever regelverket. For pensjonskassene oppleves det at EU og det felleseuropeiske forsikringstilsynet EIOPA i større grad enn det norske Finanstilsynet har et reelt og materielt fokus på proporsjonalitet, og med det skiller mellom livselskap og pensjonskasser, samt skiller pensjonskasser ut fra størrelse. Livselskapene er normalt store innretninger. Krav og forventninger som stilles til slike, kan ikke være sammenfallende til hva man oppstiller for langt mindre pensjonskasser. Mindre innretninger representer også langt mindre systemkritiske forhold.»

Verdipapirforetakenes Forbund (VPFF) «påpeker viktigheten av klarhet i DORA-forordningens virkeområde, spesielt med tanke på forholdet til eksisterende nasjonalt regelverk som IKT-forskriften og finanstilsynsloven», og uttaler videre bl.a. at:

> «Det fremkommer i høringsnotatet at enkelte foretak er unntatt fra DORA, men likevel forblir underlagt IKT-forskriften. I hvilken grad hele eller deler av IKT-forskriften også vil gjelde foretak som er underlagt DORA kommer ikke klart frem. Etter vår oppfatning bør man unngå

overlapping mellom nasjonalt regelverk og DORA for foretak som er underlagt DORA. (…)

For å oppnå en smidig implementering av DORA, er det essensielt at det tas hensyn til de ulike virksomhetstyper og ulik størrelse på foretakene i den norske finanssektoren. Proporsjonalitetsprinsippet bør ligge til grunn for alle krav som stilles, slik at både store og små virksomheter kan oppfylle de nye kravene uten uforholdsmessig belastning.»

Verdipapirfondenes forening – næringspolitikk (VFFN) uttaler følgende:

«Mens forvaltere av alternative investeringsfond med forvaltningskapital som er lavere enn fastsatte terskelverdier i AIF-loven (i praksis AIF-forvaltere som kun er registreringspliktige hos Finanstilsynet) er unntatt forordningskravene, er forvaltningsselskap for verdipapirfond som sådan omfattet av forordningen. Videre følger det at blant annet små og ikke-sammenkoplede verdipapirforetak, samt små pensjonsforetak, skal følge regler om et forenklet rammeverk for IKT-risikostyring. At forvaltningsselskap for verdipapirfond som sådan er omfattet av forordningskravene, uavhengig av virksomhetens omfang mv., gjør en fornuftig og tilstrekkelig bruk av proporsjonalitetsprinsippet desto viktigere i Finanstilsynets oppfølging av forvaltningsselskapene for verdipapirfond.

VFFN vil følgelig understreke betydningen av at hensynet til proporsjonalitet i den tilsynsmessige oppfølgingen av forvaltningsselskap for verdipapirfond blir gjennomgående og fornuftig ivaretatt etter implementeringen av DORA.»

Oslo Børs ASA mener at «innlemmingen av DORA nødvendiggjør store endringer i IKT-forskriften», og uttaler videre:

«Vi savner derfor at utredningen inneholder vurderinger på forholdet mellom de to regelsettene – især når departementet konkluderer med at det er rom for å ha nasjonale regler for IKT-risikostyring mv. parallelt med DORA. Det er uheldig at høringsnotatet ikke nærmere begrunner hvordan relevante konsekvenstilpasninger i IKT-forskriften bør utformes, og hvordan IKT-forskriften kan opprettholdes uten å kompromittere Norges EØS-rettslige forpliktelser. Vi minner om at formålet med DORA er å introdusere et harmonisert og omfattende felles europeisk regelverk for å håndtere IKT-risiko i sektoren.

Oslo Børs er av den oppfatning at IKT-forskriften bør oppheves helt for de foretak som omfattes av DORA. Dette er nødvendig både for å oppnå det uttalte formålet om felles europeisk regelverk og Norges EØS forpliktelser som følger med rettsaktene.»

Finansforbundet uttaler følgende om proporsjonalitet:

«Basert på høringsnotatet er det utfordrende å ta stilling til hvordan proporsjonalitetsprinsippet er tenkt å fungere i praksis. Slik vi oppfatter det, er det ikke klargjort hvilke deler av forordningen som gjelder for ulike aktører. Finansforbundet mener proporsjonalitetsprinsippet må implementeres og håndheves med aktsomhet med tanke på påvirkning av konkurransesituasjon for små og mellomstore aktører. Disse strever allerede med høyere kapitalkrav og omfattende compliance- og rapporteringskrav. Det er en styrke for norsk økonomi og næringsliv at finansmarkedet i Norge består av både internasjonale og nasjonale aktører, både stor og små.»

Finansforbundet kommenterer også forholdet til digitalsikkerhetsloven:

«Finansforbundet er kjent med at ettersom tidspunkt for ikrafttredelse for DORA og Digitalsikkerhetslov ikke er avklart, er det en utfordring for finansnæringen å vite hvilket lovverk man skal forholde seg til. Det kan f.eks. være et spørsmål om man først må ivareta digitalsikkehetsloven og så DORA. I implementeringen av DORA og Digitalsikkerhetsloven bør det derfor komme klart fram hvordan finansnæringen skal håndtere overgangen til nytt lovverk.»

Regelrådet uttaler bl.a. følgende om proporsjonalitet:

«Departementet viser at forordningens nyttevirkninger trolig er større enn kostnadsvirkningene. Vi mener imidlertid at utredningen har svakheter i beskrivelsen av berørt næringsliv og beskrivelsen av kostnadsvirkningene for næringslivet. Finanssektoren og IKT-sektoren er identifisert som berørte av forslaget, men det er ikke gitt en beskrivelse av sektorene.

Hele forordningen hviler på et proporsjonalitetsprinsipp, men det er ikke klargjort hvilke deler av forordningen som gjelder for de ulike aktørene i norsk næringsliv. Videre gir departementet en overordnet beskrivelse av de nye kravene som forordningen stiller til næringslivet. Fraværet av en beskrivelse av hvordan proporsjonalitetsprinsippet skal håndheves i praksis gjør det imidlertid utfordrende å vurdere hvilke konsekvenser dette vil ha for individuelle norske bedrifter.

På grunn av den manglende beskrivelse av den norske konteksten for regelverket er det vanskelig å si på dette stadiet hva kostnadene for næringslivet vil bli. En vellykket gjennomføring er avhengige av at departement og tilsyn håndterer regelverket på en effektiv måte.»

2.5.3.3 Departementets vurdering

Foretak i den norske finanssektoren har lenge vært underlagt krav etter IKT-forskriften som langt på vei tilsvarer kravene etter DORA-forordningen. Virkeområdet til DORA-forordningen omfatter kredittinstitusjoner, betalingsforetak, opplysningsfullmektiger, e-pengeforetak, verdipapirforetak, tilbydere av tjenester knyttet til kryptoverdier, verdipapirsentraler, sentrale motparter, handelsplasser, transaksjonsregistre, forvaltere av alternative investeringsfond, forvaltningsselskaper, leverandører av datarapporteringstjenester, forsikrings- og gjenforsikringsforetak, forsikringsformidlere, gjenforsikringsformidlere og tilknyttede forsikringsformidlere, pensjonsforetak, kredittvurderingsbyråer, administratorer av kritiske referanseverdier, tjenesteleverandører for folkefinansiering, verdipapiriseringsregistre og tredjepartstilbydere av IKT-tjenester, jf. omtalen av forordningen artikkel 2 nr. 1 i punkt 2.4.2.1. Forordningens virkeområde omfatter dermed i utgangspunktet alle foretakene som omfattes av IKT-forskriften, unntatt finansieringsforetak, inkassoforetak og eiendomsmeglingsforetak. I tillegg er små forsikrings- og pensjonsforetak underlagt IKT-forskriften, men unntatt fra forordningen etter artikkel 2 nr. 3.

Departementet antok derfor i høringsnotatet at det særlig kunne være aktuelt å fastsette nasjonale regler om IKT-risikostyring mv. for inkassoforetak, eiendomsmeglingsforetak og små forsikrings- og pensjonsforetak. Finansieringsforetak og låneformidlingsforetak ble i denne sammenheng ikke særskilt omtalt i høringsnotatet, men nasjonale regler vil kunne være aktuelt også for disse foretakene, jf. bl.a. at finansieringsforetak er underlagt IKT-forskriften i dag. Basert på høringsinnspillene antar departementet at det også kan vise seg å være hensiktsmessig med hjemmel til å fastsette i forskrift i hvilket omfang morselskap i finanskonsern skal være omfattet av DORA-forordningen. Utkastet til hjemmel for å fastsette slike regler omfattet imidlertid også andre foretak som er unntatt fra forordningen etter artikkel 2 nr. 3, det vil si forvaltere av alternative investeringsfond med forvaltningskapital under visse terskler, 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. Selv om departementet ikke nå ser at det er behov for å fastsette nasjonale regler om IKT-risikostyring mv. for foretak som verken omfattes av DORA-forordningen eller er underlagt IKT-forskriften, kan markeds- og risikoutviklingen gjøre slike regler nødvendige senere.

Departementet foreslår derfor en forskriftshjemmel som gir mulighet for å fastsette nasjonale regler om IKT-risikostyring mv. for foretak som er nevnt i forordningen artikkel 2 nr. 3, finansieringsforetak, låneformidlingsforetak, inkassoforetak, eiendomsmeglingsforetak og morselskap i finanskonsern. Det vises til lovforslaget § 2.

Videre er spørsmålet hvilke nasjonale krav som skal kunne fastsettes for foretak som ikke omfattes av forordningen. Etter høringsutkastet kan det fastsettes at bestemmelsene i forordningen helt eller delvis skal gjelde for de aktuelle foretakene, herunder at foretakene skal få forenklede krav i samsvar med relevante bestemmelser i forordningen. Departementet pekte i høringsnotatet på at én mulighet kan være at IKT-forskriften videreføres som forenklede krav, dog etter en gjennomgang for å sikre konsistens med forordningen, og at en annen mulighet kan være å fastsette at forordningskravene skal gjelde helt eller delvis. Som bl.a. Finans Norge, Oslo Børs og Verdipapirforetakenes Forbund har pekt på, er det ikke nærmere utredet i høringsnotatet hvordan nasjonale forskriftskrav konkret bør utformes. Departementet har imidlertid bedt Finanstilsynet utrede dette i et nytt høringsnotat, som vil bli sendt på høring. Det vil uansett ikke være aktuelt å gi nasjonale krav for foretak som omfattes av forordningen, jf. også at lovforslaget § 2 ikke åpner for dette.

Foretakene som ikke omfattes av forordningen, har generelt virksomhet av begrenset omfang og kompleksitet, noe som tilsier at nasjonale forskriftskrav om IKT-risikostyring mv. bør være vesentlig enklere enn forordningskravene.

Samtidig bør nasjonale krav så langt som mulig samsvare med forordningskravenes formål og innretning, slik at arbeidet med IKT-risikostyring mv. blir konsistent på tvers av finanssektoren. Departementet legger uansett til grunn at de nye forskriftskravene i utgangspunktet ikke bør være mer omfattende enn det som følger av dagens IKT-forskrift, og utelukker ikke at det kan være behov for ytterligere forenklinger. Departementet er enig med Finans Norge i at dersom det skulle være aktuelt å fastsette krav for foretak som i dag ikke er underlagt IKT-forskriften, må det foretas en særskilt vurdering av om slike regler er et egnet rammeverk for virksomhetenes begrensede omfang og kompleksitet. Departementet vil som nevnt sende på høring utkast til nasjonale forskriftsregler om IKT-risikostyring mv. for foretak som ikke omfattes av forordningen.

Flere av høringsinstansene har pekt på behovet for en proporsjonal anvendelse av kravene i forordningen. Dette følger for det første i noen grad direkte av forordningen, der det er angitt at foretakene selv skal bruke visse regler proporsjonalt, basert på vurderinger av foretakets størrelse og samlede risikoprofil, samt virksomhetens type, omfang og kompleksitet. Dette gir grunnlag for at enklere virksomheter kan ha en enklere tilnærming til bl.a. risikostyringskravene. I tillegg er det noen regler, som krav om avansert testing, som ikke vil være relevante for enklere virksomheter. For det andre skal Finanstilsynet legge proporsjonalitetsprinsippet til grunn for tilsyn og annen oppfølging av det nye regelverket. Dette er angitt konkret i forordningen, og samsvarer også med Finanstilsynets risikobaserte oppfølging av foretak generelt.

Når det kommer til forholdet mellom ikrafttredelse av digitalsikkerhetsloven og DORA, viser departementet til digitalsikkerhetsloven § 5, som sier at dersom det stilles krav om sikkerhet og varsling i annen lov eller forskrift som minst tilsvarer kravene etter digitalsikkerhetsloven, skal kravene etter denne andre loven eller forskriften benyttes. I Prop. 109 LS (2022–2023) s. 24 er bank- og finansmarkedsinfrastruktur nevnt som eksempler på sektorer som har sikkerhets- og varslingskrav som tilsvarer kravene i digitalsikkerhetsloven, gjennom IKT-forskriften. DORA har mer omfattende krav enn IKT-forskriften, og vil derfor benyttes fremfor digitalsikkerhetsloven. Fordi foretak i finanssektoren som blir omfattet av digitalsikkerhetslovens virkeområde uansett skal etterleve kravene i sektorregelverket fremfor kravene i digitalsikkerhetsloven og -forskriften, er det departementets oppfatning at tidspunkt for ikrafttredelse av digitalsikkerhetsloven vil ha liten praktisk betydning for foretak i finanssektoren.

2.5.4 Styret og daglig leders ansvar

2.5.4.1 Høringsutkastet

Departementet viste i høringsnotatet bl.a. til at foretakene etter forordningen artikkel 5 nr. 1 skal ha et overordnet rammeverk for IKT-risikostyring, og at rammeverket etter nr. 2 skal fastsettes, godkjennes og overvåkes av foretakets ledelsesorgan («management body» på engelsk), jf. også omtale i punkt 2.4.2.2. Ledelsesorganet er definert i forordningen 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. Departementet bemerket at dette organet i norsk kontekst vil være styret.

I høringsnotatet ble det videre pekt på at styret (ledelsesorganet) etter forordningen artikkel 5 nr. 2 bl.a. skal 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 (ledelsesorganet) skal etter bestemmelsen 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.

Det ble videre vist til at medlemmene av styret (ledelsesorganet) etter artikkel 5 nr. 4 skal 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. Det ble også vist til at IKT-ledelsen etter artikkel 13 bl.a. skal rapportere til styret (ledelsesorganet) minst årlig om funn og anbefalinger.

2.5.4.2 Høringsinstansenes syn

Advokatforeningen mener at «høringsnotatets omtale av 'management body' [bør] nyanseres for å reflektere kompetansedelingen mellom styret og daglig leder etter norsk rett». Advokatforeningen uttaler videre bl.a. følgende:

> «Som påpekt i høringsnotatet henviser DORA art. 3 (30) til nærmere definisjoner i sektor-

reglene for blant annet kredittinstitusjoner (direktiv 2013/36, CRD IV) og verdipapirforetak (direktiv 2014/65, MiFID II). Deretter avsluttes DORA art. 3 (30) med følgende oppsamlingskategori for de tilfeller som ikke fanges opp av foregående henvisninger:

'(…) or the equivalent persons who effectively run the entity or have key functions in accordance with relevant Union or national law.'

Etter norsk selskapsrett er det daglig leder, og ikke styret, som 'effectively run the entity.' Det fremgår også av forarbeidene til gjennomføringen av CRD IV og MiFID II at daglig leder i noen sammenhenger er å regne som 'management body.' I Prop. 77 L (2017–2018) om gjennomføringen av MiFID II i norsk rett er forholdet mellom management body og norske selskapsorganer grundig behandlet, se særlig punkt 5.2.3.5:

'Departementet er enig i utvalgets vurdering av at ledelsesorgan (eng. management body) som definert i MiFID II (jf. artikkel 4 nr. 1 punkt 36) etter norsk rett må forstås enten som styret eller styret og daglig leder eller styret, daglig leder og faktisk ledelse, og at det må angis hvilket organ eller person i et verdipapirforetak det enkelte krav retter seg mot når bestemmelsen i MiFID II gjennomføres i verdipapirhandelloven. Departementet bemerker imidlertid at når MiFID II artikkel 9 (jf. CRD IV artikkel 88) om styringsordninger (eng. governance arrangements) gjennomføres i bestemmelse om styrets oppgaver og ansvar (jf. forslag til § 9-11), vil bestemmelsen utfylles av aksjelovenes generelle regler om henholdsvis styrets og daglig leders ansvar og oppgaver.'

Videre er følgende uttalt i Prop. 125 L (2013–2014) om norsk gjennomføring CRD IV, se punkt 5.4.4:

'Til FNOs merknad om at det kan være uklart hva som menes med «faktisk ledelse,» viser departementet til at dette begrepet svarer til uttrykket «persons who effectively run the undertaking,» jf. bla. Solvens II-direktivet artikkel 42 nr. 1, og at uttrykket må forstås på samme måte. Departementet viser i denne forbindelse også til definisjon av «management body» i CRD IV artikkel 3 nr. 1 (7), som lyder: «management body means an institution's body or bodies, which are appointed in accordance with national law, which are empowered to set the institution's strategy, objectives and overall direction, and which oversee and monitor management decision-making, and include the persons who effectively direct the business of the institution.'

Også her er det tydelig at 'management body' ikke er ensbetydende med styret, ettersom 'faktisk ledelse' regnes inn i begrepet.

Disse uttalelsene i forarbeidene må ses i sammenheng med at både CRD IV og MiFID II uttrykkelig forutsetter og hensyntar at det er ulik regulering av kompetansefordelingen mellom selskapsorganene i de ulike medlemslandenes selskapsrett:

MiFID II, fortalens punkt 55:

'Different governance structures are used across Member States. In most cases a unitary or a dual board structure is used. The definitions used in this Directive are intended to embrace all existing structures without advocating any particular structure. They are purely functional for the purpose of setting out rules aiming to achieve a particular outcome irrespective of the national company law applicable to an institution in each Member State. The definitions should therefore not interfere with the general allocation of competences in accordance with national company law.'

CRD IV, fortalens punkt 56:

'A management body should be understood to have executive and supervisory functions. The competence and structure of management bodies differ across Member States. In Member States where management bodies have a one-tier structure, a single board usually performs management and supervisory tasks. In Member States with a two-tier system, the supervisory function is performed by a separate supervisory board which has no executive functions and the executive function is performed by a separate management board which is responsible and accountable for the day-to-day management of the undertaking. Accordingly, separate tasks are assigned to the different entities within the management body.'

I norsk rett er selskapsledelsen fordelt mellom styret og daglig leder, hvor utførende ansvar for den operative virksomheten ligger hos daglig leder, mens styret skal sørge for forsvarlig organisering og føre tilsyn med selskapets virksomhet. Dette henger sammen med at det vil være en lite hensiktsmessig ansvarsfordeling og forstyrrende for styrets kjerneoppgaver om styret

også skal ha en sentral rolle i den operative virksomheten. Ser man hen til de konkrete oppgavene som i DORA tillegges 'management body,' vil det etter Advokatforeningens oppfatning kunne være naturlig å legge følgende ansvarsområder under daglig leder:

DORA art. 5 (1)

'The management body of the financial entity shall define, approve, oversee and be responsible for the implementation of all arrangements related to the ICT risk management framework referred to in Article 6(1).'

DORA art. 5 (2) (g)

'allocate and periodically review the appropriate budget to fulfil the financial entity's digital operational resilience needs in respect of all types of resources, including relevant ICT security awareness programmes and digital operational resilience training referred to in Article 13(6), and ICT skills for all staff'

DORA art. (4)

'Members of the management body of the financial entity shall actively keep up to date with sufficient knowledge and skills to understand and assess ICT risk and its impact on the operations of the financial entity, including by following specific training on a regular basis, commensurate to the ICT risk being managed.'

Videre kan ytterligere oppgaver og ansvar bli tillagt 'management body' i delegerte kommisjonsforordninger eller gjennom utfyllende veiledning fra europeiske tilsynsmyndigheter, som det kan tenkes å være naturlig å legge under daglig leder etter norsk rett.

Etter Advokatforeningens oppfatning bør forarbeidene tydeliggjøre at ansvaret som påhviler 'management body' etter DORA i noen sammenhenger vil falle inn under ansvarsområdet til daglig leder, gitt kompetansefordelingen mellom styret og daglig leder etter norsk rett. Dette vil etter Advokatforeningens oppfatning være i samsvar med den norske implementeringen av CRD IV og MiFID II.»

2.5.4.3 Departementets vurdering

Departementet er enig i at de kravene som DORA stiller til «ledelsesorganet» bør tillegges henholdsvis styret og daglig leder i foretaket, i tråd med den alminnelige selskapsrettslige ansvarsfordelingen mellom disse organene i norsk rett. Etter departementets vurdering betyr dette at utførende ansvar for den operative virksomheten normalt ligger hos daglig leder, mens styret på sin side skal sørge for forsvarlig organisering og føre tilsyn med selskapets virksomhet, jf. eksempelvis finansforetaksloven § 8-6.

I DORA-forordningen er «ledelsesorgan» («management body») nevnt i artikkel 5, 13, 17, 28 og 50.

Artikkel 5 gjelder styring, organisering og kontroll av foretakets IKT-risiko. Departementet har en noe annen vurdering enn Advokatforeningen når det kommer til hvilket organ som bør gis plikter etter artikkel 5 i en norskrettslig kontekst. Etter departementets vurdering omfatter ansvaret etter artikkel 5 oppgaver som naturlig faller inn under styrets «påse-plikt». Dette utelukker naturligvis ikke at daglig leder eller andre i foretaket kan bistå styret med å utarbeide retningslinjer mv. De kompetansekravene som artikkel 5 nr. 4 stiller til medlemmene av den finansielle enhetens ledelsesorgan bør etter departementets syn anses å gjelde både for styret og daglig leder, men slik at kravene som stilles i noen grad kan tilpasses organenes rolle, herunder at det vil kunne sees hen til styrets samlede kompetanse.

Artikkel 13 gjelder læring og utvikling. Det følger av artikkel 13 nr. 5 at ledende IKT-ansatte minst én gang i året skal rapportere til ledelsesorganet om resultater fra tester mv. Etter departementets vurdering er dette en rapportering som i norskrettslig kontekst bør gis til styret, mens det vil være naturlig at daglig leder er løpende orientert om tester, resultater mv.

Artikkel 17 stiller krav om at foretakene har en prosess for håndtering av IKT-relaterte hendelser. Etter departementets vurdering er dette oppgaver som i norskrettslig kontekst naturlig tilligger både styret og daglig leder, men slik at styret normalt vil ha en «påse-plikt» mens daglig leder har det utførende ansvaret.

Artikkel 28 oppstiller generelle prinsipper for IKT-risikostyring. Etter departementets vurdering er dette prinsipper som vil gjelde for både styret og daglig leders arbeid når de utfører sine oppgaver i tråd med den selskapsrettslige ansvarsfordelingen.

Artikkel 50 gjelder administrative sanksjoner og avhjelpende tiltak. Etter artikkel 50 nr. 5 kan administrative sanksjoner anvendes på «medlemmer av ledelsesorganet og andre personer som i henhold til nasjonal rett er ansvarlige for overtredelsen». Etter departementets vurdering ville dette kunne være relevant å ilegge både styret og

daglig leder, jf. også forslaget til regler om overtredelsesgebyr omtalt i punkt 2.5.8 og lovforslaget § 4.

Oppsummert mener departementet at pliktene etter DORA må tolkes inn i ansvarsfordelingen mellom styret og daglig leder etter sektorregelverket og norsk selskapsrett. Der hvor det er usikkerhet om ansvarsfordelingen, påhviler det styret i det enkelte foretak å sørge for en avklaring om hva som er eller skal være styrets ansvar og hva som skal være ledelsens (daglig leders) ansvar.

2.5.5 Hendelsesrapportering, informasjonsdeling og testing av motstandsdyktighet

2.5.5.1 Høringsutkastet

Departementet viste i høringsnotatet til at forordningen har en rekke krav til håndtering, klassifisering og rapportering av IKT-hendelser, bl.a. krav etter artikkel 19 om at foretakene skal rapportere til tilsynsmyndigheten om alle alvorlige IKT-hendelser. Nasjonale myndigheter kan fastsette at denne hendelsesrapporteringen (og ev. frivillig innrapportering av vesentlige cybertrusler) også skal gå til tilsynsmyndigheter eller responsmiljøer utpekt etter NIS2-direktivet, jf. punkt 2.4.2.3 over. I høringsnotatet ble det samtidig vist til at det i den norske gjennomføringen av NIS1-direktivet (digitalsikkerhetsloven) er lagt opp til å benytte eksisterende strukturer i størst mulig grad, slik at Finanstilsynet uansett antas å være mottaker av slik ev. rapportering fra foretakene i finanssektoren. Departementet bemerket at 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, og at ev. plikter for foretak i finanssektoren etter digitalsikkerhetsloven uansett bør samordnes med pliktene etter DORA-forordningen.

I høringsnotatet ble det vist til at foretakene etter forordningen artikkel 45 på visse vilkår kan utveksle informasjon og etterretning om cybertrusler. Blant kravene er at foretakene skal informere tilsynsmyndigheten om deltakelse i slike informasjonsutvekslingsordninger.

Departementet pekte også på at foretakene etter forordningen artikkel 24 skal ha et helhetlig program for risikobaserte tester gjennomført av uavhengige parter. Etter artikkel 26 skal de mest betydningsfulle foretakene gjennomføre mer avansert testing i form av trusselbasert penetrasjonstesting («threat-led penetration test», TLPT).

2.5.5.2 Høringsinstansenes syn

Nordic Financial CERT (NFCERT) uttaler følgende om informasjonsdeling:

> «DORA-reguleringens artikkel 45 kan gi et godt grunnlag for at NFCERT og våre medlemmer kan fortsette det viktige arbeidet med samarbeid og informasjonsdeling for å hindre og motstå cyberangrep.
>
> Det er sentralt at myndighetene også bidrar. I det nye globale risikobildet, trenger næringen god informasjon og støtte til å forstå trusselbildet også fra myndigheter med kunnskap om det.»

Norges Bank uttaler følgende om trusselbasert testing:

> «Finanstilsynet og Norges Bank har allerede innført en metode for avansert trusselbasert testing av kritiske funksjoner i finanssektoren. Metoden er basert på et rammeverk fra den europeiske sentralbanken kalt TIBER-EU og er innført i alle de nordiske landene og flere land i Europa. Testingen etter TIBER-NO er frivillig.
>
> Norges Bank har etablert et TIBER Cyber Team (TCT-NO) som veileder banker og andre finansforetak i gjennomføringen av testing etter TIBER-NO. TCT-NO deltar også i grensekryssende tester i regi av andre sentralbanker og har tett samarbeid med de andre nordiske sentralbankene som også har innført TIBER. Det er også etablert et forum (TIBER-NO Forum) hvor alle foretakene som skal teste etter TIBER-NO deltar. Formålet er å diskutere erfaringer med testing og lære av hverandre.
>
> Kapittel 4 i DORA omhandler blant annet avansert sikkerhetstesting, TLPT (Threat-led penetration testing) som er basert på TIBER-EU-rammeverket. TIBER-rammeverket anerkjennes også i DORA, blant annet i fortalens avsnitt 58 (…).»

Nordic Financial CERT (NFCERT) uttaler seg også om slik testing:

> «Reguleringen inneholder også krav om såkalt trusselbasert penetrasjonstesting (TLPT) for enkelte virksomheter. NFCERT fyller i dag behovet for ekstern trusselinformasjon for

TIBER-NO testene, som foregår i regi av Norges Bank og Finanstilsynet. Vi håper at de gode ordningene som er etablert for samarbeid i forbindelse med TIBER-NO testene også kan videreføres for TLPT-tester etter DORA.»

2.5.5.3 Departementets vurdering

Foretakene som underlegges krav om hendelsesrapportering etter DORA-forordningen, skal rapportere om alvorlige hendelser til Finanstilsynet (jf. omtalen av tilsynsmyndighet nedenfor). Selv om konkrete krav, format mv. kan endres med innføringen av forordningen, innebærer rapporteringen i all hovedsak en videreføring av det som følger av dagens regler og praksis.

Som omtalt i høringsnotatet åpner forordningen for at nasjonale myndigheter kan fastsette at hendelsesrapportering også skal gå til kompetente myndigheter eller responsmiljøer (CSIRT-enheter) utpekt etter direktiv (EU) 2022/2555 om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i hele Unionen (NIS2-direktivet), og at frivillig rapportering fra foretakene om vesentlige cybertrusler også skal gå til slike responsmiljøer. Formålet med dette er å sikre god informasjonsflyt også mellom finansforetakene og relevante myndighetsaktører utenfor finansiell sektor, f.eks. slik at foretakene i finanssektoren raskt kan få tilgang til relevante tekniske innspill, oppfølging mv., fra disse aktørene.

I Norge skal NIS1-direktivet gjennomføres i digitalsikkerhetsloven med forskrifter. NIS2-direktivet opphever NIS1-direktivet i EU, men en del bestemmelser er i stor grad videreført, herunder utpeking av kompetente myndigheter og CSIRT-enhet. Digitalsikkerhetsloven er foreløpig ikke trådt i kraft. Dersom det på sikt viser seg å være hensiktsmessig at foretak i finanssektoren rapporterer direkte også til myndighetsaktører utpekt etter nasjonalt regelverk som gjennomfører NIS1-direktivet og på sikt NIS2-direktivet, bør hjemmel til å beslutte dette fremgå av lov om digital operasjonell motstandsdyktighet i finanssektoren.

Departementet foreslår derfor i lovforslaget § 3 tredje ledd en forskriftshjemmel som åpner for at departementet kan fastsette bestemmelser om hendelsesrapportering til, og informasjonsdeling med, andre varslingsmottakere enn Finanstilsynet. Dersom det blir aktuelt å rapportere om hendelser også til andre myndigheter, legger departementet til grunn at rapporteringspliktene bør samordnes.

Forordningen legger etter departementets vurdering godt til rette for at norske foretak kan fortsette å dele informasjon og etterretning knyttet til cybertrusler og sårbarheter, slik mange norske foretak allerede gjør gjennom samhandlingen med Nordic Financial CERT. Regelverket legger også til rette for å bygge videre på arbeidet som er lagt ned i utviklingen av TIBER-NO for avansert trusselbasert testing av foretakenes motstandsdyktighet.

2.5.6 Forholdet til utkontraktering generelt

2.5.6.1 Høringsutkastet

Departementet viste i høringsnotatet til at det etter forordningen artikkel 28 bl.a. er krav om at foretakene skal ha et register over bruk av tjenester fra IKT-leverandører, og minst årlig rapportere til tilsynsmyndigheten. Dersom den avtalte tjenesteleveransen ikke møter kravene i forordningen, skal foretaket stanse den på ordnet måte, og tilsynsmyndigheten skal om nødvendig gi pålegg om retting eller stans. Det ble videre vist til at det etter finanstilsynsloven § 4 c er meldeplikt ved utkontraktering generelt, og at Finanstilsynet om nødvendig kan gripe inn med pålegg. Departementet kommenterte at denne meldeplikten ikke er begrenset til avtaler om IKT-tjenester, og i utgangspunktet derfor bør kunne videreføres. Departementet uttalte likevel at det er 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 hadde ikke inntatt dette i lovutkastet, men uttalte at en ville vurdere det i lys av høringssvarene.

2.5.6.2 Høringsinstansenes syn

Advokatforeningen, *Finans Norge* og *Verdipapirforetakenes Forbund (VPFF)* mener at bestemmelsen i finanstilsynsloven bør endres slik at den bare gjelder annen utkontraktering enn det som omfattes av forordningen. *Finans Norge* uttaler bl.a. følgende:

> «Finans Norge støtter endringer i finanstilsynsloven § 4 c, slik at denne bestemmelsen kun gjelder annen utkontraktering enn det som omfattes av utkastet til ny lov om digital operasjonell motstandsdyktighet i finanssektoren.
>
> Etter Finans Norges syn, er det uhensiktsmessig at finansforetakene pålegges å melde

utkontraktering til Finanstilsynet i to ulike kanaler. Finans Norge ser med fordel at departementet samordner meldeplikten ved utkontraktering. En slik samordning vil sikre konsistens og klarhet i regelverket, samt forhindre at finansforetakene dobbelreguleres på dette punkt.

Vi foreslår at finanstilsynsloven § 4 c første ledd endres til følgende:

§ 4 c.

Foretak som nevnt i § 1 [og som ikke er omfattet av lov om digital operasjonell motstandsdyktighet i finanssektoren] skal melde fra til Finanstilsynet ved inngåelse av avtale om utkontraktering av virksomhet, ved senere [vesentlig] endring av slik avtale og ved bytte av oppdragstaker. Meldingen skal gis minst 60 [20] virkedager før iverksettelsen av avtalen, avtaleendringen eller byttet av oppdragstaker.

Finans Norge foreslår at kravet til meldeplikt ved endringer av avtale, bare bør gjelde ved 'vesentlig' endring. Utkontrakteringsavtaler vil ofte endres løpende som følge av revisjon av standardvilkår og prisendringer mv. Dette er endringer som ikke innebærer noen reell eller vesentlig endring av risikoprofil for den utkontrakterte virksomhet.

Videre foreslås det at fristen for meldeplikt, reduseres fra 60 virkedager til 20 virkedager. Dagens frist på 60 virkedager er uhensiktsmessig lang og lite praktisk anvendelig. Ofte har finansforetakene behov for å gjøre endringer på kort tid som følge av eksterne forhold utenfor deres kontroll.»

Oslo Børs ASA mener at bestemmelsen i finanstilsynsloven ikke kan beholdes i sin nåværende form, da dette ville innebære nasjonale regler i overlapp med en forordning i strid med Norges EØS-forpliktelser, og uttaler bl.a. følgende:

«I dag [har] finanstilsynsloven § 4 c i praksis størst betydning for utkontraktering av IKT-tjenester. Etter nødvendige konsekvenstilpasninger for å sikre at bestemmelsen ikke lengre overlapper med DORA, herunder sikre at utkontraktering av IKT-tjenester ikke omfattes, vil det praktiske anvendelsesområdet være svært begrenset. Bestemmelsen legger også opp til et annet regime for transparens (meldeplikt i forkant) enn det DORA legger opp til (årlig rapportering). Å opprettholde finanstilsynsloven § 4 c om meldeplikt for annen utkontraktering vil derfor medføre en regel av begrenset praktisk betydning, som dertil fragmenterer systematiseringen av meldeplikt ved utkontraktering.

Oslo Børs er av den oppfatning at en slik upraktisk og fragmenterende regel er uhensiktsmessig og uheldig. Når det først er aktuelt å endre finanstilsynsloven, bør anledningen derfor benyttes til å oppheve § 4 c i sin helhet for de foretak som omfattes av DORA. Dersom det for spesifikke avgrensede områder skulle være behov for særregulering av utkontraktering må det gjøres gjennom særlovgivningen og ikke gjennom generell tilsynslovgivning. Reglen om utkontraktering i finanstilsynsloven § 4 c har et uavklart forhold til flere sektorspesifikke EØS-rettsakter. Etterlevelse av Norges EØS-forpliktelser tilsier at et forhold som utkontraktering reguleres i samme nasjonale sektorlovgivning som tilhørende EØS rettsakt. En slik tilnærming vil legge til rette for at de nødvendige forhold utredes opp mot relevante EØS rettsaker.»

Finansforbundet uttaler følgende:

«Finansforbundet har tidligere kritisert utflagging av tjenester, blant annet grunnet tap av kompetanse. Utfordringen med å ha for lite kompetanse er at vi mister verdifull bestiller-, innkjøps- og kontrollkompetanse, noe Finansmarkedsmeldingen også belyser. Finansforbundet har videre merket seg at totalberedskapskommisjonen mener det er avgjørende at finansnæringen har et bevisst forhold til hvilken kompetanse som ikke bør utkontrakteres. Vi vil understreke at det er avgjørende med god oppfølging når det gjelder dette området. Det er positivt at Finanstilsynet har vedtatt forskrift om meldeplikt ved utkontraktering av virksomhet og utarbeidet et eget rundskriv om utkontraktering. Vi mener videre det er grunnlag for å undersøke nærmere hvilke erfaringer næringen har gjort seg med det å legge IKT-funksjoner til land utenfor Norge, for å kartlegge hvilke konsekvenser dette har med hensyn til å kunne ivareta kritisk kompetanse i Norge.»

2.5.6.3 Departementets vurdering

DORA-forordningen har omfattende krav til foretakenes avtaler om bruk av tjenester fra IKT-leverandører, herunder hvordan tilsynsmyndigheten skal informeres om avtaler og planlagte avtaler.

Dersom foretaket ikke innretter seg etter forordningens krav, kan tilsynsmyndigheten gripe inn med pålegg om retting eller stans. Finanstilsynsloven § 4 c har regler om bl.a. meldeplikt og inngripsmulighet før utkontraktering som ikke synes å samsvare med forordningens system. Videreføring av lovbestemmelsen kan derfor være i strid med Norges forpliktelser etter EØS-avtalen. Selv om et viktig formål med finanstilsynsloven § 4 c er kontroll med utkontraktering av virksomhet som omfattes av forordningen, gjelder den imidlertid også annen type utkontraktering som Finanstilsynet bør få informasjon om og ha mulighet for å gripe inn overfor. Departementet foreslår derfor, som nevnt i høringsnotatet, at finanstilsynsloven § 4 c endres slik at bestemmelsen bare gjelder annen utkontraktering enn det som omfattes av forordningen. Siden bestemmelsen er vedtatt videreført i ny finanstilsynslov, innebærer lovforslaget endring av *lov 21. juni 2024 nr. 41 om Finanstilsynet* § 4-6.

Etter DORA-forordningen artikkel 28 skal foretakene ha et register med oversikt over bruk av tjenester fra IKT-leverandører, som på forespørsel skal gjøres tilgjengelig for tilsynsmyndigheten. Foretakene skal dessuten 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. EU-kommisjonen kan fastsette nærmere regler om informasjonen som skal inngå i det nevnte registeret, men når det gjelder hyppighet, format mv. for annen informasjon om inngåtte og planlagte avtaler som etter forordningen skal nå tilsynsmyndigheten, vil det være hensiktsmessig at tilsynsmyndigheten utarbeider en veiledning. Hvilken informasjon tilsynsmyndigheten forventer å motta om inngåtte og planlagte avtaler, samt tilsynsmyndighetens behandling av informasjonen, vil da være forutsigbar for foretakene. Det samme gjelder tilsynsmyndighetens forventninger til informasjonens format og hyppighet. En veiledning vil også medføre en standardisering/forenkling for foretakene og en forenkling av tilsynsmyndighetens saksbehandling. Selv om tilsynsmyndigheten utarbeider en veiledning, kan det bli behov for at departementet gir nasjonale regler. Departementet foreslår derfor en forskriftshjemmel som gir mulighet for å fastsette utfyllende krav til rapporteringen og annen informasjon som skal gis Finanstilsynet om inngåtte og planlagte avtaler om bruk av tjenester fra IKT-leverandører. Det vises til lovforslaget § 3 annet ledd.

2.5.7 Tilsyn mv.

2.5.7.1 Høringsutkastet

Departementet viste i høringsnotatet til at Finanstilsynet er tilsynsmyndighet for foretakene som omfattes av forordningen (unntatt IKT-leverandører), og i utkastet til lov om digital operasjonell motstandsdyktighet i finanssektoren § 3 ble 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. Departementet la 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 bemerket departementet at forordningen innfører 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. 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. Departementet viste til at det etter innlemmelse av forordningen i EØS-avtalen kan 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. Departementet viste i den forbindelse til at et av prinsippene for EØS-tilpasninger er at bindende vedtak som de felleseuropeiske tilsynsmyndighetene etter regelverket skal kunne fatte i EU, skal fattes av EFTAs overvåkingsorgan i EØS/EFTA-landene. Departementet antok deretter at 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 ble også antatt å få i oppgave å følge opp de norske finansielle foretakenes håndtering av risiko som identifiseres i anbefalinger til IKT-leverandører.

Departementet pekte i høringsnotatet på at tilsynsmyndigheten etter forordningen artikkel 26 nr. 8 skal identifisere hvilke foretak som skal ha krav om å gjennomføre avansert testing i form av trusselbasert penetrasjonstesting («threat-led

penetration test», TLPT). Videre ble det vist til at den ansvarlige myndigheten for TLPT er tilsynsmyndigheten, med mindre det bestemmes noe annet nasjonalt etter artikkel 26 nr. 9 og 10.

2.5.7.2 Høringsinstansenes syn

Norges Bank uttaler bl.a. følgende om den ansvarlige myndigheten for TLPT:

> «Vi forstår [artikkel 26] nr. 9 slik at landene kan peke ut en myndighet som skal ha ansvar for TLPT på nasjonalt nivå. Det følger av nr. 10 at dersom det ikke skjer en utpeking av myndighet med ansvar for TLPT etter nr. 9 kan den kompetente myndigheten delegere noen eller alle oppgavene som følger av artikkel 26 og artikkel 27 til en annen nasjonal myndighet i finanssektoren. Kompetent myndighet for DORA (Finanstilsynet) vil ha tilgang til resultatene fra en test som en del av tilsynsvirksomheten.»

Norges Bank viser til at det i Danmark er planlagt å utpeke sentralbanken som TLPT-myndighet, og at dette er omtalt bl.a. slik i et dansk lovforslag:

> «Det er forventningen, at bemyndigelsen vil blive udnyttet til at fastsætte regler, der udpeger Danmarks Nationalbank som ansvarlig myndighed i henhold til DORA-forordningens artikel 26, stk. 9. Såfremt Danmarks Nationalbank udpeges som ansvarlig myndighed vil de være ansvarlig for TLPT-relaterede anliggender for alle virksomheder, der skal gennemføre TLPT, hvilket også omfatter at udpege de virksomheder, der skal pålægges at gennemføre TLPT, herunder operatører af finansiel digital infrastruktur ().»

Norges Bank mener at «det bør innføres en mulighet for å eksplisitt kunne utpeke TLPT-myndighet etter artikkel 26 nr. 9 i Norge». Dette vil ifølge Norges Bank gi «en fleksibilitet som er i tråd med intensjonene i DORA for hvordan organiseringen av TLPT Cyber Team (TCT) skal være». Norges Bank foreslår derfor at Finansdepartementet vurderer om det er behov for å gjøre tilpasninger i norsk lovtekst for å kunne utpeke TLPT-myndighet etter DORA-forordningen artikkel 26 nr. 9.

2.5.7.3 Departementets vurdering

Som det ble vist til i høringsnotatet er Finanstilsynet tilsynsmyndighet for foretakene som omfattes av forordningen (unntatt IKT-leverandører), og skal derfor også være nasjonal tilsynsmyndighet etter forordningen. Dette foreslås angitt uttrykkelig i loven. Foruten å føre tilsyn med foretakenes overholdelse av bestemmelser i forordningen, innebærer dette bl.a. at Finanstilsynet skal 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. Det vises til lovforslaget § 3 første ledd.

Departementet viste i høringsnotatet til at det etter innlemmelse av forordningen i EØS-avtalen 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 omtalt i punkt 2.6 skal EFTAs overvåkingsorgan (ESA) ha denne rollen i EØS/EFTA-landene.

Som Norges Bank viser til i sitt høringssvar, kan det etter forordningen artikkel 26 nr. 9 pekes ut en myndighet som skal ha ansvar for trusselbasert penetrasjonstesting («threat-led penetration test», TLPT) på nasjonalt nivå, og denne myndigheten må i tilfelle gis all vedtakskompetanse og alle oppgaver som er nødvendig for å ivareta en slik funksjon. Dersom det ikke utpekes en slik myndighet, er det tilsynsmyndigheten som skal ivareta funksjonen som TLPT-myndighet, men tilsynsmyndigheten kan da delegere noen av eller alle oppgavene til en annen myndighet i finanssektoren. En slik delegasjonsløsning vil imidlertid ikke være anvendelig mellom Finanstilsynet og Norges Bank.

TLPT-myndighetens oppgaver og myndighet følger av forordningen artikkel 26 og 27. Når en TLPT er gjennomført, skal foretaket etter artikkel 26 nr. 6 oversende sammendrag av funn, forbedringsplaner og dokumentasjon til TLPT-myndigheten. Etter artikkel 26 nr. 7 er det angitt at «myndigheter» deretter skal gi en attest på at testen er korrekt gjennomført. Siden det er TLPT-myndigheten som etter nr. 6 skal motta den relevante informasjonen fra foretaket, forstår departementet «myndigheter» i nr. 7 som TLPT-myndigheten. Etter artikkel 27 nr. 2 bokstav a må TLPT-myndigheten godkjenne ev. bruk av interne testere. Etter artikkel 26 nr. 11 kan EU-kommisjonen fastsette tekniske standarder for TLPT i samsvar med TIBER-rammeverket fra Den europeiske sentralbanken (ESB). I et forslag til tekniske standarder oversendt fra de felles-

europeiske tilsynsmyndighetene til EU-kommisjonen 17. juli 2024 er det angitt en rekke oppgaver for TLPT-myndigheten, herunder at denne myndigheten skal avgjøre hvilke foretak som skal pålegges å gjennomføre TLPT, hvilket kan synes å stride med DORA-forordningen artikkel 26 nr. 8, som angir at tilsynsmyndigheten skal ha denne myndigheten. I det danske lovforslaget sitert av Norges Bank legges det på den annen side også til grunn at det er TLPT-myndigheten som skal avgjøre dette. Det danske lovforslaget ble for øvrig vedtatt som foreslått i mai 2024. De felleseuropeiske tilsynsmyndighetenes forslag til tekniske standarder innebærer videre at TLPT-myndigheten bl.a. skal delta i alle stadier av testingen, godkjenne en del av forutsetningene for testingen og samarbeide med andre lands TLPT-myndigheter (bl.a. om testing av foretak med virksomhet i flere land).

Uavhengig av om det utpekes en TLPT-myndighet, har tilsynsmyndigheten en rekke oppgaver relatert til TLPT. Som nevnt følger det av forordningen artikkel 26 nr. 8 at tilsynsmyndigheten skal identifisere hvilke foretak som skal pålegges å gjennomføre TLPT, i tillegg til at tilsynsmyndigheten etter artikkel 26 nr. 2 skal validere hvilke kritiske eller viktige funksjoner som skal omfattes av TLPT, og etter artikkel 27 nr. 2 verifisere at et foretak som ønsker å bruke interne testere, setter av tilstrekkelige ressurser og innretter testingen på en måte som unngår interessekonflikter. Etter det nevnte forslaget til tekniske standarder skal tilsynsmyndigheten bl.a. motta en tiltaksplan fra foretaket etter testen, og det er angitt at tilsynsmyndigheten og TLPT-myndigheten skal dele all relevant informasjon med hverandre.

Norges Bank og Finanstilsynet har begge ansvar og kompetanse som er relevant for utøvelsen av myndighetsoppgaver innen TLPT etter DORA-forordningen. Begge skal fremme stabilitet i det finansielle systemet og har tung kompetanse innen vurderinger av system- og cyberrisiko. Norges Bank skal også fremme et effektivt og sikkert betalingssystem. Finanstilsynet fører tilsyn med hele bredden av foretak i finanssektoren, herunder med foretakenes bruk av IKT og ytelse av betalingstjenester, og har som tilsynsmyndighet tilgang til omfattende og detaljert informasjon om foretakene. Finanstilsynet og Norges Bank har i dag et etablert samarbeid om TLPT etter TIBER-NO-rammeverket. Etter departementets vurdering er det viktig at Norges Bank og Finanstilsynet etablerer et godt samarbeid om TLPT etter DORA-forordningen for foretak i den norske finanssektoren, jf. at vurderingen av hvilke foretak som skal pålegges testing, bl.a. skal baseres på foretakets betydning for finanssektoren og finansiell stabilitet på nasjonalt og europeisk nivå, samt foretakets IKT-risikoprofil. Departementet antar at slike vurderinger må bygge på informasjon og vurderinger bl.a. fra det løpende tilsynet (og ev. ses i sammenheng med annen tilsynsmessig oppfølging) og analyser på systemnivå. For å legge til rette for at samarbeidet og oppgavedelingen mellom Finanstilsynet og Norges Bank i tilknytning til TLPT-testing etter DORA-forordningen kan formaliseres, foreslår departementet at det tas inn en forskriftshjemmel om dette i lovforslaget § 3 fjerde ledd.

2.5.8 Sanksjoner

2.5.8.1 Høringsutkastet

Departementet viste i høringsnotatet til at Finanstilsynet vil måtte kunne ilegge administrative sanksjoner ved overtredelser av det nye regelverket, jf. forordningen artikkel 51. Departementet la foreløpig til grunn at det bare ville være aktuelt med overtredelsesgebyr, og at andre sanksjoner som f.eks. ledelseskarantene ikke vil være relevant ved brudd på forordningskravene. Departementet uttalte deretter at 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 som overtredelse av bl.a. de generelle kravene til organisering av verdipapirforetakenes virksomhet etter verdipapirhandelloven.

I lovutkastet ble det derfor foreslått at Finanstilsynet kan ilegge overtredelsesgebyr ved overtredelse av bestemmelser gitt i eller medhold av loven, jf. at forvaltningsorganer etter forvaltningsloven § 44 første ledd kan ilegge overtredelsesgebyr når det er fastsatt i lov. 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. På grunnlag av et forslag fra Finanstilsynet i 2019 om overtredelsesgebyr på ulike områder, inntok departementet i lovutkastet en foreløpig grense for overtredelsesgebyr på inntil 50 millioner kroner både for foretak og enkeltpersoner. Det ble kommentert at 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, og videre at:

> «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.»

Departementet viste til at 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. Etter lovutkastet kan fysiske personer ilegges overtredelsesgebyr for forsettlige eller uaktsomme overtredelser, mens foretak kan ilegges overtredelsesgebyr når foretaket eller noen som har handlet på foretakets vegne, forsettlig eller uaktsomt har begått en overtredelse. Departementet uttalte følgende om hva slags overtredelser som skal kunne sanksjoneres:

> «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 ble 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-risikostyring,
- 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 alvorlige 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.

Departementet ba om innspill fra høringsinstansene til disse vurderingene.

2.5.8.2 Høringsinstansenes syn

Finans Norge mener den øvre rammen for overtredelsesgebyr er for høy, og at det tydelig bør angis hvilke handlinger eller unnlatelser som kan føre til ileggelse av overtredelsesgebyr, bl.a. med henvisning til at overtredelsesgebyr etter EMK er å anse som straff. Finans Norge skriver videre bl.a. at:

> «Finans Norge er av den oppfatning at overtredelsesgebyr på inntil 50 millioner kroner er for høy. Generelt gir en høy øvre ramme signaler om at gebyrenes størrelse er lite gjennomtenkt. En høy øvre ramme skaper også en forventning om at rammene skal benyttes av Finanstilsynet, med den konsekvens at Finanstilsynets rom for skjønnsutøvelse blir videre enn nødvendig. Dette bidrar til å svekke finansforetakenes rettssikkerhet og forutberegnelighet. Finans Norge ber derfor om at den øvre rammen på overtredelsesgebyrene reduseres.
>
> Med hensyn til foreldelse, bør reglene harmoniseres med tilsvarende bestemmelser i tilstøtende regelverk. Vi foreslår at adgangen til å ilegge overtredelsesgebyr foreldes fem år etter at overtredelsen er opphørt, og at fristen avbrytes ved at Finanstilsynet gir forhåndsvarsel eller fatter vedtak om overtredelsesgebyr. (…)

For Finans Norge er det viktig at finansforetakenes rettssikkerhet og forutberegnelighet blir ivaretatt ved ileggelse av overtredelsesgebyr. For eksempel må finansforetakene gis en reell mulighet til å klage på vedtak om overtredelsesgebyr, og vedtaket må kunne overprøves av domstolene. Finans Norges forutsetter at EMKs krav til 'rettferdig rettergang' etterleves ved ileggelse av overtredelsesgebyr. Vi viser særlig til behandlingen av administrative sanksjoner og forholdet til EMK i Prop. 62 L (2015–2016).

Avslutningsvis, ønsker Finans Norge å påpeke at det er uheldig at Finanstilsynet som offentlig myndighet fungerer som utreder av nytt regelverk eller etter fullmakt fastsetter nytt regelverk, tolker det samme regelverket, kontrollerer at regelverket etterleves, og skal ilegge finansforetakene overtredelsesgebyr ved eventuelle brudd på etterlevelsen av regelverket. (…)»

Advokatforeningen viser til at flere av bestemmelsene hvis overtredelse etter høringsutkastet skal kunne sanksjoneres med overtredelsesgebyr, er generelle og konkretiseres i andre bestemmelser, og at det i høringsnotatet står at «hensynet til klarhet og forutberegnelighet kan tilsi at også de bestemmelsene som utdyper de overordnede bestemmelsene angis særskilt i loven». Advokatforeningen støtter denne vurderingen, og mener at det vil være hensiktsmessig å inkludere også de utdypende bestemmelsene slik at det ikke er tvil om hvilke bestemmelser som kan utløse overtredelsesgebyr ved brudd.

Advokatforeningen skriver også at den ikke har innvendinger til administrative sanksjoner som sådan, men «minner om at å ilegge administrative sanksjoner er å regne som straff etter EMK», og «savner derfor en grundigere vurdering av de rettssikkerhetsmessige aspektene ved innføringen og bruken av denne type hjemler». Advokatforeningen ber dessuten om at det «vurderes nærmere hvorvidt dagens saksbehandlingsordning, herunder klagesaksbehandlingstiden, er i samsvar med kravene til en forsvarlig saksbehandling».

Oslo Børs ASA mener det vil gi økt klarhet, og derfor være mer pedagogisk hensiktsmessig, å «gi presise henvisninger også der overordnede handlingsnormer (slik som artikkel 6) utfylles av konkretiserende regler i andre bestemmelser (artikkel 7-10)». Klare henvisninger er ifølge Oslo Børs «særlig av betydning dersom dokumentinterne henvisninger fremgår mer implisitt enn eksplisitt».

Verdipapirforetakenes Forbund (VPFF) uttaler følgende:

«Etter VPFFs oppfatning er det svært viktig at det er tydelighet rundt sanksjoner og kriteriene for når bøter kan ilegges for brudd på bestemmelser i DORA. 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.

Når det nå skal kunne ilegges overtredelsesgebyr på inntil 50 millioner kroner på et 'nytt område,' er transparens og forutsigbarhet essensielt.

VPFF mener det klart bør fremgå hvilke bestemmelser i forordningen som vil kunne sanksjoneres med overtredelsesgebyr, grad av skyld som kreves, samt hvilke beløpsgrenser som gjelder for de konkrete overtredelsene av ulike bestemmelser.»

Næringslivets Hovedorganisasjon (NHO) uttaler bl.a. følgende:

«Det er foreslått at 'medvirkning' til overtredelse skal kunne sanksjoneres 'på samme måte' som overtredelse. Medvirkning er derfor uttrykkelig en annen handling eller unnlatelse enn dem som er regnet opp i første ledd. Det gjelder da krav til klarhet og forutberegnelighet også når det gjelder innholdet i medvirkning.

Vi er enig i at det må være tydelig hvilke handlinger og unnlatelser som kan føre til ileggelse av overtredelsesgebyr. Det er positivt at det er fremhevet i høringsnotatet. Flere av forordningskravene er ganske overordnede. Det gjør det temmelig vanskelig for dem som skal etterleve kravene å vite hvilke overtredelser som er sanksjonerbare. Den forskriftshjemmelen som er foreslått, bør derfor utformes slik at det er mulig å både tydeliggjøre og innskrenke sanksjonsadgangen i første ledd.»

Finansforbundet uttaler følgende:

«Finansforbundet vil påpeke at det allerede er et omfattende lovverk som muliggjør sanksjoner knyttet til digital sikkerhet, herunder digitalsikkerhetsloven, finansforetaksloven og finanssikkerhetsloven. Slik vi forstår det vil dette kunne innebære at finansvirksomheter kan få ilagt sanksjoner for samme over-

tredelse i henhold til flere lovverk. Det bør foretas en gjennomgang av sanksjonsordningene i de ulike lovverkene med henblikk på at de innskrenkes for ikke å overlappe. Vi understreker at det særlig for små aktører er hensiktsmessig med forutsigbarhet med hensyn til hvilke regler som vil gjelde for ulike overtredelser.»

2.5.8.3 Departementets vurdering

Departementet foreslår at overtredelser av nærmere angitte bestemmelser i forordningen skal kunne sanksjoneres med overtredelsesgebyr. Departementet viste i høringsnotatet til at en ville 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 høringen har flere instanser pekt på viktigheten av at det tydelig fremgår hvilke overtredelser som kan gi grunnlag for overtredelsesgebyr, og at det kan være nødvendig at også utdypende forordningsbestemmelser angis i loven. Departementet har derfor foretatt en ny vurdering av hvilke bestemmelser som bør omfattes av en hjemmel for Finanstilsynet til å ilegge overtredelsesgebyr. Foruten bestemmelsene som er nevnt i høringsutkastet, mener departementet at overtredelse av følgende bestemmelser potensielt kan ha store negative konsekvenser, og derfor bør kunne sanksjoneres med overtredelsesgebyr:

- artikkel 8 om identifisering av IKT-relaterte funksjoner og avhengigheter,
- artikkel 9 nr. 4 om retningslinjer for sikkerhet mv. som del av rammeverket for IKT-risikostyring, jf. artikkel 6,
- artikkel 14 om planer for krisekommunikasjon,
- artikkel 16 om forenklet rammeverk for IKT-risikostyring,
- artikkel 25 nr. 2 om sårbarhetsvurderinger før bruk av nye systemer i verdipapirsentraler og sentrale motparter,
- artikkel 42 nr. 3 annet avsnitt om hensyntaken til risiko avdekket hos IKT-leverandører, og
- tekniske reguleringsstandarder (nivå 2-regelverk) fastsatt med hjemmel i artikkel 15 og artikkel 16 nr. 3.

I tråd med forslaget i høringsutkastet foreslås det at fysiske personer kan ilegges overtredelsesgebyr for forsettlige eller uaktsomme overtredelser, mens foretak kan ilegges overtredelsesgebyr når foretaket eller noen som har handlet på foretakets vegne, forsettlig eller uaktsomt har begått en overtredelse. Det foreslås videre at medvirkning til overtredelser som nevnt ovenfor, kan sanksjoneres på samme måte.

Når det gjelder hvilken beløpsgrense som bør gjelde for gebyr ved overtredelse av de nevnte bestemmelsene, baserte departementet seg i høringsnotatet på et forslag fra Finanstilsynet i 2019 om overtredelsesgebyr på ulike områder, og inntok en foreløpig gebyrgrense på 50 mill. kroner for foretak og fysiske personer. Finans Norge mener at denne grensen er for høy. Etter departementets vurdering er det imidlertid viktig at Finanstilsynet får mulighet for å ilegge gebyr av en størrelse som kan bidra til god etterlevelse av et viktig regelverk. De nye reglene som innføres med forordningen, blir svært viktige for å bidra til forsvarlig innretning og drift av systemer av avgjørende betydning for stabiliteten i tilgangen på finansielle tjenester. Departementet mener derfor at Finanstilsynet bør kunne ilegge forholdsvis høye gebyrer. Departementet har sett hen til bl.a. rammene for gebyr ved overtredelse av kravene til organisering av verdipapirforetakenes virksomhet etter verdipapirhandelloven. Etter verdipapirhandelloven § 21-5 kan det for foretak fastsettes overtredelsesgebyr på inntil 43 mill., eller opptil 10 pst. av den samlede årsomsetningen etter siste godkjente årsregnskap, og for fysiske personer inntil 43 mill. kroner. Gebyret kan dessuten fastsettes til inntil to ganger oppnådd fortjeneste eller unngått tap som følge av overtredelsen, dersom dette gir høyere gebyr.

Departementet foreslår at adgangen til å ilegge overtredelsesgebyr foreldes fem år etter at overtredelsen er opphørt. Fristen avbrytes ved at Finanstilsynet gir forhåndsvarsel eller fatter vedtak om overtredelsesgebyr.

Departementet foreslår videre en hjemmel for departementet til å fastsette forskrift til utfylling og avgrensning av paragrafen om overtredelsesgebyr, herunder om renter ved forsinket betaling. Det foreslås også en hjemmel for departementet til å fastsette i forskrift at overtredelse av forskriftsbestemmelser gitt i medhold av loven, kan ilegges overtredelsesgebyr.

Det vises til lovforslaget § 4.

2.5.9 Andre spørsmål

Finansforbundet har i sitt høringssvar etterlyst nye regler for behandling av personopplysninger i arbeidslivet, og anført at personvernforordningen åpner for å fastsette nærmere regler

for behandling av arbeidstakeres personopplysninger i ansettelsesforhold. Finansforbundet har også tatt opp at ansatte som skal følge opp etterlevelse av regelverket bør tilbys tilstrekkelig kompetanseheving, og pekt på tilrettelegging hos finansinstitusjonene og utvikling av kompetansetilbud fra utdanningsinstitusjonene. Departementet ser at dette er spørsmål av betydning for ansatte i finanssektoren, samtidig som det ikke er grunnlag for oppfølging av innspillene i den foreliggende lovsaken.

2.5.10 Tilpasninger i annet regelverk

2.5.10.1 Høringsutkastet

Forordnings- og direktivendringene som er omtalt i punkt 2.4, 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-forordningen), i tillegg til endringer for å sikre konsistens med kravene og begrepsbruken i forordningen. Departementets utkast til endringslov i høringsnotatet innebar slike tilpasninger i verdipapirhandelloven, verdipapirfondloven, lov om forvaltning av alternative investeringsfond, lov om kredittvurderingsbyråer, finansforetaksloven, referanseverdiloven og verdipapirsentralloven.

2.5.10.2 Høringsinstansenes syn

Ingen av høringsinstansene har hatt merknader til denne delen av høringsutkastet.

2.5.10.3 Departementets vurdering

Departementet foreslår endringer i verdipapirhandelloven, verdipapirfondloven, lov om forvaltning av alternative investeringsfond, lov om kredittvurderingsbyråer, finansforetaksloven, referanseverdiloven og verdipapirsentralloven i tråd med høringsutkastet. I tillegg foreslås en endring i ny finanstilsynslov § 4-6, jf. omtale i punkt 2.5.6.3.

2.5.11 Ikrafttredelse

DORA-forordningen har vært gjeldende i EU siden 17. januar 2025. I Norge kan forordningen tidligst tre i kraft når EØS-komitébeslutningen om innlemmelse trer i kraft, se punkt 2.6.

2.6 Samtykke til godkjenning av EØS-komiteens beslutning nr. 40/2025 om innlemmelse av DORA i EØS-avtalen

2.6.1 Bakgrunn

EØS-komiteen traff 20. februar 2025 beslutning om å endre EØS-avtalens vedlegg IX ved innlemmelse av Europaparlaments- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet for finansområdet og endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 og europaparlaments- og rådsdirektiv (EU) 2022/2556 av 14. desember 2022 om endring av direktiv 2009/65/EC, 2009/138/EC, 2011/61/EU, 2013/36/EU, 2014/59/EU, (EU) 2015/2366 og (EU) 2016/2341 (DORA), jf. EØS-komitébeslutning nr. 40/2025.

Det kreves lovendringer i norsk rett for å gjennomføre forordning (EU) 2022/2554 (DORA-forordningen) og direktiv (EU) 2022/2556 (endringsdirektiv). Stortingets samtykke til godkjennelse av EØS-komiteens beslutning er derfor nødvendig etter Grunnloven § 26 annet ledd. Forslag til lovendringer som gjennomfører forordning (EU) 2022/2554 og direktiv (EU) 2022/2556 følger av denne proposisjonen.

Forordning (EU) 2022/2554 og direktiv (EU) 2022/2556 er nærmere omtalt i punkt 2.2 ovenfor. Forordningene og EØS-komitébeslutningen i uoffisiell norsk oversettelse følger vedlagt.

2.6.2 Overordnet omtale av EØS-komiteens beslutning

EØS-komiteens beslutning nr. 40/2025 av 20. februar 2025 om innlemmelse av DORA-forordningen og endringsdirektivet inneholder en fortale og fire artikler.

Artikkel 1 fastsetter at forordning (EU) 2022/2554 og direktiv (EU) 2022/2556 innlemmes i EØS-avtalen vedlegg IX med enkelte tilpasninger.

Artikkelen fastsetter enkelte tekniske EØS-tilpasninger til forordningen, bl.a. slik at EFTAs overvåkningsorgan (ESA) gis kompetanse der de europeiske tilsynsmyndighetene (det vil si Den europeiske banktilsynsmyndigheten (EBA), Den europeiske tilsynsmyndigheten for forsikring og tjenestepensjon (ESMA) og Den europeiske verdipapir- og markedstilsynsmyndigheten (ESMA), heretter samlet omtalt som «EUs tilsynsmyndigheter» eller «EU-tilsynsmyndigheter») etter for-

ordningen er gitt kompetanse overfor EUs medlemsstater. Som nevnt i punkt 2.5.7 innfører DORA-forordningen et rammeverk for overvåkning på EU-nivå av IKT-leverandører som anses som kritiske iht. forordningen, jf. omtale i avsnitt 2.4.2.6 og 2.5.7. EØS-komitébeslutningen slår fast at ESA skal ha kompetanse som i forordningen er gitt til EUs tilsynsmyndigheter overfor kritiske IKT-leverandører som er etablert i en EØS/EFTA-stat eller som er etablert i et tredjeland, men har et datterforetak i en EØS/EFTA-stat, i tråd med EØS-tilpasningen til EUs finanstilsynsbyråstruktur, som Stortinget samtykket til 13. juni 2016 i tråd med forslag i Prop. 100 S (2015–2016). Dette er nærmere omtalt i punkt 2.6.4.

Artikkel 2 fastslår at den islandske og den norske språkversjonen av forordningene skal være offisielle språkversjoner og kunngjøres i EØS-tillegget til Den europeiske unions tidende, jf. EØS-avtalen artikkel 129 nr. 1.

Artikkel 3 fastsetter at EØS-komitébeslutningen skal tre i kraft 21. februar 2025, forutsatt at konstitusjonelle forbehold etter artikkel 103 nr. 1 i EØS-avtalen er hevet.

Av *artikkel 4* følger det at beslutningen skal kunngjøres i EØS-avdelingen og i EØS-tillegget til Den europeiske unions tidende.

2.6.3 Tilpasninger til overvåkingsrammeverket for kritiske IKT-foretak

I DORA-forordningen gis de tre felleseuropeiske tilsynsmyndighetene (EBA, ESMA og EIOPA) myndighet til å bl.a. utpeke, overvåke og pålegge administrative sanksjoner for kritiske IKT-leverandører. Gjennom tilpasningene i EØS-komitébeslutningen artikkel 1 nr. 3 er myndigheten som legges til EUs tilsynsmyndigheter overfor fysiske og juridiske personer i EUs medlemsstater, gitt til EFTAs overvåkningsorgan (ESA) når disse er etablert i en EØS/EFTA-stat eller i et tredjeland, men med et datterforetak i en EØS/EFTA-stat. Rammeverket og de ulike myndighetene som gjennom EØS-komitébeslutningen legges til ESA, er nærmere beskrevet i det følgende.

Etter DORA-forordningen artikkel 31 nr. 1 skal de felleseuropeiske tilsynsmyndighetene, gjennom EU-tilsynsmyndighetenes felles komité, utpeke IKT-leverandørene som er kritiske for finansielle foretak, etter anbefaling fra et overvåkingsforum bestående av representanter fra de felleseuropeiske tilsynsmyndighetene, relevante nasjonale tilsynsmyndigheter fra alle medlemsstatene, observatører fra EU-kommisjonen, ESRB, ESB, ENISA og, der relevant, observatører fra nasjonale tilsynsmyndigheter utpekt i henhold til direktiv (EU) 2022/2555 (NIS2-direktivet), jf. forordningen artikkel 32 nr. 4. Vurderingen av hvilke IKT-leverandører som skal anses som kritiske skal baseres på kriterier som fremgår av forordningen artikkel 31 nr. 2, se nærmere omtale i proposisjonens punkt 2.4.2.6. Videre skal de felleseuropeiske tilsynsmyndighetene, gjennom EU-tilsynsmyndighetenes felles komité og etter anbefaling fra overvåkingsforumet, utpeke den av de felleseuropeiske tilsynsmyndighetene som skal følge opp hver kritiske IKT-leverandør i rollen som hovedovervåker, avhengig av hvilken del av finanssektoren IKT-leverandøren har størst betydning for. DORA-forordningen artikkel 31 nr. 3 spesifiserer at når en IKT-leverandør inngår i konsern, skal vurderingen av om leverandøren oppfyller kravene for å anses som kritisk, ses i sammenheng med IKT-tjenestene som leveres av konsernet som helhet. Kritiske IKT-leverandører som er del av konsern, skal etter forordningen artikkel 31 nr. 4 utpeke en juridisk person for kontakt med hovedovervåker.

EØS-komitébeslutningen *artikkel 1 nr. 3 (i)* slår fast at ESA skal ha ansvar for å utpeke kritiske IKT-leverandører dersom disse er etablert i en EØS/EFTA-stat eller i et tredjeland, men med et datterforetak i en EØS/EFTA-stat. Utpekingen skal skje etter anbefaling fra overvåkningsforumet og på grunnlag av utkast forberedt av den ansvarlige EU-tilsynsmyndigheten. For IKT-leverandører som inngår i konsern som består av enheter som har aktivitet i både en EU-stat og i en EØS/EFTA-stat, skal ESA, i tråd med dette og i henhold til systemet for tilpasninger til topilarsystemet i EØS-avtalen, være kompetent myndighet dersom den juridiske personen som er utpekt etter DORA-forordningen artikkel 31 nr. 4, er etablert i en EØS/EFTA-stat.

Videre slår EØS-komitébeslutningen *artikkel 1 nr. 3 bokstav i punkt (ii)* fast at ESA skal være hovedovervåker for hver kritiske IKT-leverandør som er etablert i en EØS/EFTA-stat eller er etablert i et tredjeland, så lenge leverandøren har et datterforetak etablert i en EØS/EFTA-stat. De felleseuropeiske tilsynsmyndighetene, gjennom sin felles komité, skal utpeke hvilken av de felleseuropeiske tilsynsmyndighetene som skal assistere ESA i utøvelsen av sin rolle under forordningen, inkludert gjennom å forberede utkast. EØS-komitébeslutningen slår videre fast at ESA skal notifisere kritiske IKT-leverandører som faller inn under sitt ansvarsområde (jf. artikkel 1 nr. 3 bokstav j).

I henhold til DORA-forordningen artikkel 31 nr. 11 kan IKT-leverandører som ikke er utpekt som kritiske av de felleseuropeiske tilsynsmyndighetene, søke om å bli utpekt som kritiske. EØS-komitébeslutningen *artikkel 1 nr. 3 bokstav l* slår fast at IKT-leverandører som er etablert i en EØS/EFTA-stat, skal sende slik søknad til ESA. Beslutningen om å utpeke IKT-leverandører som kritiske etter forespørsel iht. DORA-forordningen artikkel 31 nr. 11, skal tas av ESA på basis av utkast forberedt av den ansvarlige EU-tilsynsmyndigheten.

Noen IKT-leverandører er unntatt DORA-forordningens regler om kritiske IKT-leverandører. Dette gjelder bl.a. leverandører som er konserninterne, eller leverandører som tilbyr IKT-tjenester i kun én medlemsstat til finansielle foretak som kun er aktive i denne medlemsstaten. Også IKT-leverandører som allerede er underlagt et overvåkningsrammeverk fordi de understøtter grunnleggende oppgaver som tilligger Det europeiske system av sentralbanker (ESSB) etter Traktaten om Den europeiske unions funksjonsmåte (TFEU) artikkel 127 nr. 2, er unntatt. Disse oppgavene er å utforme og gjennomføre EUs pengepolitikk, å foreta transaksjoner i utenlandsk valuta i samsvar med bestemmelsene i TFEU 219, å besitte og forvalte medlemsstatenes offisielle valutabeholdninger, og å fremme et godt fungerende betalingssystem. Tilsvarende unntak skal gjelde for IKT-leverandører som er etablert i en EØS/EFTA-stat som utfører de samme oppgavene som omtalt i artikkel 127(2) TFEU, jf. EØS-komitébeslutningen *artikkel 1 nr. 3 bokstav k*.

Som nevnt skal et overvåkningsforum gi anbefalinger om utpeking av kritiske IKT-leverandører til de felleseuropeiske tilsynsmyndighetene og ESA. Det følger av EØS-komitébeslutningen *artikkel 1 nr. 3 bokstav m* at nasjonale tilsynsmyndigheter i EØS/EFTA-statene skal ha alle de samme rettigheter og plikter som tilsynsmyndighetene i EUs medlemsstater til å delta i overvåkingsforumet. ESA har rett til å utpeke to representanter til overvåkningsforumet.

I henhold til DORA-forordningen artikkel 34 nr. 1 skal hovedovervåkerne utpekt i henhold til DORA-forordningen artikkel 31 nr. 1 bokstav b etablere et felles overvåkningsnettverk for å koordinere gjennomføring av overvåkningsaktiviteter. EØS-komitébeslutningen *artikkel 1 nr. 3 bokstav o* slår fast at ESA skal delta i felles overvåkningsnettverk med alle de samme rettighetene og pliktene som EUs tilsynsmyndigheter.

Etter DORA-forordningen artikkel 35 gis den relevante EU-tilsynsmyndigheten, i rollen som hovedovervåker, myndighet overfor kritiske IKT-leverandører til å be om informasjon, gjennomføre generelle undersøkelser og inspeksjon, utstede anbefalinger og kreve rapporter fra IKT-leverandøren om oppfølging av anbefalinger. I tillegg kan hovedovervåkeren utstede dagbøter overfor kritiske IKT-leverandører som velger å ikke følge opp en anbefaling. Hovedovervåkerens myndighet overfor kritiske IKT-leverandører er nærmere beskrevet i punkt 2.4.2.6 over. Håndheving av betalingen av dagbøter skal for øvrig falle inn under reglene som gjelder for sivilprosessreglene som er gjeldende i medlemsstaten der inspeksjoner og tilgang skal foretas. Det er domstolene i den berørte medlemsstaten som skal ha jurisdiksjon over klager knyttet til urettmessig håndheving.

Gjennom EØS-komitébeslutningen legges myndigheten overfor kritiske IKT-leverandører til ESA for foretak som er etablert i en EØS/EFTA-stat eller i tredjeland, med datterforetak i en EØS/EFTA-stat. ESAs utøvelse av myndighet overfor et foretak etablert i EØS/EFTA skal skje på basis av utkast fra den ansvarlige EU-tilsynsmyndigheten. EFTAs faste komité skal etter EØS-komitébeslutningen ha ansvaret for fordelingen av eventuelle overtredelsesgebyr som inndrives av ESA. For EUs medlemsstater skal gebyrene, jf. DORA-forordningen artikkel 35 nr. 9, tildeles EUs generelle budsjett.

Før hovedovervåker utsteder overtredelsesgebyr etter DORA-forordningen artikkel 35 nr. 11, skal den gi representanter for den kritiske IKT-leverandøren rett til å bli hørt om funnene som ligger til grunn for beslutningen. I lys av at de tekniske elementene i beslutningen om å utstede overtredelsesgebyr vil bli forberedt av den ansvarlige EU-tilsynsmyndigheten, og for å sikre samme rettigheter på tvers av det indre marked, slår EØS-komitébeslutningen *artikkel 1 nr. 3 bokstav r* fast at det er den ansvarlige EU-tilsynsmyndigheten som skal gi rett til å bli hørt også for kritiske IKT-leverandører som faller inn under ESAs myndighet.

Før utstedelse av en anbefaling etter DORA-forordningen artikkel 35 nr. 1 bokstav d skal hovedovervåkeren gi IKT-leverandøren mulighet til å gi relevant informasjon. Siden første utkast av anbefalingen vil bli utarbeidet av den ansvarlige EU-tilsynsmyndigheten, slår tilpasningen i EØS-komitébeslutningen *artikkel 1 nr. 3 bokstav p* fast at den ansvarlige EU-tilsynsmyndigheten skal gi kritiske IKT-leverandører som faller under ESAs myndighet muligheten til å gi denne informasjonen før utarbeidelse av utkast til ESA.

2.6.4 Vurdering

Under DORA-forordningen har den relevante EU-tilsynsmyndigheten myndighet til å fastsette bindende tiltak i henhold til artikkel 31, 33, 35 til 39, 42 og 43 for fysiske og juridiske personer etablert i EU. Kompetansen til å utøve samme myndighet overfor fysiske og juridiske personer etablert i EØS/EFTA-statene legges gjennom EØS-komitébeslutningen til EFTAs overvåkningsorgan (ESA). Denne tilpasningen er i tråd med EØS-tilpasningen til EUs finanstilsynsbyråstruktur, som Stortinget samtykket til 13. juni 2016 i tråd med forslag i Prop. 100 S (2015–2016). En slik tilpasning vil gi ESA myndighet til å fatte rettslig bindende vedtak med virkning for norske rettssubjekter, dersom det utpekes kritiske IKT-leverandører som er etablert i Norge. ESAs vedtak kan prøves for EFTA-domstolen.

Ettersom Grunnloven bygger på en forutsetning om at statsmaktenes kompetanse skal utøves av nasjonale statsorganer, er overføringen av myndighet til ESA vurdert opp mot Grunnloven. Etter sikker konstitusjonell praksis kan Stortinget etter Grunnlovens § 26 annet ledd med alminnelig flertall samtykke til myndighetsoverføring som er «lite inngripende».

Kriteriene for å anses som en kritisk IKT-leverandør etter DORA-forordningen er omfattende, og er innrettet mot leverandører som kan anses som systemkritiske for EUs finanssektor. Blant annet må IKT-leverandørens kunder utgjøre minst 10 prosent av foretakene i minst én kategori av foretak i finanssektoren i EU, f.eks. 10 prosent av alle kredittinstitusjoner, investeringsforetak osv., og den samlede verdien av eiendelene til disse foretakene må utgjøre minst 10 prosent av den totale verdien av alle eiendeler til sammenlignbare foretak i EU, jf. delegert kommisjonsforordning (EU) 2024/1502. Videre må IKT-leverandøren benyttes av et visst antall globalt systemviktige (G-SIIs) eller andre systemviktige (O-SIIs) foretak eller foretak som anses som systemisk viktige av kompetente myndigheter. Tjenestene som leveres, må være av en kritisk art for foretakene, og det må være krevende å erstatte IKT-leverandøren, enten på grunn av mangel på alternativer eller fordi flytting til ny leverandør vil være vanskelig. For IKT-leverandører som er etablert i EØS/EFTA-statene, antas det at kriteriene for å bli ansett som kritisk vil være de samme som for leverandører i EU, men slik at det er leverandørens betydning for finanssektoren i EØS som skal vurderes.

Departementet er ikke kjent med at det finnes norske IKT-leverandører som leverer tjenester til finanssektoren i EU/EØS av en slik karakter og utbredelse at leverandøren vil kunne anses som kritisk etter kriteriene i DORA-forordningen. Norsk finanssektor har i betydelig grad utkontraktert IKT-drift til IKT-leverandører, og benytter seg i økende grad av internasjonale IKT-leverandører som er del av store konsern. Disse har hovedkontor utenfor Norge, men kan ha datterforetak i Norge. Som beskrevet i punkt 2.4.2.6 skal IKT-leverandører som inngår i konsern, vurderes ut fra konsernets betydning, og skal ha ett kontaktpunkt for kommunikasjonen med hovedovervåkeren. Det fremgår ikke av DORA-forordningen om det er morselskapet i et konsern som vil være den juridiske personen som blir utpekt som kritisk. Det er dermed en mulighet for at et datterforetak i Norge kan utpekes som kritisk IKT-leverandør, slik at ESA etter DORA-forordningen vil kunne be om informasjon, gjennomføre undersøkelser og inspeksjon, utstede anbefalinger og be om informasjon fra foretaket om hvordan anbefalingene er fulgt opp, samt utstede dagbøter dersom en kritisk IKT-leverandør ikke følger opp ESAs anbefalinger. Departementet anser det imidlertid som lite sannsynlig at norske foretak vil oppfylle vilkårene for å bli utpekt som kritisk IKT-leverandør etter forordningen.

Oppfølgingen av foretak i den norske finanssektoren sin bruk av IKT-leverandører skal, som nevnt i punkt 2.5.7, uansett ligge til Finanstilsynet.

Myndighetsoverføringen i DORA-forordningen har altså et begrenset saklig virkeområde. Det er usikkert om myndigheten som tillegges ESA etter forordningen vil bli benyttet overfor norske aktører. Den praktiske betydningen av myndighetsoverføringen vurderes derfor som liten.

Myndighetsoverføringen til ESA anses etter dette å være av en så begrenset og reelt sett lite praktisk karakter at den vurderes for å være «lite inngripende». Departementets vurdering er derfor at Stortingets samtykke kan innhentes etter Grunnlovens § 26 annet ledd.

2.6.5 Tilrådning

Forordningen og direktivet er EØS-relevante, og Finansdepartementet anbefaler at Stortinget samtykker til innlemmelse av forordningen og direktivet med tilpasningstekster i EØS-avtalen.

3 Endringer i hvitvaskingsloven om opplysninger som skal følge overføringer av penger og visse kryptoeiendeler (TFR II)

3.1 Innledning

Europarlaments- og rådsforordning (EU) 2023/1113 («Transfer of Funds Regulation» – TFR II) om opplysninger som skal følge overføringer av penger og visse kryptoeiendeler, og om endring av direktiv (EU) 2015/849 (fjerde hvitvaskingsdirektiv), ble vedtatt i EU i mai 2023. Forordningen gir nye regler om hvilke opplysninger som skal følge med pengeoverføringer og overføringer av kryptoeiendeler. TFR II erstatter forordning (EU) 2015/847 (TFR I), som i dag regulerer banker og andre betalingstjenesteyteres forpliktelser ved pengeoverføringer. TFR I er gjennomført i *forskrift 14. september 2018 nr. 1324 om tiltak mot hvitvasking og terrorfinansiering (hvitvaskingsforskriften)* § 10-1, jf. hvitvaskingsloven § 52. Endringene i TFR II vil primært utvide virkeområdet for forpliktelsene som allerede gjelder for tradisjonelle betalingstjenesteytere, til å gjelde også for aktører som yter kryptoeiendelstjenester. TFR II ble vedtatt i EU for å reflektere endringer i Financial Action Task Force (FATF) sine anbefalinger om opplysninger som skal følge med pengeoverføringer. I 2019 ble FATFs anbefalinger endret for å hensynta hvitvaskings- og terrorfinansieringsrisikoen ved virtuell valuta og tjenesteytere av virtuell valuta.

TFR II trådte i kraft i EU 29. juni 2023 og fikk anvendelse der fra 30. desember 2024. Rettsakten ble tatt inn i EØS-avtalen 20. februar 2025 ved EØS-komiteens beslutning nr. 42/2025, med forbehold om Stortingets samtykke, jf. Grunnloven § 26 annet ledd. Departementet foreslår i denne proposisjonen lovendringer for å gjennomføre TFR II i norsk rett, og at Stortinget gir sitt samtykke til å innlemme forordningen i EØS-avtalen. Lovforslaget innebærer at TFR II inntas i hvitvaskingsloven, slik at betalingstjenesteyteres og kryptoeiendelstjenesteyteres forpliktelser til å sende opplysninger med overføringer av penger og kryptoeiendeler vil gjelde som norsk lov. Det foreslås også enkelte andre endringer i hvitvaskingsloven, bl.a. for å gjøre flere kryptoeiendelstjenesteytere til rapporteringspliktige etter hvitvaskingsregelverket.

3.2 Bakgrunn for forslaget

3.2.1 Hovedtrekkene i forordningen

Hvitvasking, terrorfinansiering og organisert kriminalitet er ofte grensekryssende. Det er derfor etablert en rekke globale standarder og felleseuropeiske reguleringer for å bekjempe slik kriminalitet. Transaksjoner med kryptoeiendeler er spesielt sårbare for hvitvasking og terrorfinansiering på grunn av hurtigheten og anonymiteten ved slike transaksjoner.

Det europeiske hvitvaskingsregelverket bygger på anbefalinger som kommer fra FATF. Det internasjonale samfunnet har gjennom FATF utviklet globale standarder som søker å forhindre hvitvasking og terrorfinansiering. Anbefaling 15 er en anbefaling til stater om å vurdere hvitvaskings- og terrorfinansieringsrisiko som følger av utviklingen av nye produkter eller praksis, herunder bruk eller utvikling av ny teknologi på bank- og betalingsfeltet. Anbefalingen har dessuten et særskilt punkt om virtuelle eiendeler og tjenesteytere tilknyttet kryptoeiendeler (i anbefalingene kalt «virtual assets»). Anbefaling 16 inneholder anbefalinger om opplysninger som bør følge med overføringer av penger for å minimere hvitvaskings- og terrorfinansieringsrisikoen. Gjennom anbefaling 15 er det stilt lignende krav som etter anbefaling 16 for overføringer av kryptoeiendeler.

Informasjonspliktene for betalingstjenesteytere har i norsk rett til nå fulgt av TFR I. TFR II utvider rekkevidden av TFR I ved å pålegge også ytere av kryptoeiendelstjenester plikt til å lagre og gi opplysninger ved overføring av kryptoeiendeler, tilsvarende det TFR I har pålagt betalingstjenesteytere ved alminnelige pengeoverføringer.

TFR II pålegger en kryptoeiendelstjenesteyter som er avsender av en overføring, å sikre at en rekke data følger transaksjonen, herunder navn, kontonummer eller lignende, adresse og kundeidentifikasjon på kunden som foretar overføringen, og navn og kontonummer eller lignende

til personen som mottar kryptoeiendelene. Mottakerens tjenesteyter pålegges bl.a. å ha på plass effektive rutiner for å identifisere at den nødvendige informasjon følger overføringen, og så bekrefte informasjonen før kryptoverdiene gjøres tilgjengelige for mottaker. Forordningen pålegger også tjenesteytere å lagre og dele opplysninger med kompetente tilsynsmyndigheter etter anmodning. I tillegg endrer TFR II hvitvaskingsdirektivet slik at kryptoeiendelstjenesteytere gjøres rapporteringspliktige og får samme plikter som andre rapporteringspliktige etter hvitvaskingsregelverket.

Forpliktelsene for alminnelige betalingstjenesteytere som fulgte av TFR I, oppdateres og videreføres i TFR II.

TFR II henger sammen med et større arbeid i EU om å regulere markedet for kryptoeiendeler. Sammen med forordning (EU) 2023/1114 om markeder i kryptoeiendeler («Markets in Crypto-Assets» – MiCA) utgjør TFR II det nye, felleseuropeiske rammeverket for regulering av markedet for kryptoeiendeler. Dette markedet har hittil bare i begrenset grad vært gjenstand for regulering. Innføringen av TFR II og MiCA vil gjøre at kryptomarkedet underlegges lignende finansregulatoriske krav som det tradisjonelle markedet for finansielle instrumenter, betalingsmidler og pengeoverføringer.

3.2.2 Høring

Finansdepartementet ga i brev 28. september 2023 Finanstilsynet i oppdrag å utrede gjennomføring av forventede EØS-forpliktelser som tilsvarer TFR II og forordning (EU) 2023/1114 om markeder for kryptoeiendeler (MiCA).

Departementet sendte Finanstilsynets høringsnotat på høring 1. mars 2024 med høringsfrist 1. juni 2024. Høringsbrevet ble sendt til følgende instanser:

Alle departementene
Arbeids- og velferdsdirektoratet
Brønnøysundregistrene
Datatilsynet
Direktoratet for forvaltning og økonomistyring
Finanstilsynet
Folketrygdfondet
Forbrukerrådet
Forbrukertilsynet
Konkurransetilsynet
Likestillings- og diskrimineringsombudet
Lotteri- og stiftelsestilsynet
Norges Bank
Regjeringsadvokaten
Riksadvokaten
Riksrevisjonen
Sivilombudet
Skattedirektoratet
Statens pensjonskasse
Statistisk sentralbyrå
Statsministerens kontor
Økokrim

Akademikerne
Aksjonærforeningen i Norge
Arbeidsgiverforeningen Spekter
Bankenes sikringsfond
Deloitte AS
Den norske advokatforening
Den Norske Aktuarforening
Den norske Revisorforening
Econa
Eiendom Norge
Energi Norge
Equinor
Evry
Finans Norge
Finansforbundet
Finansieringsselskapenes forening
Finansmarkedsfondet
Forening for Finansfag Norge
Fornybar Norge
Forum for Utvikling og Miljø
Handelshøgskolen ved Nord universitet
Handelshøyskolen BI
Havtrygd Gjensidig Forsikring
Hovedorganisasjonen for universitets- og høyskoleutdannede
Hovedorganisasjonen Virke
Huseiernes landsforbund
Høgskulen på Vestlandet
IIA Norge
Industri Energi
Initiativ for etisk handel
KnowledgeGroup AS
Kommunalbanken AS
KPMG AS
KS
Landsorganisasjonen i Norge
Nasdaq OMX Oslo ASA
NMBU – Norges miljø- og biovitenskapelige universitet
Nordic Trustee
Norges Bondelag
Norges eiendomsmeglerforbund
Norges handelshøyskole
Norges ingeniør- og teknologorganisasjon
Norges Juristforbund

Norges Kommunerevisorforbund
Norges Rederiforbund
Norges Røde Kors
Norges Skogeierforbund
Norsk Bergindustri
Norsk Crowdfunding Forening
Norsk Hydro ASA
Norsk Journalistlag
Norsk Kapitalforvalterforening
Norsk landbrukssamvirke
Norsk olje og gass
Norsk Presseforbund
Norsk Redaktørforening
Norsk Sjøoffiserers Forbund
Norsk takst
Norsk Venturekapitalforening
Norsk Økrimforening
Norske Boligbyggelags Landsforbund SA
Norske Finansanalytikeres Forening
Norske Forsikringsmegleres Forening
NTL-Skatt
Næringslivets Hovedorganisasjon
Offshore Norge
Oslo Børs ASA
Pensjonskasseforeningen
Personskadeforbundet LTN
Plan International Norge
Publish What You Pay Norway
Redd Barna
Regelrådet
Regnskap Norge
Skattebetalerforeningen
Skatterevisorenes Forening
SMB Norge
Sparebankforeningen i Norge
Stiftelsesforeningen
Storebrand ASA
Støttekomiteen for Vest-Sahara
The Nordic Association of Electricity Traders
The Nordic Association of Marine Insurers (CEFOR)
Tietoevry Norge
Tilsynsrådet for advokatvirksomhet
Universitetet i Agder
Universitetet i Bergen
Universitetet i Oslo
Universitetet i Sørøst-Norge
Universitetet i Tromsø – Norges arktiske universitet
Verdipapirfondenes forening
Verdipapirforetakenes Forbund
Verdipapirsentralen ASA
Yrkesorganisasjonenes Sentralforbund
Økonomiforbundet

Følgende instanser har avgitt realitetsmerknader til høringen som omhandler gjennomføring av TFR II:

Finans Norge
Fintech Norway
Skattedirektoratet
Økokrim

Følgende instanser har opplyst at de ikke har merknader til gjennomføring av TFR II:

Brønnøysundregistrene
Den Norske Aktuarforening
Forsvarsdepartementet
Justis- og beredskapsdepartementet
Statistisk sentralbyrå

3.3 Gjennomføring i norsk rett

3.3.1 Gjeldende rett

Forpliktelser for betalingstjenesteytere ved pengeoverføringer følger i dag av forordning TFR I, som er gjennomført i hvitvaskingsforskriften. Forordningen omfatter pengeoverføringer i enhver valuta som sendes eller mottas av en betalingstjenesteyter som er etablert i EØS, jf. artikkel 2, med unntak for ulike nærmere definerte typer betalinger. I forordningen er det i artikkel 2 nr. 5 åpnet for et nasjonalt valg om å unnta visse betalinger fra TFR I. Muligheten ble ikke benyttet da TFR I ble gjennomført i norsk rett.

Formålet med TFR I er å sikre sporbarhet av avsender og mottaker av pengeoverføringer både ved nasjonale og grensekryssende betalinger. TFR I pålegger avsenderens betalingstjenesteyter å sørge for at avsenderens navn, betalingskontonummer eller transaksjonsidentifikasjon, og adresse, offisielle personlige dokumentnummer, kundeidentifikasjonsnummer eller fødselsdato og fødested, samt mottakerens navn og betalingskontonummer, følger med overføringen, jf. artikkel 4. Betalingstjenesteyter forpliktes til å kontrollere at opplysninger som skal følge betalingen er riktige, og til ikke å gjennomføre pengeoverføringer før forpliktelsene er oppfylt. Hvis alle betalingstjenesteyterne i betalingskjeden er etablert i EØS, stiller TFR I forenklede krav til informasjonen som skal følge betalingen, jf. artikkel 5 nr. 1. I slike tilfeller er det tilstrekkelig at opplysningene som følger med overføringen, er avsenderens og mottakerens betalingskontonummer eller transaksjonsidentifikasjon. Dersom mottakerens betalingstjenesteyter anmoder

avsenderens betalingstjenesteyter om flere opplysninger, må avsenderens betalingstjenesteyter likevel gjøre tilgjengelig flere opplysninger innen tre virkedager, jf. artikkel 5 nr. 2.

Avsenderens betalingstjenesteyter er forpliktet til å kontrollere at opplysningene som følger overføringen, er korrekte fra en pålitelig og uavhengig kilde, jf. artikkel 4 nr. 4. For enkelte pengeoverføringer, som overføringer innenfor EØS som ikke overstiger 1 000 euro, er det begrensede krav til å kontrollere opplysninger. Opplysningene må likevel kontrolleres dersom pengene som skal overføres, er mottatt i kontanter eller anonyme elektroniske penger, eller det foreligger rimelig grunn til mistanke om hvitvasking eller terrorfinansiering.

Også mottakerens betalingstjenesteyter er forpliktet til å kontrollere opplysningene som følger med overføringen, jf. artikkel 7. For overføringer av beløp som overstiger 1 000 euro, må mottakerens betalingstjenesteyter kontrollere at de nødvendige opplysningene følger med overføringen, og at disse er korrekte, før midlene kan gjøres tilgjengelig for mottaker. Der beløpet er under 1 000 euro, er kravene til kontroll mindre strenge. Der mottakerens betalingstjenesteyter blir oppmerksom på at opplysninger mangler eller er ufullstendige, skal tjenesteyteren foreta en risikovurdering, og på bakgrunn av denne, avvise overføringen eller innhente de nødvendige opplysningene.

Dersom avsenderens betalingstjenesteyter gjentatte ganger unnlater å gi etterspurt informasjon, skal mottakerens betalingstjenesteyter treffe tiltak, jf. artikkel 8. Disse kan omfatte begrensning eller avslutning av forretningsforbindelsen. Manglende eller ufullstendige opplysninger skal også være en faktor i mottakerens betalingstjenesteyters vurdering av om pengeoverføringen er mistenkelig, og om den skal rapporteres til Enheten for finansiell etterretning (EFE) i Økokrim, jf. hvitvaskingsloven § 26.

TFR I krever i artikkel 17 at det i nasjonalt regelverk fastsettes regler om administrative sanksjoner og forvaltningsmessige tiltak, slik at juridiske og fysiske personer kan holdes ansvarlige ved gjentatte, systematiske eller alvorlige brudd på enkelte av betalingstjenesteyternes plikter etter forordningen. I gjeldende rett følger adgangen til å fastsette administrative sanksjoner og forvaltningsmessige tiltak av hvitvaskingsloven. Finanstilsynet er tilsynsmyndighet.

Kryptoeiendeler eller andre virtuelle verdier er ikke omtalt i TFR I. I hvitvaskingsforskriften er det enkelte bestemmelser som inneholder regler for vekslings- og oppbevaringstjenester for virtuell valuta, som gjennomfører endringer som kom med direktiv (EU) 2018/843 (femte hvitvaskingsdirektiv). Bestemmelsene inneholder ikke informasjonsplikter eller annen helhetlig regulering av kryptoeiendeler og tjenesteytere, men gjelder registreringskrav og krav om forsterkede kundetiltak for tilbydere av vekslings- og oppbevaringstjenester for virtuell valuta.

3.3.2 EØS-rett

3.3.2.1 Anvendelsesområde

TFR II får anvendelse på pengeoverføringer og overføringer av kryptoeiendeler der minst én av de involverte tjenesteyterne er etablert i eller har sitt registrerte kontor i EØS, jf. artikkel 1. Forpliktelsene etter forordningen gjelder for alle betalingstjenesteytere, kryptoeiendelstjenesteytere og ytere av mellomliggende betalingstjenester som sender, videresender eller mottar en overføring av penger eller kryptoeiendeler.

Forordningen gir separate bestemmelser for forpliktelsene til henholdsvis betalingstjenesteytere som overfører og mottar penger, og kryptoeiendelstjenesteytere som overfører og mottar kryptoeiendeler. I mange tilfeller er forpliktelsene sammenfallende, men systemet i forordningen legger opp til at kravene vil beskrives hver for seg i denne proposisjonen.

Definisjonen av kryptoeiendeler i TFR II samsvarer med definisjonen av kryptoeiendeler som er fastsatt i FATFs anbefalinger, se avsnitt 10 i fortalen til TFR II. TFR II artikkel 3 nr. 14, som definerer kryptoeiendel, refererer til forordning (EU) 2023/1114 (MiCA), som definerer kryptoeiendeler som digitale representasjoner av en verdi eller rettighet som kan overføres og oppbevares elektronisk ved bruk av distribuert registerteknologi eller lignende teknologi. Artikkel 2 nr. 4 presiserer at elektroniske pengetoken også faller inn under definisjonen av kryptoeiendeler i TFR II.

I det følgende brukes «penger», «pengeoverføring», «betalingskonto» og «betalingstjenesteyter» i beskrivelsen av bestemmelsene som omhandler alminnelige pengeoverføringer. Med «penger» og «pengeoverføringer» menes for forordningens formål penger i alle valutaer som finnes på en betalingskonto, og som overføres mellom betalingskontoer ved hjelp av betalingstjenesteytere.

Med betalingstjenesteytere menes bl.a. kredittinstitusjoner, e-pengeforetak, postgirokontorer og betalingsinstitusjoner slik disse er

definert i direktiv (EU) 2015/2366 om betalingstjenester i det indre marked, jf. TFR II artikkel 3 nr. 5. For definisjonen av kryptoeiendelstjenesteytere refererer TFR II artikkel 3 nr. 15 til MiCA, som definerer dem som juridiske personer eller andre foretak som tilbyr kryptotjenester, herunder oppbevaring og overføring av kryptoeiendeler, profesjonelt til kunder.

Forordningen får ikke anvendelse på overføringer av penger eller kryptoeiendeler som foretas uten involvering av en tjenesteyter og finner sted direkte mellom personer, eller der avsender og mottaker er tjenesteytere som handler på vegne av seg selv, jf. TFR II artikkel 2 nr. 4. Tjenesteytere som kun leverer supplerende infrastruktur, for eksempel tilbydere av internettinfrastruktur, skybaserte lagringstjenester og programvareutviklere, faller også i utgangspunktet utenfor forordningens rekkevidde. Artikkel 2 nr. 1 slår fast at overføringer som går gjennom kryptominibanker, omfattes av forordningen, men uttak av penger fra egen betalingskonto omfattes ikke, jf. artikkel 2 nr. 4.

TFR II gir gjennom et nasjonalt valg adgang til å unnta visse pengeoverføringer som er betaling for varer eller tjenester, fra forpliktelsene i forordningen. Artikkel 2 nr. 5 fastsetter tre vilkår for å vedta en slik unntaksregel. For det første må betalingstjenesteyteren til mottaker være underlagt hvitvaskingsdirektivet. For det andre må betalingstjenesteyteren til mottaker kunne spore betalingen gjennom et unikt transaksjonsnummer. For det tredje må overføringen ikke overstige 1 000 euro. Unntaket kan kun innføres for pengeoverføringer som finner sted innenfor statens territorium. Det er ingen unntaksadgang for overføringer av kryptoeiendeler.

3.3.2.2 Plikter ved overføring av penger og kryptoeiendeler

Pengeoverføringer

For pengeoverføringer pålegger TFR II artikkel 4 og 5 betalingstjenesteytere å sørge for at følgende informasjon følger med en overføring: Navn på avsender, avsenderens kontonummer, og avsenderens adresse og personnummer eller alternativt, fødselsdato og -sted. Dersom betalingsmeldingen åpner for det, og betaleren har oppgitt det til betalingstjenesteyteren, skal i tillegg et identifikasjonsnummer for juridiske personer, enten Legal Entity Identifier-nummer (LEI-nummer) eller et tilsvarende unikt identifikasjonsnummer, følge med betalingen. Avsenderens betalingstjenesteyter må verifisere, fra pålitelige og uavhengige kilder, at opplysningene som følger med overføringen, er korrekte før overføringen gjennomføres, jf. artikkel 4 nr. 4. Dersom det er gjennomført kundekontrolltiltak etter hvitvaskingsloven, er kravet til verifisering oppfylt, jf. artikkel 4 nr. 5. Overføringen kan ikke gjennomføres før avsenderens betalingstjenesteyter har fullført alle forpliktelser under TFR II, jf. artikkel 4 nr. 6. Mottakerens betalingstjenesteyter må sørge for at de påkrevde opplysningene om avsenderens navn, kontonummer, LEI-nummer eller annen tilgjengelig offisiell identifikasjon, samt et transaksjonsnummer i tilfeller der overføringen ikke er gjort til eller fra en betalingskonto, medfølger den mottatte overføringen, jf. artikkel 7.

Disse utvidede informasjonspliktene for betalingstjenesteytere trer først inn der en av partene i betalingskjeden er etablert utenfor EØS, og verdien av overføringen overstiger 1 000 euro. For overføringer der alle betalingstjenesteytere i betalingskjeden er etablert i EØS, gjelder forenklede krav til opplysninger som skal følge med overføringen, jf. artikkel 5. For slike overføringer må minst opplysninger om avsender og mottakers kontonummer og en unik transaksjonsidentifikasjon følge overføringen, jf. artikkel 5 nr. 1. Også for pengeoverføringer under 1 000 euro til land utenfor EØS gjelder de forenklede kravene der kun navn og transaksjonsidentifikasjon til mottaker og avsender må følge med overføringen. I begge tilfellene forenkles også kravene til verifikasjon. Avsenderens betalingstjenesteyter behøver ikke å verifisere informasjonen fra en uavhengig og pålitelig kilde med mindre pengene som overføres, har blitt mottatt i kontanter eller i anonyme elektroniske penger, eller det foreligger rimelig grunn til mistanke om hvitvasking eller terrorfinansiering, jf. artikkel 5 nr. 3.

Dersom de påkrevde opplysningene ikke følger med overføringen og mottakerens betalingstjenesteyter etterspør disse, må avsenderens betalingstjenesteyter tilgjengeliggjøre opplysningene for mottakerens betalingstjenesteyter innen tre virkedager, jf. artikkel 5 nr. 2. Hvis overføringens verdi overstiger 1 000 euro, enten overføringen utføres i én enkelt transaksjon eller i flere transaksjoner som synes å henge sammen, må avsenderens betalingstjenesteyter på forespørsel oppgi alle opplysninger som er påkrevd etter artikkel 4. For overføringer som ikke synes å henge sammen med andre overføringer som til sammen har verdi over 1 000 euro, må avsenderens betalingstjenesteyter kun oppgi navn og betalingskontonummer eller unik transaksjonsidentifikasjon til mottakerens betalingstjenesteyter.

Artikkel 6 gir nærmere bestemmelser for pengeoverføringer til stater utenfor EØS. Overføres pengene i en samleoverføring («batch file») fra én og samme avsender, og mottakerens betalingstjenesteyter er etablert utenfor EØS, gjelder informasjonskravene i artikkel 4 og 5 ikke for alle enkeltoverføringene. Artikkel 6 nr. 1 bestemmer at det er tilstrekkelig at opplysningene som kreves etter artikkel 4 (1), (2) og (3) følger med samlefilen, så fremt enkeltoverføringene inneholder oppdragsgiverens betalingskontonummer eller, dersom overføringen ikke foretas til eller fra en betalingskonto, den unike transaksjonsidentifikasjonen. Artikkel 6 nr. 2 bestemmer at for pengeoverføringer som ikke overstiger 1 000 euro og har mottaker etablert utenfor EØS, skal minst navn på avsenderen og mottakeren, samt avsenderens og mottakerens betalingskontonummer eller unike transaksjonsidentifikasjon, følge overføringen. Avsenderens betalingstjenesteyter plikter ikke å verifisere opplysningene om avsenderen med mindre betalingstjenesteyteren mottok pengene som skal overføres, i kontanter eller anonyme elektroniske penger, eller har rimelig grunn til mistanke om hvitvasking eller terrorfinansiering, jf. artikkel 6 nr. 2.

Mottakerens betalingstjenesteyter forpliktes i artikkel 7 til å utarbeide rutiner for å kontrollere at de nødvendige opplysningene følger overføringen. Der mottaker av overføringen vil ha pengene utbetalt i kontanter eller anonyme elektroniske penger, der det foreligger grunn til mistanke om hvitvasking eller terrorfinansiering, eller der overføringen alene eller i flere overføringer som synes å henge sammen overstiger 1 000 euro, må mottakerens betalingstjenesteyter verifisere informasjonen som følger med overføringen gjennom en uavhengig og pålitelig kilde. Der det er foretatt kundekontrolltiltak etter hvitvaskingsregelverket, regnes opplysningene som verifisert også etter TFR II, jf. artikkel 7 nr. 5. Følger de nødvendige opplysningene ikke med overføringen, må mottakerens betalingstjenesteyter ha risikobaserte rutiner for å håndtere slike situasjoner. Mottakerens betalingstjenesteyter må enten innhente de manglende opplysningene før overføringen kan gjennomføres, eller avvise eller suspendere transaksjonen, jf. artikkel 8. Ved gjentatte feil fra avsenderens betalingstjenesteyter må mottakerens betalingstjenesteyter gi avsenderens betalingstjenesteyter en advarsel, avvise fremtidige overføringer eller avslutte forretningsforbindelsen. Mottakerens betalingstjenesteyter må rapportere feilen til tilsynsmyndigheten med ansvar for etterlevelse av hvitvaskingsregelverket, jf. artikkel 8 nr. 2 andre avsnitt, og skal anse manglende eller ufullstendige opplysninger som en faktor i vurderingen av om en overføring eller en tilknyttet transaksjon er mistenkelig, og om den skal rapporteres til den nasjonale enheten for finansiell etterretning, jf. artikkel 9.

For ytere av mellomliggende betalingstjenester gjelder samme forpliktelser som for betalingstjenesteyterne til avsender og mottaker, se artikkel 10–13. Ytere av mellomliggende betalingstjenester skal sørge for at de nødvendige opplysningene følger med overføringen videre, og at det ikke mangler informasjon, jf. artikkel 10 og 11. Mangler nødvendige opplysninger, skal yter av mellomliggende betalingstjenester avvise, suspendere eller innhente nødvendige opplysninger før overføringen gjennomføres, jf. artikkel 12. Også ytere av mellomliggende betalingstjenester må rapportere gjentatte feil eller mistanke om hvitvasking og terrorfinansiering til tilsynsmyndigheten og enheten for finansiell etterretning, se artikkel 12 nr. 2 andre avsnitt og artikkel 13.

Overføring av kryptoeiendeler

Forpliktelsene for avsenderens kryptoeiendelstjenesteyter følger av artikkel 14 og 15. Tjenesteyteren må ved overføring av kryptoeiendeler sørge for at følgende informasjon følger med overføringen: avsenderens navn, adresse, og offisielle personlige dokumentnummer og kundeidentifikasjonsnummer eller alternativt, fødselsdato og fødested. I tillegg skal adressen på det distribuerte registeret følge med, i tilfeller der det brukes et nettverk som bruker distribuert registerteknologi («distributed ledger technology» – DLT). Der det ikke brukes DLT-teknologi, skal kryptokontonummeret følge med. Dersom det relevante meldingsformatet åpner for det, og avsender har oppgitt det til kryptoeiendelstjenesteyteren, skal i tillegg et identifikasjonsnummer for juridiske personer, enten Legal Entity Identifier-nummer (LEI-nummer) eller et tilsvarende unikt identifikasjonsnummer følge med overføringen. Avsenderens kryptoeiendelstjenesteyter må også sørge for at mottakerens navn, DLT-adresse, kryptokontonummer og LEI-nummer følger med overføringen. Opplysningene skal følge i forkant av eller samtidig med overføringen. Det er imidlertid ikke et krav om at opplysningene er vedlagt selve overføringen. Der flere transaksjoner overføres sammen i en gruppe, trenger opplysningene ikke å følge med den enkelte overføring, men det er tilstrekkelig at de følger med gruppefilen. Der overføringen er rettet til en frittstående adresse (i høringsnotatet

kalt «personlig kryptokonto»), må avsenderens kryptoeiendelstjenesteyter kontrollere om adressen er eid eller kontrollert av avsender der overføringens verdi overstiger 1 000 euro. Også for overføring av kryptoeiendeler må avsenderens tjenesteyter verifisere opplysningene fra en uavhengig og pålitelig kilde, med mindre det er foretatt kundekontrolltiltak etter hvitvaskingsloven jf. artikkel 14 nr. 7. Kryptoeiendelstjenesteyteren kan ikke gjennomføre en overføring før informasjonskravene er oppfylt jf. artikkel 14 nr. 8.

Forpliktelsene for mottakerens kryptoeiendelstjenesteyter følger av artikkel 16 og 17. Mottakerens kryptoeiendelstjenesteyter må ha på plass effektive rutiner for å avdekke om de nødvendige opplysningene følger med overføringen. Kommer overføringen fra en frittstående adresse og overstiger 1 000 euro, må mottakerens kryptoeiendelstjenesteyter vurdere om adressen er eid eller kontrollert av mottakeren. Før mottakerens kryptoeiendelstjenesteyter gjør kryptoeiendelene tilgjengelige for mottakeren, må tjenesteyteren verifisere opplysningene fra en uavhengig og pålitelig kilde, med mindre det er foretatt kundekontrolltiltak etter hvitvaskingsregelverket. Tilsvarende krav til rapportering til tilsynsmyndigheten som for mottakere av pengeoverføringer gjelder der mottakerens kryptoeiendelstjenesteyter avdekker manglende opplysninger med overføringen, jf. artikkel 17 nr. 2 andre avsnitt.

Mottakerens kryptoeiendelstjenesteyter skal anse manglende eller ufullstendige opplysninger som en faktor i vurderingen av om en overføring eller en tilknyttet transaksjon er mistenkelig, og om den skal rapporteres til den nasjonale enheten for finansiell etterretning, jf. artikkel 18.

For ytere av mellomliggende kryptoeiendelstjenester gjelder det tilsvarende krav til å avdekke at de nødvendige opplysningene følger med overføringen, og plikt til å verifisere at opplysningene er korrekte, som for mottakerens og avsenderens kryptoeiendelstjenesteytere, jf. artikkel 19–21. Ytere av mellomliggende kryptoeiendelstjeneste har også plikt til å innhente nødvendige opplysninger der disse mangler, eller avvise overføringen der de nødvendige opplysningene ikke gis. I tillegg må ytere av mellomliggende kryptoeiendelstjeneste lagre opplysninger om overføringer og ved forespørsel gjøre dem tilgjengelig for kompetente myndigheter. Tilsvarende krav til rapportering til tilsynsmyndigheten som for ytere av mellomliggende betalingstjenester av pengeoverføringer gjelder der yteren av mellomliggende kryptoeiendelstjenester avdekker manglende opplysninger med overføringen, jf. artikkel 21 nr. 2 andre avsnitt.

Ytere av mellomliggende kryptoeiendelstjeneste skal anse manglende eller ufullstendige opplysninger som en faktor i vurderingen av om en overføring eller en tilknyttet transaksjon er mistenkelig, og om den skal rapporteres til den nasjonale enheten for finansiell etterretning, jf. artikkel 22.

3.3.2.3 Restriktive tiltak

Både betalingstjenesteytere og kryptoeiendelstjenesteytere pålegges å ha på plass interne retningslinjer, rutiner og tiltak for å påse etterlevelse av restriktive tiltak og sanksjoner ved overføring av verdier, jf. artikkel 23. Den europeiske banktilsynsmyndigheten (EBA) har gitt retningslinjer med veiledning for interne retningslinjer, rutiner og tiltak om betalingstjenesteyteres og kryptoeiendelstjenesteyteres plikter ved overføringer som involverer sanksjonerte enheter eller individer.

I Norge er det Utenriksdepartementet som forvalter sanksjonsloven med forskrifter, hvor FNs sanksjoner og deler av EUs restriktive tiltak gjennomføres. EUs restriktive tiltak gjelder derfor ikke direkte i Norge. I EØS-versjonen av TFR II er det foretatt en tilpasning i artikkel 23, slik at teksten gjenspeiler praksis og gjeldende rett om at tjenesteytere i Norge kun skal ta hensyn til restriktive tiltak som er tatt inn i nasjonal rett, se også omtale av tilpasningen i punkt 3.4 nedenfor. Med tilpasningen forplikter TFR II betalingstjenesteytere og kryptoeiendelstjenesteytere til å påse etterlevelse av restriksjoner gjennomført i nasjonal rett og andre restriksjoner som EØS/EFTA-statene har implementert med grunnlag i bilaterale eller multilaterale traktater.

3.3.2.4 Administrative sanksjoner

TFR II har tilsvarende bestemmelser om administrative sanksjoner og overvåking som TFR I, jf. artikkel 28 og 29. Reglene i TFR I videreføres stort sett uendret i TFR II, men utvides til å omfatte kryptoeiendelstjenesteytere. Nasjonale myndigheter må sørge for at betalingstjenesteytere og kryptoeiendelstjenesteytere, samt personer i ledende stillinger og andre ansatte hos tjenesteyterne, kan holdes ansvarlige og ilegges administrative sanksjoner eller forvaltningstiltak for manglende etterlevelse og regelbrudd. TFR II fremhever fire regelbrudd som minst må medføre administrative sanksjoner eller forvaltningstiltak, jf. artikkel 29: a. gjentatte eller systematiske feil i opplysninger som skal medfølge pengeoverføringer

eller overføringer av kryptoeiendeler, b. gjentatte, systematiske eller alvorlige mangler i tjenesteyternes lagring av opplysninger, c. mangler i etablering av effektive risikobaserte rutiner for avdekke mangler, og d. alvorlige brudd på plikten til å avdekke, rapportere eller innhente manglende opplysninger for ytere av mellomliggende betalingstjenester.

De administrative sanksjonene og forvaltningstiltakene som skal være tilgjengelige for tilsynsmyndigheten, skal være konsistente med de som skal være tilgjengelige etter hvitvaskingsdirektivet kapittel VI avsnitt 4, jf. artikkel 28 nr. 1. Administrative sanksjoner og forvaltningstiltak som minst skal være tilgjengelige for tilsynsmyndigheten, er å

- avgi en offentlig erklæring som identifiserer den fysiske eller juridiske personen og overtredelsens art,
- gi pålegg der det kreves at den fysiske eller juridiske personen stanser atferden og avstår fra å gjenta slik atferd,
- tilbaketrekke eller midlertidig suspendere en tillatelse,
- ilegge et midlertidig forbud mot å utøve ledelsesfunksjoner i ansvarlige enheter for personer som har lederansvar eller for andre fysiske personer som holdes ansvarlige for overtredelsen, og
- ilegge administrative overtredelsesgebyr.

Gebyrets størrelse varierer etter typen rapporteringspliktig, og for bl.a. betalingstjenesteytere skal gebyret kunne være på inntil 10 pst. av samlet årsomsetning. Artikkel 31 nr. 1 bestemmer at tilsynsmyndigheten skal ta i betraktning alle relevante forhold, herunder forholdene angitt i hvitvaskingsdirektivet artikkel 60 nr. 4, når det avgjøres hvilken type forvaltningstiltak eller sanksjon som skal ilegges, samt ved utmåling av overtredelsesgebyr. Videre er det bestemt i TFR II artikkel 31 nr. 2 at reglene i hvitvaskingsdirektivet artikkel 62 skal gjelde for ileggelsen av forvaltningstiltak og sanksjoner etter forordningen. Hvitvaskingsdirektivet artikkel 62 gjelder i denne sammenhengen rapportering til EBA om ileggelsen av forvaltningstiltak og sanksjoner og EBAs føring av en internettside med lenker til publiserte forvaltningstiltak og sanksjoner.

TFR II stiller krav om at avgjørelser om administrative sanksjoner eller tiltak skal publiseres der det er nødvendig og proporsjonalt etter en konkret vurdering, jf. artikkel 30. Artikkel 32 nr. 1 krever at statene etablerer effektive mekanismer for å oppfordre til rapportering til tilsynsmyndigheten av brudd på forordningen, og mekanismene skal minst omfatte kravene i hvitvaskingsdirektivet artikkel 61 nr. 2. Videre fremgår det av artikkel 32 nr. 2 at betalingstjenesteytere og kryptoeiendelstjenesteytere, i samarbeid med tilsynsmyndigheten, skal etablere rutiner for intern rapportering om brudd gjennom en sikker, uavhengig, særskilt og anonym kanal. Dette skal være proporsjonalt med arten og størrelsen på betalingstjenesteyteren eller kryptoeiendelstjenesteyteren.

Artikkel 28 nr. 1 gir statene adgang til et nasjonalt valg. Statene kan velge at brudd på regler i forordningen som er kriminalisert og kan straffes, ikke skal være gjenstand for administrative sanksjoner eller forvaltningstiltak. Straffehjemmelen må i slike tilfeller kommuniseres til EU-kommisjonen.

3.3.2.5 Andre bestemmelser

TFR II artikkel 24 pålegger betalingstjenesteytere og kryptoeiendelstjenesteytere å gi opplysninger til tilsynsmyndighetene når de anmoder om det, fullt ut og uten opphold. Artikkel 25 inneholder bestemmelser om databeskyttelse. Det slås fast at betalingstjenesteytere og kryptoeiendelsytere må etterleve personvernreglene i forordning (EU) 2016/679 (GDPR) når de lagrer og behandler opplysninger for å oppfylle forpliktelsene i TFR II. Personopplysninger skal ikke lagres lenger enn det som er strengt nødvendig, jf. TFR II artikkel 26 nr. 1, men det må lagres opplysninger etter artikkel 4 til 7 og 14 til 16 i fem år. Ved utløpet av lagringstiden skal betalingstjenesteytere og kryptoeiendelstjenesteytere sørge for sletting av opplysningene om ikke nasjonal rett bestemmer noe annet, jf. artikkel 26 nr. 2. For å tillate eller kreve ytterligere lagring må statene bestemme under hvilke omstendigheter dette skal være tillatt eller påkrevd, og statene må ha gjennomført en grundig vurdering av nødvendigheten og proporsjonaliteten av slik ytterligere lagring. Nødvendighetsvurderingen må knyttes til forebygging, avdekking eller etterforskning av hvitvasking eller terrorfinansiering, og den ytterligere lagringstiden skal ikke overstige fem år. Informasjonsutveksling mellom kompetente myndigheter og med myndigheter i tredjestater er underlagt informasjonsdelingsbestemmelsene i hvitvaskingsdirektivet, jf. artikkel 27.

Artikkel 35 handler om avtaler med land utenfor EU («tredjeland»). Artikkel 35 nr. 1. gir EU-kommisjonen kompetanse til å tillate EUs medlemsstater å inngå avtaler med tredjeland som inneholder unntak fra forordningens bestemmelser, bl.a. for å muliggjøre pengeoverføringer

mellom landene. Artikkel 35 faller utenfor EØS-avtalen, fordi det gjelder forholdet til tredjeland, og bestemmelsen skal dermed ikke gjelde som norsk rett.

3.3.2.6 Endringer i hvitvaskingsdirektivet

TFR II artikkel 38 gjør endringer i direktiv (EU) 2015/849 (EUs fjerde hvitvaskingsdirektiv) for å samkjøre hvitvaskingsregelverket med TFR II.

TFR II artikkel 38 nr. 1 opphever bestemmelsene i hvitvaskingsdirektivet artikkel 2 nr. 1 punkt 3 (g) og (h) som gjør tjenesteyterne for vekslingstjenester og oppbevaringstjenester for virtuell valuta til rapporteringspliktige. Nye definisjoner av kryptoeiendeler og kryptoeiendelstjenesteytere vil følge av TFR II artikkel 3 nr. 14 og 15, som henviser til MiCA. TFR II artikkel 38 nr. 2 (c) innfører nye definisjoner av kryptoeiendeler og kryptoeiendelstjenesteytere også i hvitvaskingsdirektivet, og det presiseres i den nye definisjonen at kryptoeiendelstjenesteytere ikke skal være omfattet av hvitvaskingsdirektivet når de kun yter rådgivning om kryptoeiendeler, som regulert i MiCA artikkel 3 nr. 1 punkt 16 (h).

TFR II artikkel 38 nr. 2 (a) tilføyer kryptoeiendelstjenesteytere til hvitvaskingsdirektivets definisjon av «finansinstitusjon» i artikkel 3 nr. 2 ny bokstav (g). Gjennom artikkel 38 nr. 2 (b) blir også definisjonene av «korrespondentforbindelse» i hvitvaskingsdirektivet endret. Den nye definisjonen inkluderer relasjoner som er etablert for gjennomføring av kryptoeiendelstransaksjoner eller for overføringer av kryptoeiendeler.

TFR II stiller videre krav til forsterkede tiltak for kundekontroll for overføringer til eller fra frittstående adresser («self-hosted addresses»). TFR II artikkel 38 nr. 2 (d) gir hvitvaskingsdirektivet en definisjon av frittstående adresser i direktivets artikkel 3 nr. 20. Som frittstående adresse regnes adresse på en distribuert registerteknologi som ikke er knyttet til en tilbyder av konsesjonspliktige tjenester. I ny artikkel 19a er det bestemt at statene skal kreve at kryptoeiendelstjenesteytere identifiserer og vurderer hvitvaskings- og terrorfinansieringsrisikoen forbundet med, og ha særlige rutiner og tiltak ved, overføring av kryptoeiendeler til eller fra en frittstående adresse. Statene skal kreve at tjenesteyterne iverksetter risikoreduserende tiltak i tråd med den identifiserte risikoen, og de tiltakene skal inkludere ett eller flere av følgende:

a. gjennomføre risikobaserte tiltak til å identifisere og verifisere identiteten av avsender eller mottaker og deres reelle rettighetshavere,
b. kreve ytterligere informasjon om midlenes opprinnelse og mottakeren av de overførte kryptoeiendelene,
c. gjennomføre løpende forsterkede kundetiltak av transaksjonene, eller
d. treffe andre tiltak for å motvirke og håndtere risikoen for hvitvasking, terrorfinansiering, oppfølging av økonomiske sanksjoner og sanksjoner knyttet til finansiering av masseødeleggelsesvåpen.

TFR II artikkel 38 nr. 4 gir også en ny regel om korrespondentrelasjoner utenfor EØS som involverer overføringer av kryptoeiendeler, se hvitvaskingsdirektivet ny artikkel 19b. Når respondentinstitusjonen er etablert utenfor EØS, skal kryptoeiendelstjenesteyter, i tillegg til de alminnelige kundetiltakene i hvitvaskingsdirektivet artikkel 13, gjennomføre forsterkede kundetiltak ved avtaleinngåelsen. De forsterkede tiltakene er å

a. avklare om respondentinstitusjonen har konsesjon eller er registrert,
b. innhente informasjon om respondentens art, kvalitet og omdømme,
c. vurdere respondentinstitusjonens tiltak mot hvitvasking og terrorfinansiering,
d. innhente godkjenning fra overordnet før etablering av ny korrespondentforbindelse,
e. dokumentere institusjonens ansvar, og
f. dersom det brukes oppgjørskonti for kryptoeiendeler, forsikre seg om at korrespondenten har bekreftet identiteten til og fører oppfølgning av kunder som har adgang til kontoer, og på anmodning kan fremlegge relevante opplysninger om kundetiltak og oppfølgningen av kundene.

Dersom kryptoeiendelstjenesteytere avslutter en korrespondentforbindelse begrunnet i rutiner etter hvitvaskingsregelverket, skal beslutningen dokumenteres. Kryptoeiendelstjenesteyteren skal regelmessig oppdatere kundetiltakene for korrespondentforholdet, i tillegg til når nye risikoer fremkommer om respondentinstitusjonen, se ny artikkel 19b nr. 1 tredje avsnitt. Statene skal sørge for at kryptoeiendelstjenesteytere tar i betraktning informasjonen referert til i artikkel 19b nr. 1 for å avgjøre, på risikosensitiv basis, de aktuelle tiltakene som skal redusere risikoene forbundet med respondentinstitusjonen, jf. artikkel 19b nr. 2.

TFR II artikkel 38 nr. 6 tilføyer kryptoeiendelstjenesteytere til kravet i hvitvaskingsdirektivet artikkel 45 nr. 9 om at tjenesteytere som er etablert på deres territorier i en annen form enn filialer, og hvis hovedkontor ligger i en annen

medlemsstat, skal utpeke et sentralt kontaktpunkt på statens territorium for å sikre at bestemmelsene om bekjempelse av hvitvasking og terrorfinansiering blir overholdt.

Flere av endringene i TFR II artikkel 38 innebærer at EBA får i oppgave å utarbeide ulike retningslinjer, jf. endringene til hvitvaskingsdirektivet artikkel 18 og ny artikkel 19a, 19b og 24a. Blant annet skal EBA utarbeide retningslinjer om risikovariabler og -faktorer som kryptoeiendelstjenesteytere må vurdere når de inngår nye forretningsforbindelser eller foretar overføringer, retningslinjer om kriterier og metoder for å verifisere identiteten til avsender og mottaker ved en transaksjon til eller fra en frittstående adresse, og retningslinjer om kriterier og faktorer som kryptoeiendelstjenesteytere må vurdere når de etablerer korrespondentforbindelser med respondenter utenfor EØS.

3.3.3 Forslaget i høringsnotatet

Finanstilsynet foreslår å gjennomføre TFR II ved inkorporasjon i hvitvaskingsloven, mens forordningens forgjenger har vært gjennomført i forskrift. I høringsnotatet foreslås inkorporasjonen av TFR II gjennomført i hvitvaskingsloven § 52. Enkelte av direktivendringene i TFR II artikkel 38 krever endring i hvitvaskingsloven med forskrift. Finanstilsynet foreslår derfor en rekke endringer i det norske hvitvaskingsregelverket.

Hovedendringen er at hvitvaskingsregelverket utvides fra å gjelde for vekslings- og oppbevaringstjenester for virtuell valuta, til å gjelde for kryptoeiendelstjenesteytere. Finanstilsynet foreslår at «kryptoeiendelstjenesteytere» inntas i oppregningen av rapporteringspliktige i hvitvaskingsloven § 4 første ledd, og at definisjonen av «kryptoeiendel» og «kryptoeiendelstjenesteytere» inntas i hvitvaskingsloven § 2 med en henvisning til definisjonen i MiCA artikkel 3 nr. 1 punkt 15. Fordi kryptoeiendelstjenesteytere ikke er omfattet av hvitvaskingsloven når de kun yter rådgivning om kryptoeiendeler, foreslår Finanstilsynet at dette presiseres i hvitvaskingsloven § 2. I tillegg foreslås et tillegg i hvitvaskingsloven § 2 bokstav i nr. 2 slik at kryptoeiendeler tas inn i definisjonen av korrespondentforbindelse.

Om kundetiltak vurderer Finanstilsynet at det i hvitvaskingsdirektivet og hvitvaskingsloven allerede ligger et krav om at rapporteringspliktige må ha risikovurderinger, rutiner og tiltak for alle produkter og tjenester de tilbyr, og som inngår i den registreringspliktige virksomheten. Finanstilsynet forstår direktivendringen som en fremheving av en særlig risikofylt transaksjonstype. Frittstående adresse (i høringsnotatet kalt «personlig kryptokonto») har ikke tilknytning til en registreringspliktig eller konsesjonspliktig virksomhet, jf. definisjonen i TFR II artikkel 3 punkt 20. Det kan derfor være større risiko for at midlene er tilknyttet hvitvasking og terrorfinansiering, ettersom det ikke er gjennomført kundetiltak overfor eier av kontoen av en annen rapporteringspliktig. Etter Finanstilsynets vurdering er det ikke behov for å spesifikt regulere kravet til risikovurderinger og rutiner. Dette følger av hvitvaskingsloven §§ 7 og 8, og vil være viktigere for produkter og tjenester med høyere risiko. Det foreslås derfor en bestemmelse om forsterkede kundetiltak knyttet til transaksjonstypen. Finanstilsynet legger til grunn at flere av tiltakene vil måtte gjennomføres uavhengig av de konkrete forpliktelsene som følger av hvitvaskingsdirektivet artikkel 19a. Forskjellen blir at rapporteringspliktige ikke kan vurdere dette ut fra en risikobasert tilnærming, men blir nødt til å gjennomføre tiltak for hver overføring. Finanstilsynet foreslår at dette inntas som ny § 17a i hvitvaskingsloven.

TFR II forutsetter nasjonal gjennomføring av bestemmelser om tilsyn, herunder at det gis regler om tilsynsvirkemidler, administrative sanksjoner og andre forvaltningstiltak. I dag gjennomfører hvitvaskingsloven § 49 sanksjonsbestemmelsene om ileggelse av overtredelsesgebyr og ledelseskarantene i bl.a. TFR I. Finanstilsynet vurderer at bestemmelsene om overtredelsesgebyr i TFR II vil være dekket ved at kryptoeiendelstjenesteytere underlegges hvitvaskingsloven og henvisningen i hvitvaskingsloven § 49 oppdateres.

TFR II gir adgang til nasjonale valg om unntak fra informasjonsplikter for overføringer av mindre beløp, utvidet lagringstid for personopplysninger, og unntak fra kravet til å ha tilgjengelig administrative sanksjoner og forvaltningstiltak der regelbrudd kan straffesanksjoneres. Også TFR I ga nasjonale valg. Da TFR I ble gjennomført i norsk rett, ble de nasjonale valgene ikke benyttet.

Når det gjelder forsterkede tiltak ved korrespondentforbindelser med en institusjon fra stat utenfor EØS som respondentinstitusjon, tilsvarer bestemmelsen i TFR II i stor grad gjeldende bestemmelse om forsterkede tiltak ved korrespondentforbindelser, jf. hvitvaskingsdirektivet artikkel 19, som er gjennomført i hvitvaskingsloven § 19. Finanstilsynet foreslår at den nye bestemmelsen i TFR II implementeres ved justering av § 19 i hvitvaskingsloven. Dette kan gjøres ved å inkludere kryptoeiendelstjenesteytere i

angivelsen av hvem bestemmelsen gjelder for. Tiltaket om å fastslå om motparten er registrert eller innehar konsesjon, samt inkludere kryptokontoer som oppgjørskontoer, kan inntas i andre ledd i hvitvaskingsloven § 19. I tillegg foreslår Finanstilsynet et nytt tredje ledd om krav til å dokumentere visse beslutninger. Finanstilsynet anser det ikke som nødvendig å endre hvitvaskingsloven § 19 som følge av justeringene i hvitvaskingsdirektivets nye bestemmelse om korrespondentforbindelse for kryptoeiendeler. Finanstilsynet mener det ikke bør gis særregulering for én type korrespondentforhold, når den generelle bestemmelsen om løpende oppfølging gjelder for en rekke andre rapporteringspliktige.

For retningslinjer fra EBA knyttet til artikkel 18, 19a, 19b og 24a vil Finanstilsynet publisere informasjon om slike retningslinjer og i hvilken grad det forventes at disse følges av norske foretak.

For øvrig peker Finanstilsynet på at begrepet «virtuell valuta» i norsk rett avviker fra definisjonen av «kryptoeiendeler» i TFR II og MiCA, og foreslår at definisjonen av virtuell valuta i hvitvaskingsforskriften § 1-3 oppheves.

3.3.4 Høringsinstansenes syn

Finans Norge har følgende merknad til Finanstilsynets forslag til ny hvitvaskingslov § 17a om krav til forsterkede kundetiltak:

> «Ordlyden innledningsvis viser til at det skal gjennomføres forsterkede kundetiltak ved transaksjoner til eller fra 'personlige kryptokontoer.' Ordlyden isolert sett skaper tvil om hvem som skal gjennomføre kundetiltakene. Finans Norge forstår høringsnotatet slik at kravet gjelder for kryptoeiendelstjenesteytere. Det vises til uttalelsen på side 39 i høringsnotatet hvor følgende fremgår:
>
> 'TFR II artikkel 38 nr. 4 innfører en ny bestemmelse i hvitvaskingsdirektivet artikkel 19a som pålegger medlemsstatene å gi regler om forsterkede kundetiltak for *kryptoeiendelstjenesteytere*.' [Understreket her].
>
> Det bør fremgå tydelig av bestemmelsens ordlyd at kravet til forsterkede kundetiltak gjelder kryptoeiendelstjenesteytere. Det bør også inntas en henvisning til ny § 2 bokstav m som definerer kryptoeiendelstjenesteyter.»

Fintech Norway mener at det er viktig at de nye kravene som kommer i TFR II, må være praktisk gjennomførbare for betalingsforetak. Fintech Norway mener at banker i dag ikke tillater betalingsforetak å motta informasjonen som er påkrevd i forordningen, og at betalingsforetak ikke har adgang til å lese eller lagre informasjonen i API-ene som er gitt av bankene. Fintech Norway peker videre på at 1 000 euro-terskelen i forordningens artikkel 5 og 6 ikke er samkjørt med dagens hvitvaskingslov, som refererer til enkeltstående transaksjoner på 8000 kroner i hvitvaskingsloven § 10 første ledd bokstav b nr. 2. Det bes også om en presisering av om verifikasjonen som kreves for overføringer som overstiger 1 000 euro som skal anses gjennomført dersom det er truffet kundetiltak etter hvitvaskingsloven, gjelder for både avsenderens og mottakerens tjenesteyter. Fintech Norway peker videre på at det er en utfordring at viktige jurisdiksjoner som Storbritannia, USA og Singapore ikke er tatt høyde for, og at det ikke er tatt hensyn til regulering omkring høyrisikoland innenfor EU.

Om tilganger til nødvendig register skriver Fintech Norway:

> «Betalingsforetak har samtidig heller ikke tilgang til nødvendige register, for å verifisere informasjonen mottatt som det er krav om i forordningens artikkel 4.4. hvor det er krav om å verifisere informasjonen som er medfølgende transaksjonen, hvor det er nødvendig. Betalingsforetak har ikke adgang til OCR, hvor banker forhindrer betalingsforetak i å kvalitetssikre betalinger, ved å ikke tillate tilgang.
>
> Dette inkluderer også KAR-registeret hvor banker har direkte tilgang. Derimot hvis betalingsforetak skal ha tilgang, vil dette forutsette en kunderelasjon til en bank som tilbyr denne tilgangen som et produkt eller tjeneste. Hensyn til å inkludere nyoppstartede selskaper, som betalingsforetak regulert av PSD2 i det finansielle landskapet, er påpekt blant annet ved kontraheringsplikten i Norge. I motsetning til andre nordiske land opprettholder Norge kontraheringsplikten ovenfor både fysiske så vel som juridiske personer, med hensikt om å fostre opp under innovasjon og nyskaping. Dette strider direkte i mot at betalingsforetak må betale banker for å opprettholde sine forpliktelser.»

Til slutt peker Fintech Norway på at dagens hvitvaskingslov § 31 tredje ledd stenger for at kryptoeiendelstjenesteytere kan anmode om og motta informasjon som mangler ved pengeoverføringer.

Økokrim har merknad til den foreslåtte beløpsgrensen på 8 000 kroner i Finanstilsynets forslag

til endring i hvitvaskingsforskriften § 4-1a bokstav b. Økokrim er kjent med at overføringer knyttet til terrorfinansiering og kjøp av overgrepsmateriale også gjennomføres med lave beløpsstørrelser. En beløpsgrense på 8 000 kroner kan medføre at slike transaksjoner ikke blir avdekket. Økokrim mener det bør vurderes om beløpsgrensen skal settes lavere eller utgå i sin helhet. Til forslag til ny § 17a i hvitvaskingsloven om forsterkede kundetiltak for transaksjoner til og fra personlige kryptokontoer (frittstående adresser) har Økokrim følgende merknad:

> «Økokrim mener at det bør fremkomme tydeligere av ordlyden at rapporteringspliktige ikke her står fritt til å velge tiltak. Økokrim mener at rapporteringspliktige minimum skal gjennomføre tiltak a, og at hvor langt en må gå for å identifisere og verifisere reelle rettighetshavere skal følge en risikobasert tilnærming. De følgende tiltakene kommer eventuelt i tillegg. Fra et hvitvaskingsperspektiv er det også naturlig at det første trinnet i en forsterket kundekontroll er å undersøke hvem som reelt sett er involvert i transaksjonen. Som Finanstilsynet skriver i høringsnotatet, er det ved transaksjoner til eller fra personlige kryptokontoer en økt hvitvaskingsrisiko nettopp fordi 'det ikke er gjennomført kundetiltak overfor eier av kontoen av en annen rapporteringspliktig.' Videre mener Økokrim at sammenhengen mellom tiltak a til c bør komme tydeligere frem av ordlyden. For tiltak 'a. Identifisere og verifisere identiteten av avsender, mottaker og deres reelle rettighetshavere,' bør det gis veiledning til hvordan identitet skal verifiseres. Videre mener Økokrim at det bør vurderes om det kan gis tydeligere krav eller veiledning til hvordan de forsterkede kundetiltakene skal gjennomføres, herunder en utdypning av 'alle andre tiltak for å motvirke og håndtere risikoen for hvitvasking og terrorfinansiering' samt 'gjennomføre forsterket løpende oppfølging av transaksjonene.'»

3.3.5 Departementets vurdering

Departementet slutter seg til Finanstilsynets forslag om å inkorporere TFR II i hvitvaskingsloven, slik at forordningen vil gjelde som norsk lov. Ved også å innta de foreslåtte regelendringene i hvitvaskingsloven og gjøre kryptoeiendelstjenesteytere til rapporteringspliktige, vil kravene forordningen stiller til det norske lovverket, være dekket.

Departementet er enig i Finans Norge sitt forslag om å presisere den foreslåtte ordlyden i ny § 17a i hvitvaskingsloven, slik at det tydeligere kommer frem at forpliktelsen til å gjennomføre forsterkede kundetiltak ved overføringer til og fra frittstående adresser, gjelder for kryptoeiendelstjenesteytere.

Når det gjelder Økokrims merknad til forslag til ny § 17a i hvitvaskingsloven om å presisere minimumstiltakene rapporteringspliktige skal gjennomføre, viser departementet til at Finanstilsynets forslag til ny § 17a reflekterer kravene i ny artikkel 19a i hvitvaskingsdirektivet. For overføringer til og fra frittstående adresser krever TFR II artikkel 14 nr. 5 at avsenderens tjenesteyter anskaffer og lagrer opplysninger om avsenderens og mottakerens identitet. Artikkel 16 nr. 2 pålegger mottakerens tjenesteyter å anskaffe og lagre samme informasjon. Kravene utløses av at det er en frittstående adresse i den ene enden av betalingskjeden, uavhengig av beløpsgrenser. Departementet foreslår å presisere i ny § 17a at tjenesteytere må gjennomføre en konkret risikovurdering ved overføringer til eller fra frittstående adresser, og basert på risikovurderingen, gjennomføre minst ett av tiltakene som er listet opp i bestemmelsen. Etter departementets vurdering er det en fordel å synliggjøre dette kravet direkte i bestemmelsen, som en særlig forpliktelse i forbindelse med denne typen transaksjoner, selv om det også vil følge av de overordnede kravene i hvitvaskingsloven om å gjennomføre en risikovurdering, utarbeide rutiner og ha en risikobasert tilnærming, jf. hvitvaskingsloven §§ 7, 8 og 9.

Departementet har i arbeidet med gjennomføringen av TFR II, og i lys av høringssvarene fra Fintech Norway og Økokrim om Finanstilsynets forslag til regler om kundetiltak ved overføringer av kryptoeiendeler, sett behov for å justere hvitvaskingslovens regler om når det er krav om å gjennomføre kundetiltak. I hvitvaskingsloven § 10 første ledd bokstav b er det i dag satt en beløpsgrense på 8 000 kroner for kundetiltak ved enkeltstående transaksjoner som nærmere definert i forskrift. Med enkeltstående transaksjoner menes her transaksjoner for kunder som rapporteringspliktig ikke har et etablert kundeforhold til.

For oversiktens skyld fremhever departementet at TFR II opererer med beløpsgrenser i to tilfeller. For det første skiller forordningen mellom pengeoverføringer som har høyere og lavere verdi enn 1 000 euro. Skillet har betydning for betalingstjenesteyteres forpliktelser med hensyn til hvor omfattende opplysningene som følger med overføringen skal være, samt til verifiseringen av

opplysningene. Kravene forenkles for overføringer som ikke overstiger 1 000 euro. For det andre gir TFR II særlige regler for overføringer over 1 000 euro til eller fra såkalte frittstående adresser.

For overføringer av kryptoeiendeler krever TFR II at verifiserte opplysninger følger med overføringen uavhengig av verdien av overføringen. Dagens regel om kundetiltak ved transaksjoner over 8 000 kroner vil derfor ikke dekke kravene i forordningen hva gjelder overføringer av kryptoeiendeler.

For pengeoverføringer er det i forordningen krav om at nærmere bestemte pengeoverføringer over 1 000 euro, uten hensyn til om overføringene utføres i én enkelt transaksjon eller flere transaksjoner som synes å henge sammen, skal medfølges av visse verifiserte opplysninger. Dagens regel om kundetiltak ved enkeltstående transaksjoner over 8 000 kroner er ikke omfattet av regelen i hvitvaskingsloven § 10 annet ledd første punktum om at beløpsgrensen skal beregnes samlet for transaksjoner som gjennomføres i flere operasjoner som synes å ha sammenheng. Begrunnelsen for denne forskjellen i loven er at hvitvaskingsdirektivet artikkel 11 bokstav b, c og d inneholder et slikt skille mellom ulike typer transaksjoner, til tross for at TFR I også krever at overføringer ses i sammenheng. Konsekvensen er at dagens beløpsgrense på 8 000 kroner ikke vil innebære at kundetiltak påkreves i tråd med forordningen, fordi kriteriet om overføringer som synes å henge sammen, ikke er fanget opp.

Spørsmålet blir etter dette hvordan TFR IIs krav til gjennomføring av visse kundetiltak skal ivaretas. Departementet foreslår en særskilt bestemmelse om krav til kundetiltak i tilfeller der dette ellers er påkrevd av TFR II, se forslag til § 10 første ledd ny bokstav d. Riktignok vil krav til verifisering av opplysningene følge av forordningen selv, som altså foreslås inkorporert i lov, men departementet mener det er behov for en mer tilgjengelig regel for rapporteringspliktige om å gjennomføre kundetiltak. Forslaget til ny bokstav d i hvitvaskingsloven § 10 skal sikre at relevante rapporteringspliktige skal gjennomføre kundetiltak som påkrevd av forordningen, også om grensen på 8 000 kroner beholdes.

Departementet bemerker at det kan reise spørsmål ved om gjeldende hvitvaskingslov § 10 første ledd bokstav b om 8 000-kronersgrensen bør oppheves. Departementet foreslår ikke det nå, og det er flere grunner til det. For det første bør regelverket være så forutsigbart som mulig, noe som tilsier at mengden endringer begrenses. For det andre kan det være nyttig med en særskilt regel om kundetiltak for pengeoverføringer også utenfor tilfeller der dette er påkrevd av TFR II. Kundetiltak som innebærer innhenting og dokumentasjon av opplysninger kan forebygge at kriminelle tar i bruk rapporteringspliktiges tjenester. Det bidrar også til at opplysninger og dokumentasjon er tilgjengelig for myndighetene, om det skulle være behov for dem i forbindelse med f.eks. etterforskning. I hvitvaskingsforskriften § 4-1a er det gitt regler om hvilke transaksjoner som er omfattet av 8 000-kronersgrensen i § 10 første ledd bokstav b. Departementet bemerker at det tas sikte på å fastsette konsekvensendringer i denne når TFR II trer i kraft, slik som å oppheve bokstav c, som i dag henviser til TFR I, som gjennomført i hvitvaskingsforskriften § 10-1.

Når det gjelder Fintech Norway sitt innspill om taushetsplikten i hvitvaskingsloven § 31 tredje ledd, mener departementet at bestemmelsen ikke er til hinder for at tjenesteytere innhenter informasjon fra avsenderens eller mottakerens tjenesteyter for å oppfylle informasjonskravene i TFR II.

TFR II gir videre stater adgang til å ha nasjonale valg i forordningens artikkel 2 nr. 5, artikkel 26 nr. 2 og artikkel 28 nr. 1. Disse valgene lå også inne i TFR I, men ble ikke benyttet da forordningen ble gjennomført i hvitvaskingsregelverket.

For valget om å unnta transaksjoner med verdi under 1 000 euro når formålet med disse er å betale for varer eller tjenester, og mottakerens betalingstjenesteyter er underlagt hvitvaskingsregelverket og kan spore betalingen tilbake til avsender, mener departementet at det ikke er behov for å benytte det nasjonale valget. Et nasjonalt unntak vil frita en rekke overføringer fra informasjonskravene i TFR II, og slik gi færre muligheter for å avdekke og kontrollere hvitvaskingsrisiko. Det nasjonale valget ble heller ikke benyttet ved inkorporeringen av TFR I.

Det er som nevnt et nasjonalt valg å utvide den femårige lagringstiden for personopplysninger i inntil fem år til, men dette forutsetter en grundig vurdering av om det er nødvendig og proporsjonalt for å forebygge, avdekke eller etterforske hvitvasking eller terrorfinansiering. Det er ikke ennå foretatt noen slik vurdering i Norge, og departementet foreslår derfor ikke å benytte det nasjonale valget i loven nå. Hvitvaskingsloven § 30 fjerde ledd åpner imidlertid for at departementet i forskrift kan gi nærmere regler om hvordan opplysninger og dokumenter skal registreres og lagres, samt om lagring av personopplysninger utover fem år, med en maksimal lagringstid på ti år. Bestemmelsen refererer i første ledd til hvitvaskingsloven §§ 9 til 26, og det kan derfor

være uklart om hjemmelen også kan brukes til å forlenge lagringstiden som pålegges i TFR II. Departementet foreslår derfor å inkludere en forskriftshjemmel i inkorporasjonsbestemmelsen til TFR II, se forslag til § 52 annet ledd, slik at lagringstiden kan forlenges hvis det vurderes som nødvendig og proporsjonalt i et senere forskriftsarbeid.

Departementet slutter seg til Finanstilsynets forslag om at hvitvaskingslovens § 49 om overtredelsesgebyr skal gjelde for overtredelser av TFR II. Departementet mener derfor at det ikke er behov for å benytte det nasjonale valget om at stater kan velge å ikke innføre regler om administrative sanksjoner og forvaltningstiltak hvis det aktuelle regelbruddet er straffsanksjonert i nasjonal rett.

3.4 Samtykke til godkjenning av EØS-komiteens beslutning om innlemmelse av forordningen

3.4.1 Omtale av beslutningen

EØS-komiteen besluttet 20. februar 2025 å innlemme forordning (EU) 2023/1113 (TFR II) om opplysninger som skal følge overføringer av penger og visse kryptoeiendeler i EØS-avtalen, jf. EØS-komitébeslutning 42/2025. Gjennomføring i norsk rett av beslutning nr. 42/2025 om innlemmelse i EØS-avtalen av TFR II vil kreve lovendring. Det er derfor nødvendig med Stortingets samtykke til godkjennelse av EØS-komiteens beslutning.

Beslutningen inneholder en fortale og tre artikler.

Artikkel 1 innlemmer forordningen i EØS-avtalen. Etter artikkel 1 nr. 1 i EØS-komiteens beslutning skal det tilføyes en henvisning til TFR II i EØS-avtalens vedlegg XII punkt 23b, som viser til direktiv (EU) 2015/849 (fjerde hvitvaskingsdirektiv). Etter artikkel 1 nr. 2 skal punkt 23ba som henviser til forordning (EU) 2015/847 (TFR I), erstattes med en henvisning til TFR II. Det foreslås her en tilpasning av forordningsteksten i TFR II artikkel 23 om restriktive tiltak. Tilpasningen er nærmere omtalt nedenfor.

Artikkel 2 fastsetter at EØS-komiteens beslutning skal tre i kraft 21. februar 2025, forutsatt at konstitusjonelle forbehold etter artikkel 103 nr. 1 i EØS-avtalen er hevet. Fordi den angitte datoen er passert, vil beslutningen tre i kraft den første dag i den annen måned etter siste meddelelse om heving av konstitusjonelle forbehold, jf. artikkel 103 nr. 1 annet ledd.

I artikkel 3 følger det at EØS-komiteens beslutning på vanlig måte skal kunngjøres i EØS-avdelingen og EØS-tillegget til Den europeiske unions tidende.

EØS-komiteens beslutning nr. 42/2025 og forordningen i uoffisiell norsk oversettelse er vedlagt denne proposisjonen.

3.4.2 Tilpasninger i EØS-komitébeslutningen

Det gjøres én særskilt tilpasning i forordningsteksten i EØS-komitébeslutningens artikkel 1 nr. 2. Tilpasningen gjelder artikkel 23 i forordningen, som pålegger betalingstjenesteytere og kryptoeiendeltjenesteytere å ha interne rutiner, prosedyrer og kontroller for å sikre gjennomføring av sanksjoner. I artikkelen er det referert til «Union and national restrictive measures», der «restrictive measures» er navnet på EUs sanksjoner. Siden EUs sanksjonsregime faller utenfor EØS-avtalen, går tilpasningen ut på å endre teksten til «nationally applicable restrictive measures». Tilpasningen gjenspeiler praksis og norsk rett, som er at Norge og EFTA-landene ikke skal forholde seg direkte til EUs restriktive tiltak (sanksjoner), men til restriksjoner og sanksjoner som er implementert i norsk rett.

3.4.3 Tilrådning

Forordningen er EØS-relevant, og Finansdepartementet anbefaler at Stortinget samtykker til innlemmelse av forordningen med tilpasningstekster i EØS-avtalen.

4 Økonomiske og administrative konsekvenser

4.1 Lov om digital operasjonell motstandsdyktighet i finanssektoren (DORA-loven)

4.1.1 Innledning

Forslaget om gjennomføring av forordning (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.

4.1.2 Konsekvenser for foretak i finanssektoren

Gjennomføring av 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., se vedlegg 5 i EU-kommisjonens konsekvensanalyse 24. september 2020 (SWD (2020) 198). Dagens kostnader forbundet med hendelser er en usikker størrelse, og EU-kommisjonen anslo i 2020 årlige besparelser i sektoren på mellom 0,2 og 2,7 mrd. euro. EU-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 (TLPT-testing) vil medføre egne behov for administrasjon og oppfølging i de 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 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.

4.1.3 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. 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.

4.1.4 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.

4.1.5 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, delta i IKT-overvåkingsforumet og ev. undersøkelsesgrupper, og følge opp anbefalinger til IKT-leverandører. I tillegg vil det være behov for å følge opp regelverkets krav om trusselbasert penetrasjonstesting (TLPT) i samarbeid med Norges Bank, samt 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. Arbeidet som Finanstilsynet og Norges Bank har lagt ned i utviklingen av TIBER-NO, antas å redusere behovet for økt ressursbruk for å følge opp TLPT-kravene.

4.2 Endringer i hvitvaskingsloven om opplysninger som skal følge overføringer av penger og visse kryptoeiendeler (TFR II)

4.2.1 Innledning

I dag har kryptoeiendelstjenesteytere begrensede plikter etter hvitvaskingsregelverket. TFR II gir, sammen med MiCA, nye forpliktelser for tjenesteytere som driver virksomhet med kryptoeiendeler. Ved gjennomføring i norsk rett av TFR II vil både tilsynsmyndigheter og tjenesteytere som foretar overføringer få mer omfattende forpliktelser etter hvitvaskingsregelverket. De nye kravene, herunder utvidelsen av kretsen av rapporteringspliktige, ventes å styrke arbeidet mot hvitvasking og terrorfinansiering og legge til rette for en ordnet utvikling og bruk av kryptoeiendeler.

4.2.2 Konsekvenser for foretak

TFR II fastsetter at samtlige kryptoeiendelstjenesteytere vil være rapporteringspliktige etter hvitvaskingsregelverket. Dette forventes å gi økte kostnader for markedsaktører som nå blir underlagt hvitvaskingsregelverket og må utarbeide rutiner og treffe tiltak for å etterleve det. De nye kravene om opplysninger som skal følge med overføringer av kryptoeiendeler vil også gi flere forpliktelser knyttet til systemer og rutiner. Det antas imidlertid at de fleste registrerte tjenesteyterne av vekslings- og oppbevaringstjenester allerede har begynt å tilpasse seg de nye informasjonskravene etter TFR II, mens andre foretak kan måtte legge en større innsats i å tilpasse seg.

4.2.3 Konsekvenser for myndigheter

TFR II innebærer at flere foretak blir rapporteringspliktige etter hvitvaskingsregelverket. Dette kan medføre noe økt aktivitet hos Finanstilsynet og Enheten for finansiell etterretning (EFE) i Økokrim. For Finanstilsynet forventer departementet at gjennomføringen av TFR II ikke i seg selv vil gi vesentlige økonomiske og administrative konsekvenser. Etter finanstilsynsloven skal kostnader ved tilsyn med aktørene i kryptoeiendelsmarkedet utliknes på aktørene. De nærmere reglene må fastsettes i forskrift. For EFE kan det bli en økning i innrapportering av mistenkelige transaksjoner som må håndteres tidsnært.

5 Merknader til de enkelte bestemmelsene

5.1 Til lov om digital operasjonell motstandsdyktighet i finanssektoren (DORA-loven)

Til § 1

I *første ledd* gjennomføres DORA-forordningen ved inkorporasjon, og bestemmelsene i forordningen vil etter dette gjelde som lov.

Annet ledd viser til at med DORA-forordningen menes forordningen slik den er gjennomført i første ledd, det vil si i EØS-tilpasset form, og med eventuelle endringer gjennomført eller henvist til i første ledd, eller gjennomført i forskrift med hjemmel i fjerde ledd.

Tredje ledd gir departementet hjemmel til å fastsette utfyllende regler i forskrift. Hjemmelen kan bl.a. brukes til å gjennomføre utfyllende EU-rettsakter som er fastsatt i medhold av DORA-forordningen (nivå 2-regelverk), og til å fastsette andre utfyllende regler.

Fjerde ledd gir hjemmel for departementet til å gjennomføre endringer i forordningen ved forskrift, selv om forordningen er gjennomført i lov. Dette gir mulighet til å gjennomføre endringer i DORA-forordningen som er av en karakter som normalt ville vært gjennomført ved forskrift, i forskrifts form i stedet for ved lovendring. Hjemmelen kan bare brukes til å gjennomføre EØS-forpliktelser. Hvorvidt derogasjonshjemmelen kan anvendes, må bero på en konkret skjønnsmessig vurdering.

Se nærmere omtale i punkt 2.5.2.3.

Til § 2

Første ledd gir departementet forskriftshjemmel til å bestemme at forordningen helt eller delvis skal gjelde for finansieringsforetak, låneformidlingsforetak, inkassoforetak og eiendomsmeglingsforetak, samt for foretak som i forordningen er unntatt fra dens virkeområde. Hjemmelen vil kunne benyttes til å fastsette fullstendige eller forenklede krav for foretak som ikke omfattes av forordningen. Departementet gis også hjemmel til å fastsette regler om i hvilket omfang DORA-forordningen skal gjelde for morselskap i finanskonsern.

I *annet ledd* fremgår det at departementet i forskrift bl.a. vil kunne bestemme at foretakene nevnt i første ledd skal underlegges et forenklet regelverk, herunder ved videreføring eller innføring av de plikter som følger av IKT-forskriften.

Til § 3

I *første ledd* slås det fast at Finanstilsynet er nasjonal tilsynsmyndighet etter forordningen og skal føre tilsyn med overholdelse av bestemmelser gitt i eller i medhold av loven. Dette samsvarer med Finanstilsynets myndighet etter de regelverkene som er nevnt i forordningens artikkel 46.

I *annet ledd* gis departementet hjemmel til å fastsette utfyllende krav til rapportering og annen informasjon som foretak omfattet av §§ 1 og 2 skal gi Finanstilsynet om inngåtte og planlagte avtaler om bruk av tjenester fra IKT-leverandører. Bestemmelsen er bl.a. ment å legge til rette for regler som er nødvendig for at Finanstilsynet skal kunne gjennomføre et effektivt tilsyn med foretakenes utkontraktering, herunder om hyppighet av rapportering for nye IKT-tjenesteavtaler og meldinger om planlagte IKT-tjenesteavtaler som understøtter kritiske eller viktige funksjoner, og ev. behov for utfyllende regler knyttet til register over IKT-tjenesteavtaler.

I *tredje ledd* gis departementet hjemmel til å fastsette regler om hendelsesrapportering og informasjonsdeling til andre varslingsmottakere enn Finanstilsynet. Bestemmelsen er nærmere omtalt i punkt 2.5.5.3.

I *fjerde ledd* gis departementet hjemmel til å fastsette nærmere regler om trusselbasert penetrasjonstesting (TLPT), herunder om oppgavefordeling mellom Finanstilsynet og Norges Bank. Det vises til DORA-forordningen artikkel 26 og omtale i punkt 2.5.7.

Til § 4

Bestemmelsen gir nærmere regler om overtredelsesgebyr etter DORA-forordningen, jf. omtale i punkt 2.5.8.

I *første ledd* fastsettes det at Finanstilsynet kan ilegge fysiske personer eller foretak overtredelsesgebyr på inntil 50 millioner kroner ved overtredelse av nærmere angitte bestemmelser i DORA-forordningen.

Det følger av *annet ledd* at også medvirkning til overtredelse av de bestemmelsene i DORA-forordningen som er nevnt i første ledd, kan sanksjoneres med overtredelsesgebyr på opptil 50 millioner kroner.

Tredje ledd gir nærmere regler om hvilket skyldkrav som gjelder for ileggelse av overtredelsesgebyr. Fysiske personer kan ilegges overtredelsesgebyr for forsettlige eller uaktsomme overtredelser, mens foretak kan ilegges overtredelsesgebyr når foretaket eller noen som har handlet på foretakets vegne, forsettlig eller uaktsomt har begått en overtredelse.

Fjerde ledd første punktum bestemmer at adgangen til å ilegge overtredelsesgebyr foreldes fem år etter at overtredelsen er opphørt. Det fremgår av annet punktum at foreldelsesfristen avbrytes ved at Finanstilsynet gir forhåndsvarsel eller fatter vedtak om overtredelsesgebyr.

I *femte ledd* gis det forskriftshjemler til departementet til å fastsette utfyllende bestemmelser om overtredelsesgebyr og renter ved forsinket betaling, herunder hjemmel til å fastsette i forskrift at den som forsettlig eller uaktsomt overtrer bestemmelser i forskrift gitt i medhold av loven, kan ilegges overtredelsesgebyr.

Til § 5

Bestemmelsen regulerer lovens ikrafttredelse.

Første ledd fastsetter at loven gjelder fra den tid Kongen bestemmer. Kongen kan sette i kraft de enkelte bestemmelser til forskjellig tid.

Annet ledd gir departementet hjemmel til å fastsette overgangsregler.

Til § 6

Forordnings- og direktivendringene som er omtalt i punkt 2.4, 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 følge av forordning (EU) 2022/2554 (DORA-forordningen), i tillegg til endringer for å sikre konsistens med kravene og begrepsbruken i forordningen. Det foreslås slike tilpasninger i:

- verdipapirhandelloven § 8-1 første ledd, § 9-16 første ledd, § 9-23 første og annet ledd, § 11-18 første ledd nr. 2, § 11-19 første og annet ledd, § 11-21 fjerde ledd, § 17-1 første ledd og § 19-2 første ledd,
- verdipapirfondloven § 2-11 første ledd nr. 1,
- lov om forvaltning av alternative investeringsfond § 3-1 første ledd bokstav b,
- lov om kredittvurderingsbyråer § 1,
- finansforetaksloven § 13-5 første ledd og § 20-6 a tredje ledd bokstav g,
- referanseverdiloven § 1 første ledd, og
- verdipapirsentralloven § 1-1 første ledd.

I tillegg foreslås en endring i finanstilsynsloven § 4-6 for å sørge for klarhet om forholdet mellom rapporteringsforpliktelsene som gjelder etter lov om digital motstandsdyktighet i finanssektoren og finanstilsynsloven § 4-6, se omtale i punkt 2.5.6.

5.2 Til endringer i hvitvaskingsloven (TFR II)

Til § 2

Paragrafen inneholder hvitvaskingslovens definisjoner.

I *bokstav i nr. 2* oppdateres definisjonen av korrespondentforbindelse til å inkludere kryptoeiendelstjenesteytere gjennom en henvisning til ny § 4 første ledd bokstav p som definerer kryptoeiendelstjenesteytere. I tillegg tilføyes kryptooverføringer til opplistingen av tjenester som foranlediger en korrespondentforbindelse. Forslaget retter dessuten en inkurie, slik at bokstav i nr. 2 nå også refererer til rapporteringspliktige som nevnt i § 4 første ledd bokstav a.

I ny *bokstav l* kommer det inn en definisjon av kryptoeiendeler. Det vises til definisjonen i MiCA, med noen begrensninger. MiCA artikkel 3 nr. 1 punkt 5 definerer kryptoeiendeler som en digital representasjon av en verdi eller en rettighet som kan overføres og oppbevares elektronisk ved bruk av distribuert registerteknologi eller lignende teknologi. Unntatt fra definisjonen av kryptoeiendeler er en rekke type verdier som opplistet i MiCA artikkel 2 nr. 2 til 4, samt betalingsmidler som definert i TFR II artikkel 3 nr. 8.

I ny *bokstav m* defineres kryptoeiendelstjenesteyter. Det vises til definisjonen i MiCA artikkel 3 nr. 1 punkt 5 som definerer kryptoeiendelstjenesteytere som juridiske personer eller

andre foretak som har tillatelse til å drive virksomhet med å tilby kryptoeiendelstjenester til kunder på profesjonell basis. Bokstav m presiserer at kryptoeiendelstjenesteytere ikke omfattes av kravene i TFR II når de kun yter rådgivning og ikke yter tjenestene som er listet opp i MiCA artikkel 3 nr. 1 punkt 16.

I ny *bokstav n* defineres frittstående adresse. Det vises til definisjonen i TFR II artikkel 3 nr. 1 punkt 20 som definerer frittstående adresse («self-hosted address») som en adresse på en distribuert registerteknologi som ikke er knyttet til en tilbyder av konsesjonspliktige tjenester.

Til § 4

I ny *bokstav p* tilføyes kryptoeiendelstjenesteytere til listen over rapporteringspliktige.

Femte ledd oppdateres ved å fjerne delen om vekslingsplattformer og oppbevaringstjenester for virtuell valuta. Heretter vil forskriftshjemmelen i femte ledd dermed gjelde å gi loven anvendelse for foretak som formidler finansiering ved donasjon.

Til § 10

Første ledd bokstav d er ny, og bestemmer at kundetiltak skal gjennomføres når og i den grad det er påkrevd av TFR II. Hvilke opplysninger som ved behov må innhentes og bekreftes, vil være avhengig av reglene i TFR II om opplysninger som skal følge pengeoverføringer og overføringer av kryptoeiendelstjenester. Bestemmelsen er nærmere omtalt i punkt 3.3.5.

Til § 17a

Paragrafen er ny, og reflekterer kravene til forsterkede kundetiltak for overføringer til og fra frittstående adresse. Kryptoeiendelstjenesteytere må først foreta en konkret risikovurdering av overføringen som gjennomføres. Tjenesteyterne må gjennomføre minst ett av de forsterkede kundetiltakene som er opplistet i bokstav a til e. Basert på risikovurderingen må tjenesteytere gjennomføre flere kundetiltak der det er nødvendig for å håndtere risikoen for hvitvasking, terrorfinansiering eller oppfølgning av økonomiske sanksjoner.

Til § 19

Første ledd oppdateres for å inkludere en henvisning til ny bokstav p i lovens § 4, slik at kryptoeiendelstjenesteytere blir omfattet av kretsen av rapporteringspliktige som bestemmelsen gjelder for.

Annet ledd justeres slik at konto for kryptoeiendeler inngår i definisjonen av oppgjørskonto.

Tredje ledd tilføyer at kryptoeiendelstjenesteytere som avslutter en korrespondentforbindelse på grunn av egne rutiner, skal dokumentere begrunnelsen for beslutningen. Avslutning av korrespondentforbindelser kan eksempelvis være aktuelt der en korresponderende kryptoeiendelstjenesteyter gjentatte ganger bryter informasjonspliktene i TFR II, jf. forordningens artikkel 8 nr. 2 bokstav b og artikkel 12 nr. 2 bokstav b.

Til § 49

Første ledd første punktum oppdateres til å inkludere en henvisning til oppdatert § 52, slik at inkorporeringsbestemmelsen til TFR II blir med i opplistingen av regler hvis overtredelse kan medføre overtredelsesgebyr fra tilsynsmyndigheten.

Femte ledd første og annet punktum oppdateres til å inkludere en henvisning til § 4 bokstav p, slik at kryptoeiendelstjenesteytere, samt styremedlemmer, ledere, ansatte og andre som utfører oppdrag på vegne av kryptoeiendelstjenesteyteren, kan ilegges overtredelsesgebyr på inntil 44 millioner kroner.

Til § 52

Første ledd oppdateres med en henvisning til TFR II i EØS-avtalen, og angir at TFR II gjelder som lov med tilpasningene som følger av vedlegg IX, protokoll 1 til avtalen og avtalen for øvrig.

Nytt *annet ledd* inneholder en forskriftshjemmel til å gi nærmere bestemmelser om forlengelse av lagringstid av personopplysninger utover fem år, men ikke i mer enn til sammen ti år. Forskriftshjemmelen reflekterer det nasjonale valget i TFR II artikkel 26 nr. 2 som åpner for at stater kan gi regler om utvidet lagringstid for personopplysninger der det er nødvendig og proporsjonalt for å forebygge, avdekke eller etterforske hvitvasking eller terrorfinansiering.

Finansdepartementet

t i l r å r :

At Deres Majestet godkjenner og skriver under et framlagt forslag til proposisjon til Stortinget om lov om digital operasjonell motstandsdyktighet i finanssektoren, lov om endringer i hvitvaskingsloven (gjennomføring av forordning (EU) 2023/1113) og samtykke til godkjenning av to beslutninger i EØS-komiteen om innlemmelse i EØS-avtalen av forordning (EU) 2022/2554, direktiv (EU) 2022/2556 og forordning (EU) 2023/1113.

Vi HARALD, Norges Konge,

s t a d f e s t e r :

Stortinget blir bedt om å gjøre vedtak til lov om digital operasjonell motstandsdyktighet i finanssektoren (DORA-loven), lov om endringer i hvitvaskingsloven (gjennomføring av forordning (EU) 2023/1113) og vedtak om samtykke til godkjenning av EØS-komiteens beslutning nr. 40/2025 om innlemmelse i EØS-avtalen av forordning (EU) 2022/2554 og direktiv (EU) 2022/2556, og nr. 42/2025 om innlemmelse av forordning (EU) 2023/1113 i samsvar med et vedlagt forslag.

A

Forslag

til lov om digital operasjonell motstandsdyktighet i finanssektoren (DORA-loven)

§ 1 *Forordningen om digital operasjonell motstandsdyktighet i finanssektoren*

(1) EØS-avtalen vedlegg IX nr. 31q (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) Når det i loven her vises til DORA-forordningen, menes forordningen slik den til enhver tid er gjennomført og endret etter første eller fjerde ledd.

(3) Departementet kan fastsette utfyllende forskrifter til bestemmelsene i første ledd.

(4) Departementet kan i forskrift gjøre endringer i, herunder fastsette unntak fra, bestemmelsene i første ledd til gjennomføring av Norges forpliktelser etter EØS-avtalen.

§ 2 *Forordningens anvendelse på andre foretak*

(1) Departementet kan i forskrift fastsette at bestemmelsene i § 1 helt eller delvis skal gjelde for:

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

(2) Departementet kan i forskrift fastsette forenklede krav for foretak nevnt i første ledd i samsvar med relevante bestemmelser i DORA-forordningen.

§ 3 *Tilsyn mv.*

(1) Finanstilsynet er nasjonal tilsynsmyndighet etter DORA-forordningen og fører tilsyn med overholdelse av bestemmelser gitt i eller i medhold av denne loven.

(2) Departementet kan i forskrift fastsette utfyllende krav til rapportering, register over IKT-tjenesteavtaler og annen informasjon som foretak omfattet av §§ 1 eller 2 skal gi Finanstilsynet om inngåtte og planlagte avtaler om bruk av tjenester fra IKT-leverandører.

(3) Departementet kan i forskrift fastsette bestemmelser om rapportering av hendelser og deling av informasjon til andre varslingsmottakere enn Finanstilsynet.

(4) Departementet kan i forskrift fastsette bestemmelser om trusselbasert penetrasjonstesting (TLPT), herunder om fordeling av oppgaver og ansvar mellom norske myndighetsorgan i henhold til DORA-forordningen artikkel 26.

§ 4 *Overtredelsesgebyr*

(1) Finanstilsynet kan ilegge fysiske personer eller foretak overtredelsesgebyr på inntil 50 millioner kroner ved overtredelse av følgende bestemmelser i DORA-forordningen:

a. artikkel 5 om forvaltning og organisasjon,
b. artikkel 6 om rammeverk for IKT-risikostyring,
c. artikkel 8 om identifisering av IKT-relaterte funksjoner og avhengigheter,
d. artikkel 9 nr. 4 om retningslinjer for sikkerhet mv. som del av rammeverket for IKT-risikostyring, jf. artikkel 6,
e. artikkel 11 om respons og gjenoppretting,
f. artikkel 12 om retningslinjer og prosedyrer for sikkerhetskopiering og gjenoppretting,
g. artikkel 14 om planer for krisekommunikasjon,
h. artikkel 16 nr. 1 og 2 om forenklet rammeverk for IKT-risikostyring,
i. artikkel 17 om prosess for håndtering av IKT-relaterte hendelser,
j. artikkel 19 nr. 1, 3 og 4 om rapportering av alvorlige IKT-relaterte hendelser,
k. artikkel 24 om generelle krav til gjennomføringen av testing av digital operasjonell motstandsdyktighet,
l. artikkel 25 nr. 2 om sårbarhetsvurderinger før bruk av nye systemer i verdipapirsentraler og sentrale motparter,
m. artikkel 28 om generelle prinsipper for forsvarlig styring av IKT-tredjepartsrisiko,

n. artikkel 42 nr. 3 annet avsnitt om hensyntaken til risiko avdekket hos IKT-leverandører.

Første punktum gjelder tilsvarende ved overtredelse av forskrifter som gjennomfører tekniske reguleringsstandarder fastsatt etter DORA-forordningen artikkel 15 og artikkel 16 nr. 3.

(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) Adgangen til å ilegge overtredelsesgebyr foreldres fem år etter at overtredelsen er opphørt. Fristen avbrytes ved at Finanstilsynet gir forhåndsvarsel eller fatter vedtak om overtredelsesgebyr.

(5) Departementet kan i forskrift fastsette bestemmelser til utfylling og avgrensning av paragrafen her, og renter ved forsinket betaling av overtredelsesgebyret. Departementet kan i forskrift fastsette at den som forsettlig eller uaktsomt overtrer bestemmelser i forskrift gitt i medhold av loven, kan ilegges overtredelsesgebyr.

§ 5 *Ikrafttredelse og overgangsbestemmelser*

(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 *Endringer i andre lover*

Fra den tid loven trer i kraft gjøres følgende endringer i andre lover:

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

§ 8-1 første ledd skal lyde:

(1) 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, jf. lov om digital operasjonell motstandsdyktighet i finanssektoren § 1* 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:

(1) Verdipapirforetak skal innrette sin virksomhet på følgende måte:

1. Foretaket skal ha tilstrekkelige og betryggende retningslinjer, rutiner og kontrollmeto-

der 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, jf. lov om digital operasjonell motstandsdyktighet i finanssektoren § 1.*
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, jf. lov om digital operasjonell motstandsdyktighet i finanssektoren § 1.*
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, jf. lov om digital operasjonell motstandsdyktighet i finanssektoren § 1,* 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, jf. lov om digital operasjonell motstandsdyktighet i finanssektoren § 1,* 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 i forordning (EU) 2022/2554 kapittel II og IV, jf. lov om digital operasjonell motstandsdyktighet i finanssektoren § 1.*

§ 11-18 første ledd nr. 2 skal lyde:

2. 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, jf. lov om digital operasjonell motstandsdyktighet i finanssektoren § 1*,

§ 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, jf. lov om digital operasjonell motstandsdyktighet i finanssektoren § 1,* 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, jf. lov om digital operasjonell motstandsdyktighet i finanssektoren § 1,* som sikrer kontinuerlig drift ved svikt i handelssystemet.

§ 11-21 fjerde ledd skal lyde:

(4) 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, jf. lov om digital operasjonell motstandsdyktighet i finanssektoren § 1.*

§ 17-1 første ledd skal lyde:

(1) 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, jf. lov om digital operasjonell motstandsdyktighet i finanssektoren § 1,* 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:

(1) Verdipapirforetak, sentrale motparter, datarapporteringsforetak og markedsoperatører, *samt IKT tredjeparts tjenesteleverandører som referert til i kapittel V i forordning (EU) 2022/2554, jf. lov om digital operasjonell motstandsdyktighet i finanssektoren § 1,* 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.

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

1. 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, jf. lov om digital operasjonell motstandsdyktighet i finanssektoren § 1,

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

a. 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, jf. lov om digital operasjonell motstandsdyktighet i finanssektoren § 1,* og regler for ansattes personlige transaksjoner,

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

§ 1 *EØS-regler om kredittvurderingsbyråer*

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, jf. lov om digital operasjonell motstandsdyktighet i finanssektoren § 1,* gjelder som lov med de tilpasninger som følger av vedlegg IX, protokoll 1 til avtalen og avtalen for øvrig.

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

§ 13-5 første ledd skal lyde:

(1) 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, jf. lov om digital operasjonell motstandsdyktighet i finanssektoren § 1.* Foretaket skal også ha hensiktsmessige retningslinjer og rutiner for gjennomføring, overvåkning og regelmessig vurdering av godtgjørelsesordninger.

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

g. 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,*

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

(1) 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, jf. lov om digital operasjonell motstandsdyktighet i finanssektoren § 1,* gjelder som lov med de tilpasninger som følger av vedlegg IX, protokoll 1 til avtalen og avtalen for øvrig.

7. 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 verdipapiroppgjør 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 (verdipapirsentralforordningen)) *som endret ved forordning (EU) 2022/2554, jf. lov om digital operasjonell motstandsdyktighet i finanssektoren § 1,* gjelder som lov med de tilpasninger som følger av vedlegg IX til avtalen, protokoll 1 til avtalen og avtalen for øvrig.

8. I lov 21. juni 2024 nr. 41 om Finanstilsynet (finanstilsynsloven) skal § 4-6 første ledd lyde:

(1) *Med unntak av avtaler om bruk av tjenester fra IKT-leverandører som nevnt i forordning (EU) 2022/2554 kapittel V, jf. lov om digital operasjonell motstandsdyktighet i finanssektoren §§ 1 og 2, skal foretak under tilsyn* melde fra til Finanstilsynet ved inngåelse av avtale om utkontraktering av virksomhet som er kritisk eller viktig for foretaket, og ved endringer av slike avtaler. Meldingen skal gis minst 60 dager før iverksettelsen av avtalen eller avtaleendringen.

B

Forslag

til lov om endringer i hvitvaskingsloven (gjennomføring av forordning (EU) 2023/1113)

I

I lov 1. juni 2018 nr. 23 om tiltak mot hvitvasking og terrorfinansiering gjøres følgende endringer:

§ 2 bokstav i nr. 2 skal lyde:

2. forbindelsene mellom rapporteringspliktige som nevnt i § 4 første ledd bokstav *a til c*, e, g til l og *n til p* seg imellom, herunder der lignende tjenester ytes av en korrespondentinstitusjon til en respondentinstitusjon, samt forbindelsene som er opprettet med sikte på verdipapirtransaksjoner, *pengeoverføringer og overføringer av kryptoeiendeler.*

§ 2 ny bokstav l, m og n skal lyde:

l. kryptoeiendeler: eiendeler som nevnt i forordning (EU) 2023/1114 artikkel 3 nr. 1 punkt 5, med unntak av eiendeler som nevnt i artikkel 2 nr. 2 til 4 og eiendeler som nevnt i forordning (EU) 2023/1113 artikkel 3 punkt 8.

m. kryptoeiendelstjenesteyter: person som nevnt i forordning (EU) 2023/1114 artikkel 3 nr. 1 punkt 15, når vedkommende yter tjenester som nevnt i artikkel 3 nr. 1 punkt 16, unntatt når vedkommende yter rådgivning som nevnt i artikkel 3 nr. 1 punkt 16 bokstav h.

n. frittstående adresse: frittstående adresse som nevnt i forordning (EU) 2023/1113 artikkel 3 punkt 20.

§ 4 første ledd ny bokstav p skal lyde:

p. kryptoeiendelstjenesteytere

§ 4 femte ledd skal lyde:

(5) Departementet kan i forskrift gi regler som gir loven anvendelse for foretak som formidler finansiering ved *donasjon.*

§ 10 første ledd ny bokstav d skal lyde:

d. pengeoverføringer og overføringer av kryptoeiendeler når dette er påkrevd etter forordning (EU) 2023/1113, jf. § 52.

Ny § 17 a skal lyde:

§ 17 a *Forsterkede kundetiltak for transaksjoner på frittstående adresse*

Ved gjennomføring av transaksjoner til eller fra frittstående adresser skal kryptoeiendelstjenesteytere foreta en konkret risikovurdering av transaksjonen. Minst ett av følgende forsterkede kundetiltak skal gjennomføres:

a. identifisering og verifisering av identiteten til avsenderen og mottakeren og deres reelle rettighetshavere

b. krav om ytterligere informasjon om midlenes opprinnelse og mottakeren av de overførte kryptoeiendelene

c. forsterket løpende oppfølging av transaksjonene

d. andre tiltak for å motvirke og håndtere risikoen for hvitvasking og terrorfinansiering

e. tiltak for å motvirke og håndtere risiko knyttet til oppfølging av økonomiske sanksjoner og sanksjoner tilknyttet finansiering av masseødeleggelsesvåpen, som følger av regler om gjennomføring av internasjonale sanksjoner.

§ 19 skal lyde:

§ 19 *Forsterkede kundetiltak ved korrespondentforbindelse*

(1) Ved inngåelse av en avtale om korrespondentforbindelse med en institusjon fra stat utenfor EØS som respondentinstitusjon, skal rapporteringspliktige som nevnt i § 4 første ledd bokstav a til c, e, g til l og *n til p*

a. innhente tilstrekkelige opplysninger om respondentinstitusjonen for å forstå virksomhetens art og omdømme og tilsynets kvalitet. *Rapporteringspliktige etter § 4 første ledd bokstav p skal også fastslå om respondentinstitusjonen er registrert eller har konsesjon.*

b. vurdere respondentinstitusjonens tiltak mot hvitvasking og terrorfinansiering

c. påse at det innhentes godkjenning fra overordnet før etablering av ny korrespondentforbindelse

d. dokumentere institusjonenes ansvar
e. ved oppgjørskonti forsikre seg om at respondentinstitusjonen
   1. har bekreftet identiteten til og fører løpende oppfølging av kunder som har direkte adgang til konti hos korrespondentinstitusjonen, og
   2. på anmodning kan fremlegge relevante opplysninger fra kundetiltakene og den løpende oppfølgingen til korrespondentinstitusjonen.

(2) Med oppgjørskonto som nevnt i første ledd bokstav e, *menes konto eller konto for kryptoeiendeler hos rapporteringspliktig som kan disponeres av en tredjepart som er kunde av respondentinstitusjon*.

(3) En kryptoeiendelstjenesteyter som avslutter en korrespondentforbindelse på grunn av egne rutiner etter denne loven, skal dokumentere begrunnelsen for beslutningen.

§ 49 første ledd første punktum skal lyde:
Dersom rapporteringspliktige eller noen som har handlet på vegne av et rapporteringspliktig foretak, har overtrådt §§ 6 til 8, kapittel 4, §§ 25, 26, 27, 28, 30, 35, 36, 39, 42 *eller 52 eller forskrift gitt i medhold av disse bestemmelsene,* kan tilsynsmyndigheten ilegge den rapporteringspliktige overtredelsesgebyr.

§ 49 femte ledd første og annet punktum skal lyde:
Rapporteringspliktige som nevnt i § 4 første ledd bokstav a til c, e, g til k, *n og p*, kan ilegges overtredelsesgebyr på inntil 44 millioner kroner. Det samme gjelder styremedlemmer, ledere, ansatte og andre som utfører oppdrag på vegne av rapporteringspliktige som nevnt i § 4 første ledd bokstav a til c, e, g til k, *n og p*, dersom de kan ilegges overtredelsesgebyr etter annet og tredje ledd.

§ 52 skal lyde:
§ 52 *Opplysninger som skal følge overføringer av penger og visse kryptoeiendeler*

(1) EØS-avtalen vedlegg IX nr. 23b (forordning (EU) 2023/1113) om opplysninger som skal følge overføringer av penger og visse kryptoeiendeler (TFR II) gjelder som lov med de tilpasninger som følger av vedlegg IX, protokoll 1 til avtalen og avtalen for øvrig.

(2) Departementet kan i forskrift gi regler i tråd med forordning (EU) 2023/1113 artikkel 26 om lagring av personopplysninger utover fem år, men ikke i mer enn til sammen ti år.

II

1. Loven gjelder fra den tid Kongen bestemmer. Kongen kan sette i kraft de enkelte bestemmelsene til forskjellig tid.
2. Departementet kan gi overgangsregler.

C

Forslag

til vedtak om samtykke til godkjenning av EØS-komiteens beslutning nr. 40/2025 om innlemmelse i EØS-avtalen av forordning (EU) 2022/2554 og direktiv (EU) 2022/2556, og nr. 42/2025 om innlemmelse av forordning (EU) 2023/1113

I

Stortinget samtykker til godkjenning av EØS-komiteens beslutning nr. 40/2025 av 20. februar 2025 om innlemmelse i EØS-avtalen av forordning (EU) 2022/2554 og direktiv (EU) 2022/2556 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren.

II

Stortinget samtykker til godkjenning av EØS-komiteens beslutning nr. 42/2025 av 20. februar 2025 om innlemmelse i EØS-avtalen av forordning (EU) 2023/1113 av 31. mai 2023 om opplysninger som skal følge overføringer av penger og visse kryptoeiendeler, og om endring av direktiv (EU) 2015/849.

Vedlegg 1

Europaparlaments- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011

EUROPAPARLAMENTET OG RÅDET FOR DEN EUROPEISKE UNION HAR

under henvisning til traktaten om Den europeiske unions virkemåte, særlig artikkel 114,

under henvisning til forslag fra Europakommisjonen,

etter oversending av utkast til regelverksakt til de nasjonale parlamentene,

under henvisning til uttalelse fra Den europeiske sentralbank[1],

under henvisning til uttalelse fra Den europeiske økonomiske og sosiale komité[2],

etter den ordinære regelverksprosedyren[3] og ut fra følgende betraktninger:

1) I den digitale tidsalderen støtter informasjons- og kommunikasjonsteknologi (IKT) komplekse systemer som brukes i forbindelse med daglige aktiviteter. Det holder økonomien i gang i viktige sektorer, herunder finanssektoren, og forbedrer det indre markeds virkemåte. Økt digitalisering og innbyrdes forbindelser øker også IKT-risikoen og gjør samfunnet som helhet, og særlig finanssystemet, mer sårbart overfor cybertrusler eller IKT-forstyrrelser. Den allment utbredte bruken av IKT-systemer og en høy grad av digitalisering og konnektivitet er i dag sentrale trekk i den virksomheten som drives av Unionens finansielle enheter, men deres digitale motstandsdyktighet må fortsatt håndteres bedre og integreres i deres bredere operasjonelle rammer.
2) Bruken av IKT har de siste tiårene fått en sentral rolle i leveringen av finansielle tjenester og har nådd det punktet der den i dag er avgjørende for driften av alle finansielle enheters vanlige daglige funksjoner. Digitalisering omfatter i dag for eksempel betalinger som i økende grad har gått fra kontanter og papirbaserte metoder til bruk av digitale løsninger, samt clearing og oppgjør av verdipapirer, elektronisk handel og algoritmehandel, utlån og finansiering, peer-to-peer-finansiering, kredittvurdering, skadebehandling og back-office-funksjoner. Forsikringssektoren har også forandret seg med bruken av IKT, fra framveksten av forsikringsformidlere som tilbyr sine tjenester online ved hjelp av forsikringsteknologien InsurTech, til digital tegning av forsikring. Hele finanssektoren er i høy grad blitt digital, og digitaliseringen har også utdypet de innbyrdes forbindelsene og avhengigheten innen finanssektoren og med tredjepartsinfrastruktur og tredjepartsleverandører av tjenester.
3) Det europeiske råd for systemrisiko (ESRB) bekreftet i en rapport fra 2020 om systemrisiko på cyberområdet hvordan det eksisterende høye nivået av innbyrdes forbindelser blant finansielle enheter, finansmarkeder og finansmarkedsinfrastrukturer, og særlig den gjensidige avhengigheten mellom deres IKT-systemer, kan utgjøre en systemisk sårbarhet ettersom lokale cyberhendelser raskt kan spre seg fra en av de nærmere 22 000 finansielle enhetene i Unionen til hele finanssystemet, uhindret av geografiske grenser. Alvorlige IKT-relaterte overtredelser i finanssektoren påvirker ikke bare finansielle enheter isolert sett. De baner også veien for spredning av lokaliserte sårbarheter gjennom de finansielle overføringskanalene og kan få negative konsekvenser for stabiliteten i Unionens finanssystem, for eksempel gjen-

---

1 EUT C 343 av 26.8 2021, s. 1.

2 EUT C 155 av 30.4. 2021, s. 38.

3 Europaparlamentets holdning av 10. november 2022 (ennå ikke offentliggjort i EUT) og rådsbeslutning av 28. november 2022.

nom likviditetsmangel og generelt tap av tillit til finansmarkedene.

4) I de senere årene har IKT-risiko tiltrukket seg oppmerksomheten til politiske beslutningstakere, reguleringsmyndigheter og standardiseringsorganer på internasjonalt plan, unionsplan og nasjonalt plan i et forsøk på å øke den digitale motstandsdyktigheten, fastsette standarder og koordinere regulerings- eller tilsynsarbeid. På internasjonalt plan har Basel-komiteen for banktilsyn, Komiteen for betalings- og markedsinfrastruktur, Rådet for finansiell stabilitet, Financial Stability Institute samt G7 og G20 som mål å utstyre vedkommende myndigheter og markedsoperatører i ulike jurisdiksjoner med verktøyer for å styrke deres finanssystemers motstandsdyktighet. Dette arbeidet har også vært motivert av behovet for å ta behørig hensyn til IKT-risiko i et globalt finanssystem med sterke innbyrdes forbindelser og for å etterstrebe større samstemmighet når det gjelder relevant beste praksis.
5) Til tross for målrettede politiske og lovgivningsmessige initiativ på unionsplan og nasjonalt plan utgjør IKT-risiko fortsatt en utfordring for den operasjonelle motstandsdyktigheten, ytelsen og stabiliteten i Unionens finanssystem. De reformene som fulgte etter finanskrisen i 2008, styrket først og fremst den finansielle motstandsdyktigheten i Unionens finanssektor og tok sikte på å bevare Unionens konkurranseevne og stabilitet sett fra et økonomisk, tilsynsmessig og markedsmessig perspektiv. Selv om IKT-sikkerhet og digital motstandsdyktighet inngår i den operasjonelle risikoen, har de ikke fått like mye oppmerksomhet på den reguleringsmessige dagsordenen etter finanskrisen og er bare utviklet på noen områder av Unionens politikk og regelverk for finansielle tjenester, eller bare i noen få medlemsstater.
6) I sin kommisjonsmelding av 8. mars 2018 med tittelen «*Handlingsplan for FinTech: – et viktig skritt mot en mer konkurransedyktig og innovativ finanssektor i Europa*» understreket Kommisjonen at det er ytterst viktig å gjøre Unionens finanssektor mer motstandsdyktig, herunder sett fra et operasjonelt perspektiv, for å sikre dens teknologiske sikkerhet og at den fungerer godt, samt at den raskt kan gjenopprettes etter IKT-relaterte overtredelser og IKT-relaterte hendelser, noe som til slutt gjør det mulig å levere finansielle tjenester på en effektiv og smidig måte i hele Unionen, herunder i forbindelse med krisesituasjoner, samtidig som forbrukernes og markedets tillit bevares.
7) I april 2019 utstedte Den europeiske tilsynsmyndighet (Den europeiske banktilsynsmyndighet) (EBA), som ble opprettet ved europaparlaments- og rådsforordning (EU) nr. 1093/2010[4], Den europeiske tilsynsmyndighet (Den europeiske tilsynsmyndighet for forsikring og tjenestepensjoner) (EIOPA), som ble opprettet ved europaparlaments- og rådsforordning (EU) nr. 1094/2010[5], og Den europeiske tilsynsmyndighet (Den europeiske verdipapir- og markedstilsynsmyndighet) (ESMA), som ble opprettet ved europaparlaments- og rådsforordning (EU) nr. 1095/2010[6] (samlet kalt «de europeiske tilsynsmyndighetene» eller «ESMA»), i fellesskap en teknisk uttalelse og etterlyste en sammenhengende tilnærming til IKT-risiko i finanssektoren og anbefalte å styrke finansnæringens digitale operasjonelle motstandsdyktighet på en forholdsmessig måte gjennom et sektorspesifikt initiativ fra Unionen.
8) Unionens finanssektor er regulert av et felles regelverk og underlagt et europeisk finanstilsynssystem. Ikke desto mindre er bestemmelsene om håndtering av digital operasjonell motstandsdyktighet og IKT-sikkerhet ennå ikke fullstendig eller konsekvent harmoniserte, til tross for at den digitale operasjonelle motstandsdyktigheten er avgjørende for å sikre finansiell stabilitet og markedsintegritet i den digitale tidsalderen, og ikke mindre viktige enn for eksempel felles standarder for tilsyn eller markedsatferd. Det felles regelverket og tilsynssystemet bør derfor utvikles slik at det også omfatter digital operasjonell motstandsdyktighet gjennom å

---

4 Europaparlaments- og rådsforordning (EU) nr. 1093/2010 av 24. november 2010 om opprettelse av en europeisk tilsynsmyndighet (Den europeiske banktilsynsmyndighet), om endring av beslutning nr. 716/2009/EF og om oppheving av kommisjonsbeslutning 2009/78/EF (EUT L 331 av 15.12.2010, s. 12).

5 Europaparlaments- og rådsforordning (EU) nr. 1094/2010 av 24. november 2010 om opprettelse av en europeisk tilsynsmyndighet (Den europeiske tilsynsmyndighet for forsikring og tjenestepensjoner), om endring av beslutning nr. 716/2009/EF og om oppheving av kommisjonsbeslutning 2009/79/EF (EUT L 331 av 15.12.2010, s. 48).

6 Europaparlaments- og rådsforordning (EU) nr. 1095/2010 av 24. november 2010 om opprettelse av en europeisk tilsynsmyndighet (Den europeiske verdipapir- og markedstilsynsmyndighet), om endring av beslutning nr. 716/2009/EF og om oppheving av kommisjonsbeslutning 2009/77/EF (EUT L 331 av 15.12.2010, s. 84).

styrke vedkommende myndigheters mandat, slik at de får mulighet til å føre tilsyn med styringen av IKT-risiko i finanssektoren for å beskytte det indre markeds integritet og effektivitet, og for å fremme at det fungerer etter hensikten.

9) Lovgivningsmessige forskjeller og ulike nasjonale reguleringsstrategier for IKT-risiko skaper hindringer for et velfungerende indre marked for finansielle tjenester og hindrer en smidig utøvelse av etableringsadgangen og av retten til fri utveksling av tjenester for finansielle enheter som driver virksomhet over landegrensene. Konkurransen mellom samme type finansielle enheter som driver virksomhet i forskjellige medlemsstater, kan også bli vridd. Dette gjelder særlig for områder der Unionens harmonisering har vært svært begrenset, for eksempel testing av digital operasjonell motstandsdyktighet, eller ikke-eksisterende, for eksempel overvåking av IKT-tredjepartsrisiko. Forskjeller som skyldes planlagt utvikling på nasjonalt plan, kan skape ytterligere hindringer for det indre markeds virkemåte på bekostning av markedsdeltakere og finansiell stabilitet.

10) På grunn av at bestemmelser om IKT-risiko bare delvis er blitt behandlet på unionsplan, er det på det nåværende tidspunktet hull eller overlappinger på viktige områder, for eksempel når det gjelder rapportering av IKT-relaterte hendelser og testing av digital operasjonell motstandsdyktighet, samt manglende konsekvens når nye avvikende nasjonale regler utarbeides, eller overlappende regler anvendes på en kostnadsineffektiv måte. Dette er særlig skadelig for en IKT-intensiv bruker som finanssektoren, ettersom teknologirisikoer ikke kjenner noen grenser og finanssektoren anvender sine tjenester på et bredt grenseoverskridende grunnlag innen og utenfor Unionen. Enkelte finansielle enheter som driver virksomhet over landegrensene, eller som har flere tillatelser (én finansiell enhet kan for eksempel ha tillatelse som bank, verdipapirforetak og betalingsinstitusjon, der hver tillatelse er utstedt av ulike vedkommende myndigheter i en eller flere medlemsstater), står overfor operasjonelle utfordringer når det gjelder å styre IKT-risiko og redusere IKT-hendelsers negative virkninger på egen hånd og på en sammenhengende kostnadseffektiv måte.

11) Ettersom det felles regelverket ikke har vært ledsaget av et omfattende rammeverk for IKT eller operasjonell risiko, er det nødvendig med ytterligere harmonisering av viktige krav til digital operasjonell motstandsdyktighet for alle finansielle enheter. Den IKT-kapasiteten og den generelle motstandsdyktigheten som finansielle enheter med utgangspunkt i disse viktige kravene skal utvikle for å stå imot driftsforstyrrelser, vil bidra til å bevare stabiliteten og integriteten på Unionens finansmarkeder og dermed bidra til å sikre et sterkt investor- og forbrukervern i Unionen. Ettersom denne forordningen har som formål å bidra til at det indre marked virker tilfredsstillende, bør den bygge på artikkel 114 i traktaten om Den europeiske unions virkemåte (TEUV) slik den tolkes i Den europeiske unions domstols rettspraksis.

12) Denne forordningen har som formål å konsolidere og oppgradere kravene til IKT-risiko som en del av kravene til operasjonell risiko, som fram til nå har vært behandlet separat i ulike unionsrettsakter. Selv om disse rettsaktene omfatter hovedkategoriene av finansiell risiko (for eksempel kredittrisiko, markedsrisiko, motpartskredittrisiko, likviditetsrisiko og markedsatferdsrisiko), ble ikke alle komponentene i den operasjonelle motstandsdyktigheten behandlet på en fullstendig måte da disse rettsaktene ble vedtatt. Da reglene om operasjonell risiko ble nærmere utformet i disse unionsrettsaktene, ble det ofte foretrukket en tradisjonell kvantitativ strategi for å styre risiko (nemlig å fastsette et kapitalkrav for å dekke IKT-risiko) i stedet for målrettede kvalitative regler om beskyttelse, påvisning, begrensning, gjenoppretting og avhjelping av IKT-relaterte hendelser, eller om rapporteringskapasitet og digital testkapasitet. Disse rettsaktene skulle først og fremst omfatte og oppdatere grunnleggende regler om tilsyn, markedsintegritet eller atferd. Ved å konsolidere og oppgradere de ulike reglene om IKT-risiko, bør alle bestemmelser om digital risiko i finanssektoren for første gang bli samlet på en konsekvent måte i én enkelt rettsakt. Denne forordningen tetter derfor hullene eller avhjelper manglende konsekvens i noen av de tidligere rettsaktene, herunder med hensyn til terminologien som brukes i dem, og den viser eksplisitt til IKT-risiko gjennom målrettede regler om kapasitet til IKT-risikostyring, rapportering av hendelser, testing av operasjonell motstandsdyktighet og overvåking av IKT-tredjeparts-

risiko. Denne forordningen bør derfor også øke bevisstheten om IKT-risiko og anerkjenne at IKT-hendelser og manglende operasjonell motstandsdyktighet kan utgjøre en fare for finansielle enheters soliditet.

13) Finansielle enheter bør følge den samme tilnærmingen og de samme prinsippbaserte reglene i sin styring av IKT-risiko, samtidig som det tas hensyn til deres størrelse og generelle risikoprofil samt til arten, omfanget og kompleksiteten av deres tjenester, aktiviteter og drift. Konsekvens bidrar til å øke tilliten til finanssystemet og bevare dets stabilitet, særlig i tider med høy avhengighet av IKT-systemer, -plattformer og -infrastrukturer, noe som medfører økt digital risiko. Overholdelse av en grunnleggende cyberhygiene bør også hindre at økonomien påføres høye kostnader, ved at virkningene av og kostnadene i forbindelse med IKT-forstyrrelser minimeres.

14) En forordning bidrar til å redusere regelverkets kompleksitet, fremmer tilsynsmessig tilnærming og øker rettssikkerheten, og den bidrar også til å begrense kostnadene for å overholde bestemmelsene, særlig for finansielle enheter som driver virksomhet over landegrensene, og til å redusere konkurransevridninger. Derfor er valget av en forordning med henblikk på å opprette et felles rammeverk for finansielle enheters digitale operasjonelle motstandsdyktighet den mest hensiktsmessige måten for å sikre en homogen og sammenhengende anvendelse av alle de komponentene som inngår i IKT-risikostyring i Unionens finanssektor.

15) Europaparlaments- og rådsdirektiv (EU) 2016/1148[7] var det første overgripende rammeverket for cybersikkerhet som ble vedtatt på unionsplan, og som også får anvendelse på tre typer av finansielle enheter, nemlig kredittinstitusjoner, handelsplasser og sentrale motparter. Ettersom direktiv (EU) 2016/1148 fastsetter en ordning for identifisering av ytere av samfunnsviktige tjenester på nasjonalt plan, var det imidlertid bare visse kredittinstitusjoner, handelsplasser og sentrale motparter som ble utpekt av medlemsstatene, og som i praksis ble omfattet av direktivets virkeområde, og som derfor skal overholde de aktuelle rapporteringskravene til IKT-sikkerhet og IKT-hendelser som er fastsatt i direktivet. I europaparlaments- og rådsdirektiv (EU) 2022/2555[8] fastsettes enhetlige kriterier for å bestemme hvilke enheter som er omfattet av direktivets virkeområde (størrelsesbasert regel), samtidig som de tre typene av finansielle enheter fortsatt er omfattet av direktivets virkeområde.

16) Ettersom denne forordningen fører til en økt grad av harmonisering for de ulike komponentene som inngår i digital motstandsdyktighet, gjennom å innføre krav til IKT-risikostyring og rapportering av IKT-relaterte hendelser som er strengere enn dem som er fastsatt i gjeldende unionsregelverk for finansielle tjenester, utgjør imidlertid denne høyere graden en økt harmonisering også sammenlignet med de kravene som er fastsatt i direktiv (EU) 2022/2555. Denne forordningen utgjør derfor *lex specialis* med hensyn til direktiv (EU) 2022/2555. Samtidig er det svært viktig å opprettholde en tett forbindelse mellom finanssektoren og Unionens overgripende rammeverk for cybersikkerhet som for øyeblikket er fastsatt i direktiv (EU) 2022/2555, for å sikre samsvar med de strategiene for cybersikkerhet som er vedtatt av medlemsstatene, og for å gi finansielle tilsynsmyndigheter mulighet til få kjennskap til cyberhendelser som påvirker andre sektorer som er omfattet av det nevnte direktivet.

17) I samsvar med artikkel 4 nr. 2 i traktaten om Den europeiske union og uten at det berører Domstolens rettslige overprøving, bør denne forordningen ikke berøre medlemsstatenes ansvar med hensyn til vesentlige statlige funksjoner som gjelder offentlig sikkerhet, forsvar og ivaretakelse av nasjonal sikkerhet, for eksempel vedrørende utlevering av opplysninger som ville være i strid med ivaretakelse av nasjonal sikkerhet.

18) For å muliggjøre læring på tvers av sektorene og for å kunne dra nytte av andre sektorers erfaringer når det gjelder håndtering av cybertrusler, bør de finansielle enhetene som er nevnt i direktiv (EU) 2022/2555, forbli en del av «økosystemet» i det nevnte direktivet

---

[7] Europaparlaments- og rådsdirektiv (EU) 2016/1148 av 6. juli 2016 om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i hele Unionen (EUT L 194 av 19.7.2016, s. 1).

[8] Europaparlaments- og rådsdirektiv (EU) 2022/2555 av 14. desember 2022 om tiltak for å sikre et høyt felles nivå av cybersikkerhet i hele Unionen, om endring av forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om oppheving av direktiv (EU) 2016/1148 (NIS-2-direktiv) (se EUT L 333 av 27.12.2022, s. 80).

(for eksempel samarbeidsgruppen og nettverket av enheter for håndtering av digitale hendelser (CSIRT-enheter)). De europeiske tilsynsmyndighetene og de nasjonale vedkommende myndighetene bør kunne delta i de strategiske politiske drøftingene og det tekniske arbeidet i samarbeidsgruppen i henhold til det nevnte direktivet, og utveksle opplysninger og samarbeide videre med de felles kontaktpunktene som er utpekt eller opprettet i samsvar med det nevnte direktivet. De vedkommende myndighetene i henhold til denne forordningen bør også rådføre seg med og samarbeide med CSIRT-enhetene. De vedkommende myndighetene bør også kunne anmode om en teknisk uttalelse fra de vedkommende myndighetene som er utpekt eller etablert i samsvar med direktiv (EU) 2022/2555, og etablere samarbeidsordninger som har til formål å sikre effektive og raske koordineringsordninger.

19) Med tanke på de sterke innbyrdes forbindelsene mellom finansielle enheters digitale motstandsdyktighet og fysiske motstandsdyktighet er det nødvendig med en sammenhengende tilnærming med hensyn til motstandsdyktigheten til kritiske enheter i denne forordningen og i europaparlaments- og rådsdirektiv (EU) 2022/2557[9]. Ettersom finansielle enheters fysiske motstandsdyktighet behandles på en omfattende måte i de forpliktelsene som gjelder IKT-risikostyring og rapportering i denne forordningen, bør forpliktelsene i kapittel III og IV i direktiv (EU) 2022/2557 ikke få anvendelse på finansielle enheter som er omfattet av det nevnte direktivets virkeområde.

20) Leverandører av skytjenester er én kategori av digital infrastruktur som er omfattet av direktiv (EU) 2022/2555. Unionsovervåkingsrammeverket («overvåkingsrammeverket») som er fastsatt ved denne forordningen, får anvendelse på alle kritiske tredjepartsleverandører av IKT-tjenester, herunder leverandører av skytjenester som leverer IKT-tjenester til finansielle enheter, og bør anses som et supplement til det tilsynet som utføres i henhold til direktiv (EU) 2022/2555. Videre bør det overvåkingsrammeverket som er fastsatt ved denne forordningen, omfatte leverandører av skytjenester i fravær av en overgripende unionsramme om opprettelse av en digital overvåkingsmyndighet.

21) For at finansielle enheter skal kunne opprettholde full kontroll over IKT-risiko, må de ha omfattende kapasitet som muliggjør en sterk og effektiv IKT-risikostyring, samt særskilte ordninger og retningslinjer for håndtering av alle IKT-relaterte hendelser og for rapportering av alvorlige IKT-relaterte hendelser. På samme måte bør finansielle enheter ha innført retningslinjer for testing av IKT-systemer, IKT-kontroller og IKT-prosesser, samt for styring av IKT-tredjepartsrisiko. Referansenivået for digital operasjonell motstandsdyktighet hos finansielle enheter bør økes, samtidig som det også skapes mulighet for en forholdsmessig anvendelse av krav til visse finansielle enheter, særlig svært små bedrifter, samt finansielle enheter som er underlagt et forenklet rammeverk for IKT-risikostyring. For å legge til rette for et effektivt tilsyn med tjenestepensjonsforetak som er forholdsmessig og ivaretar behovet for å redusere den administrative byrden for de vedkommende myndighetene, bør de relevante nasjonale tilsynsordningene for slike finansielle enheter ta hensyn til deres størrelse og generelle risikoprofil, samt til arten, omfanget og kompleksiteten av deres tjenester, aktiviteter og drift, selv når de relevante tersklene fastsatt i artikkel 5 i europaparlaments- og rådsdirektiv (EU) 2016/2341[10] overskrides. Framfor alt bør tilsynsvirksomheten først og fremst fokusere på behovet for å håndtere alvorlige risikoer i forbindelse med IKT-risikostyringen i en bestemt enhet.

De vedkommende myndighetene bør også opprettholde en årvåken, men forholdsmessig tilnærming når det gjelder tilsyn med tjenestepensjonsforetak som, i samsvar med artikkel 31 i direktiv (EU) 2016/2341, utkontrakterer en betydelig del av sin kjernevirksomhet til tjenesteytere, for eksempel kapitalforvaltning, aktuarielle beregninger, regnskap og databehandling.

22) Terskler og taksonomier for rapportering av IKT-relaterte hendelser varierer vesentlig på nasjonalt plan. Selv om det kan oppnås enighet gjennom det relevante arbeidet som utføres av Den europeiske unions byrå for

[9] Europaparlaments- og rådsdirektiv (EU) 2022/2557 av 14. desember 2022 om kritiske enheters motstandsdyktighet og om oppheving av rådsdirektiv 2008/114/EF (se EUT L 333 av 27.12.2022, s. 164).

[10] Europaparlaments- og rådsdirektiv (EU) 2016/2341 av 14. desember 2016 om virksomhet i og tilsyn med tjenestepensjonsforetak (EUT L 354 av 23.12.2016, s. 37).

cybersikkerhet (ENISA), opprettet ved europaparlaments- og rådsforordning (EU) 2019/881[11], og samarbeidsgruppen i henhold til direktiv (EU) 2022/2555, kan det fortsatt forekomme eller oppstå ulike strategier for terskler og taksonomier for andre finansielle enheter. På grunn av disse forskjellene er det flere krav som finansielle enheter må oppfylle, særlig når de driver virksomhet i flere medlemsstater, og når de inngår i et finanskonsern. Disse forskjellene kan dessuten hindre opprettelsen av ytterligere ensartede eller sentraliserte ordninger på unionsplan som framskynder rapporteringsprosessen og støtter en rask og smidig utveksling av opplysninger mellom vedkommende myndigheter, noe som er svært viktig for å styre IKT-risiko ved storstilte angrep med eventuelle systemiske konsekvenser.

23) For å redusere den administrative byrden og mulige overlappende rapporteringsforpliktelser for visse finansielle enheter bør kravet om rapportering av hendelser i henhold til europaparlaments- og rådsdirektiv (EU) 2015/2366[12] ikke lenger gjelde for betalingstjenesteytere som er omfattet av virkeområdet for denne forordningen. Derfor bør de kredittinstitusjonene, e-pengeforetakene, betalingsinstitusjonene og yterne av kontoopplysningstjenester som er nevnt i artikkel 33 nr. 1 i det nevnte direktivet, fra denne forordningens anvendelsesdato rapportere i henhold til denne forordningen alle betalingsrelaterte operasjonelle hendelser eller sikkerhetshendelser som tidligere er rapportert i henhold til det nevnte direktivet, uavhengig av om slike hendelser er IKT-relaterte.

24) For at de vedkommende myndighetene skal kunne ivareta sin tilsynsrolle gjennom å skaffe seg en fullstendig oversikt over arten, hyppigheten, betydningen og virkningen av IKT-relaterte hendelser, og for å styrke utvekslingen av opplysninger mellom relevante offentlige myndigheter, herunder rettshåndhevende myndigheter og krisehåndteringsmyndigheter, bør denne forordningen fastsette en robust ordning for rapportering av IKT-relaterte hendelser der de relevante kravene bøter på nåværende hull i regelverket for finansielle tjenester, og fjerne eksisterende overlappinger og dobbeltbestemmelser for å redusere kostnadene. Derfor er det viktig å harmonisere ordningen for rapportering av IKT-relaterte hendelser gjennom å kreve at alle finansielle enheter skal rapportere til sine vedkommende myndigheter gjennom et harmonisert rammeverk i samsvar med denne forordningen. I tillegg bør de europeiske tilsynsmyndighetene ha myndighet til ytterligere å spesifisere relevante elementer med hensyn til rammeverket for rapportering av IKT-relaterte hendelser, for eksempel taksonomier, tidsrammer, datasett, maler og gjeldende terskler. For å sikre fullt samsvar med direktiv (EU) 2022/2555 bør finansielle enheter på frivillig grunnlag gis tillatelse til å underrette den berørte vedkommende myndigheten om betydelige cybertrusler, når de anser at cybertrusselen er av relevans for finanssystemet, tjenestebrukerne eller kundene.

25) Det er utarbeidet krav til testing av digital operasjonell motstandsdyktighet i visse finansielle delsektorer med rammer som ikke alltid er fullt ut harmoniserte. Dette fører potensielt til en fordobling av kostnader for finansielle enheter over landegrensene, og gjør en gjensidig anerkjennelse av resultatene av testingen av digital operasjonell motstandsdyktighet komplisert, noe som igjen kan fragmentere det indre marked.

26) I de tilfellene der det ikke kreves noen IKT-testing, vil sårbarheter ikke bli oppdaget, hvilket fører til at en finansiell enhet utsettes for en IKT-risiko og til slutt skaper en høyere risiko for stabiliteten og integriteten i finanssektoren. Uten unionstiltak vil testingen av digital operasjonell motstandsdyktighet fortsatt være inkonsekvent, og det vil ikke finnes et system for gjensidig anerkjennelse av IKT-testresultater i ulike jurisdiksjoner. Ettersom det er usannsynlig at andre finansielle delsektorer vil ta i bruk testordninger i et meningsfullt omfang, vil de i tillegg gå glipp av de potensielle fordelene med en testramme, for eksempel å påvise IKT-sårbarheter og IKT-risikoer, og å teste forsvarskapasitet og kontinuitet i virksomheten, hvilket bidrar til å øke tilliten til kunder, leverandører

---

[11] Europaparlaments- og rådsforordning (EU) 2019/881 av 17. april 2019 om ENISA (Den europeiske unions byrå for cybersikkerhet), om cybersikkerhetssertifisering av informasjons- og kommunikasjonsteknologi, og om oppheving av forordning (EU) nr. 526/2013 (cybersikkerhetsforordningen) (EUT L 151 av 7.6.2019, s. 15).

[12] Europaparlaments- og rådsdirektiv (EU) 2015/2366 av 25. november 2015 om betalingstjenester i det indre marked, om endring av direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om oppheving av direktiv 2007/64/EF (EUT L 337 av 23.12.2015, s. 35).

og forretningspartnere. For å utbedre disse overlappingene, forskjellene og hullene er det nødvendig å fastsette regler om koordinering av testordningen og dermed legge til rette for gjensidig anerkjennelse av avanserte tester for finansielle enheter som oppfyller kriteriene i denne forordningen.

27) Finansielle enheters avhengighet av bruken av IKT-tjenester skyldes delvis deres behov for å tilpasse seg en framvoksende konkurransedyktig digital global økonomi, for å effektivisere sin virksomhet og for å imøtekomme forbrukernes etterspørsel. Arten og omfanget av en slik avhengighet har utviklet seg kontinuerlig de siste årene, noe som har bidratt til kostnadsreduksjoner innen finansformidling, muliggjort utvidelse og skalerbarhet av virksomheter i forbindelse med utrullingen av finansielle aktiviteter, og samtidig gitt tilgang til et bredt spekter av IKT-verktøyer for å håndtere komplekse interne prosesser.

28) Den omfattende bruken av IKT-tjenester framgår av komplekse kontraktsregulerte ordninger, der finansielle enheter ofte støter på vanskeligheter med å forhandle om kontraktsvilkår som er tilpasset til de tilsynsstandardene eller andre forskriftsmessige krav som de er omfattet av, eller på annen måte med å håndheve særskilte rettigheter, som for eksempel tilgangs- eller revisjonsrettigheter, selv når sistnevnte er fastsatt i deres kontraktsregulerte ordninger. Mange av disse kontraktsregulerte ordningene inneholder dessuten ikke tilstrekkelige garantier som muliggjør en fullstendig overvåking av utkontrakteringsprosesser, hvilket gjør at den finansielle enheten ikke har mulighet til å vurdere disse risikoene. Ettersom tredjepartsleverandører av IKT-tjenester ofte leverer standardiserte tjenester til ulike typer kunder, kan det dessuten hende at slike kontraktsregulerte ordninger ikke alltid tilgodeser de individuelle eller spesifikke behovene til aktører i finansnæringen.

29) Selv om unionsregelverket for finansielle tjenester inneholder visse generelle regler om utkontraktering, er overvåkingen av den kontraktsregulerte dimensjonen ikke fullt ut forankret i unionsretten. I mangel av klare og skreddersydde EU-standarder som får anvendelse på de kontraktsregulerte ordningene som er inngått med tredjepartsleverandører av IKT-tjenester, er det ikke på en fyllestgjørende måte tatt høyde for den eksterne kilden til IKT-risiko. Derfor er det nødvendig å fastsette visse sentrale prinsipper for å veilede finansielle enheters styring av IKT-tredjepartsrisiko, som er av særlig betydning når finansielle enheter benytter tredjepartsleverandører av IKT-tjenester for å støtte kritiske eller viktige funksjoner. Disse prinsippene bør ledsages av et sett av grunnleggende kontraktfestede rettigheter når det gjelder flere aspekter av gjennomføring og oppsigelse av kontraktsregulerte ordninger, med henblikk på å yte visse minstegarantier for å styrke de finansielle enhetenes evne til effektivt å overvåke alle IKT-risikoer som oppstår hos tredjepartsleverandører av tjenester. Disse prinsippene utfyller den sektorspesifikke lovgivningen som får anvendelse på utkontraktering.

30) I dag er det tydelig at det er en viss mangel på homogenitet og tilnærming når det gjelder overvåking av IKT-tredjepartsrisiko og avhengighet av IKT-tredjeparter. Til tross for innsatsen for å håndtere utkontraktering, som for eksempel EBAs retningslinjer for utkontraktering fra 2019 og ESMAs retningslinjer for utkontraktering til leverandører av skytjenester fra 2021, tas det i unionsretten ikke i tilstrekkelig grad høyde for det bredere spørsmålet om å motvirke systemrisiko som kan utløses av finanssektorens eksponering mot et begrenset antall av kritiske tredjepartsleverandører av IKT-tjenester. Mangelen på regler på unionsplan forsterkes av mangelen på nasjonale regler om mandater og verktøyer som gjør det mulig for finansielle tilsynsmyndigheter å oppnå en god forståelse for avhengighet av IKT-tredjeparter, og foreta en tilstrekkelig overvåking av risikoer som oppstår som følge av konsentrasjoner av avhengighet av IKT-tredjeparter.

31) Med hensyn til den potensielle systemrisikoen som følger av økt bruk av utkontraktering og konsentrasjon av IKT-tredjeparter, og tatt i betraktning de utilstrekkelige nasjonale ordningene med hensyn til å gi finansielle tilsynsmyndigheter tilstrekkelige verktøyer for å kvantifisere, kvalifisere og avhjelpe konsekvensene av IKT-risiko, som oppstår hos kritiske tredjepartsleverandører av IKT-tjenester, er det nødvendig å fastsette et hensiktsmessig overvåkingsrammeverk som gjør det mulig å foreta løpende overvåking av aktivitetene hos tredjepartsleverandører av IKT-tjenester, som er kritiske tredjepartsleverandører av IKT-tjenester til finansielle enheter,

samtidig som det sikres at fortroligheten og sikkerheten for andre kunder enn finansielle enheter, bevares. Selv om konsernintern levering av IKT-tjenester innebærer spesifikke risikoer og fordeler, bør den ikke automatisk anses som mindre risikabel enn levering av IKT-tjenester fra leverandører utenfor et finanskonsern, og den bør derfor være omfattet av samme regelverk. Når IKT-tjenester leveres innenfor samme finanskonsern, kan imidlertid finansielle enheter ha en høyere grad av kontroll over konserninterne leverandører, noe som bør tas hensyn til i den samlede risikovurderingen.

32) Med IKT-risiko som blir stadig mer komplisert og sofistikert, er gode tiltak for påvisning og forebygging av IKT-risiko i høy grad avhengig av regelmessig utveksling av etterretninger om trusler og sårbarheter mellom finansielle enheter. Utveksling av opplysninger bidrar til å skape økt bevissthet om cybertrusler. Dette styrker også finansielle enheters evne til å forhindre at cybertrusler blir til virkelige IKT-relaterte hendelser, og det setter finansielle enheter i stand til å begrense virkningen av IKT-relaterte hendelser mer effektivt og til å hente seg inn raskere. I fravær av veiledning på unionsplan synes flere faktorer å ha hindret en slik utveksling av etterretninger, særlig usikkerhet omkring forenligheten med regler om vern av personopplysninger, antitrust og ansvar.

33) I tillegg fører tvil om hvilke typer opplysninger som kan utveksles med andre markedsdeltakere, eller med myndigheter som ikke er tilsynsmyndigheter (som for eksempel ENISA, med henblikk på analytisk underlag, eller Europol, med henblikk på rettshåndheving), til at nyttige opplysninger holdes tilbake. Derfor er omfanget av og kvaliteten på utveksling av opplysninger for tiden fortsatt begrenset og fragmentert, med relevante utvekslinger som for det meste er lokale (gjennom nasjonale initiativ), og ingen enhetlige ordninger for utveksling av opplysninger på unionsplan som er tilpasset behovene til et integrert finanssystem. Derfor er det viktig å styrke disse kommunikasjonskanalene.

34) Finansielle enheter bør derfor oppfordres til å utveksle opplysninger og etterretninger om cybertrusler seg imellom, og til å utnytte i fellesskap individuell kunnskap og praktisk erfaring på strategisk, taktisk og operasjonelt nivå med sikte på å styrke sin kapasitet til i tilstrekkelig grad å vurdere, overvåke, forsvare seg mot og reagere på cybertrusler, gjennom å delta i ordninger for utveksling av opplysninger. Derfor er det nødvendig å gjøre det mulig å opprette frivillige ordninger for utveksling av opplysninger på unionsplan som, når de gjennomføres i pålitelige miljøer, vil hjelpe finansnæringen med å forebygge og reagere i fellesskap på cybertrusler ved raskt å begrense spredningen av IKT-risiko og hindre potensiell smitte gjennom de finansielle kanalene. Disse ordningene bør være i samsvar med gjeldende konkurranseregler i Unionen som fastsatt i kommisjonsmelding av 14. januar 2011 med tittelen «Retningslinjer for anvendelsen av artikkel 101 i traktaten om Den europeiske unions virkemåte på horisontale samarbeidsavtaler», samt med Unionens personvernregler, særlig europaparlaments- og rådsforordning (EU) 2016/679[13]. De bør fungere på grunnlag av et eller flere av de rettsgrunnlagene som er fastsatt i artikkel 6 i den nevnte forordningen, som for eksempel i forbindelse med behandlingen av personopplysninger som er nødvendige for at den dataansvarlige eller en tredjepart kan forfølge en rettmessig interesse i henhold til artikkel 6 nr. 1 bokstav f) i den nevnte forordningen, samt i forbindelse med den behandlingen av personopplysninger som er nødvendig for å oppfylle en rettslig forpliktelse, som påhviler den dataansvarlige, og som er nødvendig for å utføre en oppgave i allmennhetens interesse, eller som et ledd i den dataansvarliges utøvelse av myndighet i henhold til henholdsvis artikkel 6 nr. 1 bokstav c) og e) i den nevnte forordningen.

35) For å opprettholde et høyt nivå av digital operasjonell motstandsdyktighet i hele finanssektoren og samtidig holde tritt med den teknologiske utviklingen bør denne forordningen styre de risikoene som stammer fra alle typer av IKT-tjenester. Med henblikk på dette bør definisjonen av IKT-tjenester i forbindelse med denne forordningen forstås bredt og omfatte digitale tjenester og datatjenester som fortløpende leveres gjennom IKT-systemer, til en eller flere interne eller

[13] Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) (EUT L 119 av 4.5.2016, s. 1).

eksterne brukere. Denne definisjonen bør for eksempel omfatte såkalte «over the top»-tjenester, som faller inn under kategorien elektroniske kommunikasjonstjenester. Den bør bare utelukke den begrensede kategorien av tradisjonelle analoge telefontjenester som kan betegnes som det offentlige telefonnettet («Public Switched Telephone Network» (PSTN)), tjenester innen faste nett, konvensjonelle telefontjenester («Plain Old Telephone Service» (POTS)) eller telefonitjenester innen faste nett.

36) Til tross for den brede dekningen som er fastsatt i denne forordningen, bør det ved anvendelse av reglene om digital operasjonell motstandsdyktighet tas hensyn til de vesentlige forskjellene mellom finansielle enheter når det gjelder deres størrelse og generelle risikoprofil. Som et generelt prinsipp bør finansielle enheter, når de fordeler ressurser og kapasitet for å gjennomføre rammeverket for IKT-risikostyring, på behørig vis veie sine IKT-relaterte behov opp mot sin størrelse og generelle risikoprofil, og arten, omfanget og kompleksiteten av sine tjenester, aktiviteter og drift, mens vedkommende myndigheter bør fortsette å vurdere og gjennomgå tilnærmingen til en slik fordeling.

37) Ytere av kontoopplysningstjenester som nevnt i artikkel 33 nr. 1 i direktiv (EU) 2015/2366 er uttrykkelig omfattet av virkeområdet for denne forordningen, samtidig som det tas hensyn til den spesifikke arten av deres virksomhet og de risikoene som den gir opphav til. Dessuten er e-pengeforetak og betalingsinstitusjoner som er unntatt i henhold til artikkel 9 nr. 1 i europaparlaments- og rådsdirektiv 2009/110/EF[14] og artikkel 32 nr. 1 i direktiv (EU) 2015/2366, omfattet av denne forordningen, selv om de ikke har fått tillatelse i samsvar med direktiv 2009/110/EF til å utstede elektroniske penger, eller dersom de ikke har fått tillatelse i samsvar med direktiv (EU) 2015/2366 til å yte og utføre betalingstjenester. Postgirokontorer som omhandlet i artikkel 2 nr. 5 punkt 3) i europaparlaments- og rådsdirektiv 2013/36/EU[15] er imidlertid unntatt fra denne forordningens virkeområde. Den vedkommende myndigheten for betalingsinstitusjoner som er unntatt i henhold til direktiv (EU) 2015/2366, e-pengeforetak som er unntatt i henhold til direktiv 2009/110/EF, og ytere av kontoopplysningstjenester som omhandlet i artikkel 33 nr. 1 i direktiv (EU) 2015/2366, bør være den vedkommende myndigheten som er utpekt i samsvar med artikkel 22 i direktiv (EU) 2015/2366.

38) Ettersom større finansielle enheter kan ha tilgang til flere ressurser og raskt kan avsette midler til å utvikle styringsstrukturer og innføre ulike foretaksstrategier, er det bare finansielle enheter som ikke er svært små bedrifter i henhold til denne forordningen, som skal pålegges å innføre mer komplekse styringsordninger. Framfor alt er slike enheter bedre rustet til å innføre egne styringsfunksjoner for å føre tilsyn med ordninger med tredjepartsleverandører av IKT-tjenester eller for å ivareta krisehåndtering, organisere sin IKT-risikostyring i henhold til modellen med tre forsvarslinjer eller for å innføre en intern modell for risikostyring og kontroll og underkaste sitt rammeverk for IKT-risikostyring internrevisjon.

39) Noen finansielle enheter drar nytte av unntak eller er underlagt et svært begrenset regelverk i henhold til relevant sektorspesifikk unionsrett. Slike finansielle enheter omfatter forvaltere av alternative investeringsfond som nevnt i artikkel 3 nr. 2 i europaparlaments- og rådsdirektiv 2011/61/EU[16], forsikrings- og gjenforsikringsforetak som nevnt i artikkel 4 i europaparlaments- og rådsdirektiv 2009/138/EF[17] og tjenestepensjonsforetak som forvalter pensjonsordninger som til sammen ikke har mer enn 15 medlemmer. I lys av disse unntakene ville det ikke være rimelig å ta med slike finansielle enheter i denne forordningens virkeområde. Dessuten anerkjenner denne forordningen de særtrekkene som gjør seg gjeldende for mar-

[14] Europaparlaments- og rådsdirektiv 2009/110/EU av 16. september 2009 om adgang til å starte og utøve virksomhet som e-pengeforetak og om tilsyn med slik virksomhet, om endring av direktiv 2005/60/EF og 2006/48/EF og om oppheving av direktiv 2000/46/EF (EUT L 267 av 10.10.2009, s. 7).

[15] Europaparlaments- og rådsdirektiv 2013/36/EU av 26. juni 2013 om adgang til å utøve virksomhet som kredittinstitusjon og om tilsyn med kredittinstitusjoner, om endring av direktiv 2002/87/EF og om oppheving av direktiv 2006/48/EF og 2006/49/EF (EUT L 176 av 27.6.2013, s. 338).

[16] Europaparlaments- og rådsdirektiv 2011/61/EU av 8. juni 2011 om forvaltere av alternative investeringsfond og om endring av direktiv 2003/41/EF og 2009/65/EF og forordning (EF) nr. 1060/2009 og (EU) nr. 1095/2010 (EUT L 174 av 1.7.2011, s. 1).

[17] Europaparlaments- og rådsdirektiv 2009/138/EF av 25. november 2009 om adgang til å starte og utøve virksomhet innen forsikring og gjenforsikring (Solvens II) (EUT L 335 av 17.12.2009, s. 1).

kedsstrukturen for forsikringsformidling, med det resultatet at forsikringsformidlere, gjenforsikringsformidlere og forsikringsformidlere som har forsikringsformidling som tilleggsvirksomhet, og som kan regnes som svært små bedrifter eller som små eller mellomstore bedrifter, ikke bør være omfattet av denne forordningen.

40) Ettersom de enhetene som er nevnt i artikkel 2 nr. 5 punkt 4)–23) i direktiv 2013/36/EU, er unntatt fra det nevnte direktivets virkeområde, bør medlemsstatene derfor kunne velge å unnta slike enheter som befinner seg på deres respektive territorier, fra denne forordningens anvendelse.

41) For å tilpasse denne forordningen til virkeområdet for europaparlaments- og rådsdirektiv 2014/65/EU[18] er det også hensiktsmessig å unnta fysiske og juridiske personer som er nevnt i artikkel 2 og 3 i det nevnte direktivet, og som har lov til å levere investeringstjenester uten å måtte innhente tillatelse i henhold til direktiv 2014/65/EU, fra virkeområdet for denne forordningen. I henhold til artikkel 2 i direktiv 2014/65/EU er enheter som anses som finansielle enheter i henhold til denne forordningen, som for eksempel verdipapirsentraler, innretninger for kollektive investeringer eller forsikrings- og gjenforsikringsforetak, imidlertid også unntatt fra dette direktivets virkeområde. Unntak fra denne forordningens virkeområde for personer og enheter nevnt i artikkel 2 og 3 i det nevnte direktivet bør ikke omfatte disse verdipapirsentralene, innretningene for kollektive investeringer eller forsikrings- og gjenforsikringsforetakene.

42) I henhold til sektorspesifikk unionsrett er enkelte finansielle enheter underlagt forenklede krav eller unntak av årsaker knyttet til deres størrelse eller de tjenestene de leverer. Denne kategorien av finansielle enheter omfatter små verdipapirforetak uten innbyrdes forbindelser, små tjenestepensjonsforetak som kan unntas fra virkeområdet for direktiv (EU) 2016/2341 på vilkårene fastsatt av den berørte medlemsstaten i artikkel 5 i det nevnte direktivet, og som forvalter pensjonsordninger som til sammen ikke har mer enn 100 medlemmer, samt institusjoner som er unntatt i henhold til direktiv 2013/36/EU. I samsvar med forholdsmessighetsprinsippet og for å bevare ånden i den sektorspesifikke unionsretten er det derfor også hensiktsmessig å underlegge disse finansielle enhetene et forenklet rammeverk for IKT-risikostyring i henhold til denne forordningen. Den forholdsmessige karakteren av rammeverket for IKT-risikostyring som omfatter disse finansielle enhetene, bør ikke endres av de tekniske reguleringsstandardene som skal utarbeides av de europeiske tilsynsmyndighetene. I samsvar med forholdsmessighetsprinsippet er det dessuten hensiktsmessig også å underlegge betalingsinstitusjoner omhandlet i artikkel 32 nr. 1 i direktiv (EU) 2015/2366 og e-pengeforetak omhandlet i artikkel 9 i direktiv 2009/110/EF som er unntatt i samsvar med nasjonal rett, som innarbeider disse unionsrettsaktene, et forenklet rammeverk for IKT-risikostyring i henhold til denne forordningen, mens betalingsinstitusjoner og e-pengeforetak som ikke er unntatt i samsvar med sin respektive nasjonale rett, som innarbeider sektorspesifikk unionsrett, bør overholde det generelle rammeverket fastsatt i denne forordningen.

43) På samme måte bør finansielle enheter som anses som svært små bedrifter, eller som er underlagt det forenklede rammeverket for IKT-risikostyring i henhold til denne forordningen, ikke være forpliktet til å opprette en funksjon for å overvåke de ordningene som de har inngått med tredjepartsleverandører av IKT-tjenester om bruk av IKT-tjenester; eller til å utpeke et medlem av den øverste ledelsen som skal være ansvarlig for å føre tilsyn med den tilhørende risikoeksponeringen og relevant dokumentasjon; til å overføre ansvaret for å styre og overvåke IKT-risiko til en kontrollfunksjon og sikre et passende nivå av uavhengighet for den kontrollfunksjonen for å unngå interessekonflikter; til å dokumentere og gjennomgå minst én gang i året rammeverket for IKT-risikostyring; til regelmessig å underlegge rammeverket for IKT-risikostyring internrevisjon; til å foreta grundige vurderinger etter store endringer i deres infrastruktur og prosesser for nettverk og informasjon; til regelmessig å foreta risikoanalyser av eldre IKT-systemer; til å underkaste gjennomføringen av planer for IKT-respons og -gjenoppretting uavhengig internrevisjon; til å ha en krisestyringsfunksjon, til å

[18] Europaparlaments- og rådsdirektiv 2014/65/EU av 15. mai 2014 om markeder for finansielle instrumenter og om endring av direktiv 2002/92/EF og direktiv 2011/61/EU (EUT L 173 av 12.6.2014, s. 349).

utvide testingen av kontinuitet i virksomheten og respons- og gjenopprettingsplaner for å fange opp scenarioer med overflytting mellom den primære IKT-infrastrukturen og redundante anlegg; til å innberette til vedkommende myndigheter, på deres anmodning, et overslag over samlede årlige kostnader og tap forårsaket av alvorlige IKT-relaterte hendelser, til å opprettholde redundant IKT-kapasitet; til å informere nasjonale vedkommende myndigheter om gjennomførte endringer etter gjennomgåelsen av IKT-relaterte hendelser; til fortløpende å overvåke relevant teknologisk utvikling, til å etablere et omfattende program for testing av digital operasjonell motstandsdyktighet som en integrert del av det rammeverket for IKT-risikostyring som er fastsatt i denne forordningen, eller til å vedta og regelmessig gjennomgå en strategi for IKT-tredjepartsrisiko. I tillegg bør svært små bedrifter bare være forpliktet til å vurdere behovet for å opprettholde slik redundant IKT-kapasitet på grunnlag av hvilken risikoprofil de har. Svært små bedrifter bør dra nytte av en mer fleksibel ordning når det gjelder programmer for testing av digital operasjonell motstandsdyktighet. Når de overveier hvilken type og hyppighet av testing som skal utføres, bør de på en passende måte skape balanse mellom målet om å opprettholde en høy digital operasjonell motstandsdyktighet, de tilgjengelige ressursene og sin generelle risikoprofil. Svært små bedrifter og finansielle enheter som er underlagt det forenklede rammeverket for IKT-risikostyring i henhold til denne forordningen, bør unntas fra kravet om å utføre avansert testing av IKT-verktøyer, IKT-systemer og IKT-prosesser på grunnlag av trusselbasert penetrasjonstesting (TLPT), ettersom bare finansielle enheter som oppfyller kriteriene fastsatt i denne forordningen, bør være forpliktet til å utføre slik testing. På bakgrunn av sin begrensede kapasitet bør svært små bedrifter kunne bli enige med tredjepartsleverandøren av IKT-tjenester om å delegere den finansielle enhetens rett til tilgang, inspeksjon og revisjon til en uavhengig tredjepart, som skal utpekes av tredjepartsleverandøren av IKT-tjenester, forutsatt at den finansielle enheten når som helst kan anmode den respektive uavhengige tredjeparten om alle relevante opplysninger og garantier når det gjelder de resultatene som tredjepartsleverandøren av IKT-tjenester oppnår.

44) Ettersom bare de finansielle enhetene som er utpekt med henblikk på avansert testing av digital motstandsdyktighet, bør være forpliktet til å utføre trusselbaserte penetrasjonstester, bør de administrative prosessene og de finansielle kostnadene som er forbundet med gjennomføringen av slike tester, overføres til en liten prosentdel av finansielle enheter.

45) For å sikre full tilpasning av og overordnet sammenheng mellom de finansielle enhetenes forretningsstrategier på den ene side og gjennomføringen av IKT-risikostyring på den annen side, bør de finansielle enhetenes ledelsesorganer være forpliktet til å ha en sentral og aktiv rolle i styringen og tilpasningen av rammeverket for IKT-risikostyring og den samlede strategien for digital operasjonell motstandsdyktighet. Ledelsesorganenes strategi bør ikke bare fokusere på hvordan IKT-systemenes motstandsdyktighet sikres, men bør også omfatte mennesker og prosesser gjennom et sett av retningslinjer som, på hvert foretaksnivå og for alle ansatte, fremmer en sterk følelse av bevissthet om cyberrisikoer og et tilsagn om å overholde en streng cyberhygiene på alle nivåer. Ledelsesorganets endelige ansvar for å styre en finansiell enhets IKT-risiko bør være et overordnet prinsipp for denne helhetlige strategien og omsettes i et fortløpende engasjement hos ledelsesorganet for å kontrollere overvåkingen av IKT-risikostyringen.

46) Dessuten går prinsippet om ledelsesorganets fulle og endelige ansvar for styringen av den finansielle enhetens IKT-risiko hånd i hånd med behovet for å sikre et nivå av IKT-relaterte investeringer og et samlet budsjett for den finansielle enheten som vil gjøre det mulig for den finansielle enheten å oppnå et høyt nivå av digital operasjonell motstandsdyktighet.

47) Med inspirasjon fra relevant beste praksis og relevante retningslinjer, anbefalinger og strategier på internasjonalt og nasjonalt plan samt på sektorplan når det gjelder styring av cyberrisiko, fremmer denne forordningen et sett av prinsipper som letter den overordnede strukturen for IKT-risikostyring. Så lenge finansielle enheters hovedsakelige kapasitet oppfyller de ulike funksjonene for IKT-risikostyring (identifisering, beskyttelse og forebygging, påvisning, respons og gjenoppretting, læring og utvikling samt kommunikasjon) som er fastsatt i denne forordningen,

bør finansielle enheter stå fritt til å bruke modeller for IKT-risikostyring som er utformet eller kategorisert på en annen måte.

48) For å holde tritt med et cybertrusselbilde som er i utvikling, bør finansielle enheter opprettholde oppdaterte IKT-systemer som er pålitelige og egnede til ikke bare å garantere den databehandlingen som er nødvendig for deres tjenester, men også for å sikre tilstrekkelig teknologisk motstandsdyktighet, slik at de i tilstrekkelig grad kan håndtere ytterligere behandlingsrelaterte behov på grunn av stressede markedsforhold eller andre vanskelige situasjoner.

49) Effektive planer for kontinuitet i virksomheten og gjenopprettingsplaner er nødvendige for at finansielle enheter omgående og raskt kan finne en løsning på IKT-relaterte hendelser, særlig cyberangrep, gjennom å begrense skaden og prioritere gjenopptakelse av aktiviteter og tiltak for gjenoppretting i samsvar med sine beredskapsplaner. En slik gjenopptakelse bør imidlertid på ingen måte sette integriteten og sikkerheten i nettverks- og informasjonssystemene eller dataenes tilgjengelighet, autentisitet, integritet eller fortrolighet i fare.

50) Selv om denne forordningen gir finansielle enheter mulighet til å fastsette sine mål for gjenopprettingstid og gjenopprettingspunkt på en fleksibel måte og dermed fullt ut ta hensyn til de relevante funksjonenes egenskaper og kritiske verdi og til eventuelle spesifikke forretningsmessige behov, bør den likevel kreve at de foretar en vurdering av den eventuelle samlede innvirkningen på markedseffektiviteten når slike mål fastsettes.

51) Bakmennene bak cyberangrep har en tendens til å søke å oppnå økonomiske gevinster direkte fra kilden og dermed utsette finansielle enheter for vesentlige konsekvenser. For å forhindre at IKT-systemer mister integritet eller blir utilgjengelige, og dermed unngå datainnbrudd og skade på fysisk IKT-infrastruktur, bør finansielle enheters rapportering av alvorlige IKT-relaterte hendelser forbedres betydelig og forenkles. Rapportering av IKT-relaterte hendelser bør harmoniseres gjennom å innføre et krav om at alle finansielle enheter skal rapportere direkte til sine berørte vedkommende myndigheter. Dersom en finansiell enhet er underlagt tilsyn av mer enn én nasjonal vedkommende myndighet, bør medlemsstatene utpeke én enkelt vedkommende myndighet som mottaker av slik rapportering. Kredittinstitusjoner som er klassifisert som betydelige i samsvar med artikkel 6 nr. 4 i rådsforordning (EU) nr. 1024/2013[19], skal legge fram slik rapportering for de nasjonale vedkommende myndighetene, og disse bør deretter oversende rapporten til Den europeiske sentralbank (ESB).

52) Direkte rapportering bør gjøre det mulig for finansielle tilsynsmyndigheter å få umiddelbar tilgang til opplysninger om alvorlige IKT-relaterte hendelser. Finansielle tilsynsmyndigheter bør i sin tur videreformidle opplysninger om alvorlige IKT-relaterte hendelser til offentlige myndigheter som ikke er finansielle myndigheter (som for eksempel vedkommende myndigheter og felles kontaktpunkter i henhold til direktiv (EU) 2022/2555, nasjonale personvernmyndigheter og rettshåndhevende myndigheter i forbindelse med alvorlige IKT-relaterte hendelser av kriminell karakter) for å øke disse myndighetenes bevissthet om slike hendelser og, når det gjelder CSIRT-enheter, for å fremme hurtig bistand, alt etter hva som er relevant. Medlemsstatene bør dessuten kunne bestemme at finansielle enheter selv bør gi slike opplysninger til offentlige myndigheter utenfor området for finansielle tjenester. Disse informasjonsstrømmene bør gi finansielle enheter mulighet til raskt å dra nytte av eventuelle relevante tekniske innspill, råd om avhjelpende tiltak og påfølgende oppfølgning fra slike myndigheter. Opplysninger om alvorlige IKT-relaterte hendelser bør sendes begge veier: Finansielle tilsynsmyndigheter bør gi alle nødvendige tilbakemeldinger eller veiledning til den finansielle enheten, mens de europeiske tilsynsmyndighetene bør dele anonymiserte opplysninger om cybertrusler og sårbarheter knyttet til en hendelse for å bidra til et bredere kollektivt forsvar.

53) Selv om det bør kreves at alle finansielle enheter rapporterer hendelser, forventes det at dette kravet ikke vil påvirke dem alle på samme måte. Relevante vesentlighetsterskler og rapporteringsfrister bør således behørig tilpasses gjennom delegerte rettsakter basert på de tekniske reguleringsstandardene som skal utarbeides av de europeiske tilsynsmyn-

[19] Rådsforordning (EU) nr. 1024/2013 av 15. oktober 2013 om tildeling av særskilte oppgaver til Den europeiske sentralbank i forbindelse med politikken for tilsyn med kredittinstitusjoner (EUT L 287 av 29.10.2013, s. 63).

dighetene, med henblikk på å dekke bare alvorlige IKT-relaterte hendelser. I tillegg bør det tas hensyn til de finansielle enhetenes særtrekk når det fastsettes tidsfrister for rapporteringsforpliktelser.

54) Denne forordningen bør fastsette et krav om at kredittinstitusjoner, betalingsinstitusjoner, ytere av kontoopplysningstjenester og e-pengeforetak skal rapportere alle betalingsrelaterte operasjonelle hendelser eller sikkerhetshendelser – som tidligere er rapportert i henhold til direktiv (EU) 2015/2366 – uavhengig av hendelsens IKT-karakter.

55) De europeiske tilsynsmyndighetene bør ha til oppgave å vurdere gjennomførbarheten og vilkårene for en mulig sentralisering av rapporter om IKT-relaterte hendelser på unionsplan. En slik sentralisering kan bestå av et felles EU-knutepunkt for rapportering av alvorlige IKT-relaterte hendelser, som enten direkte mottar de relevante rapportene og automatisk underretter nasjonale vedkommende myndigheter, eller som bare sentraliserer relevante rapporter fra de nasjonale vedkommende myndighetene, og dermed oppfyller en koordineringsrolle. De europeiske tilsynsmyndighetene bør ha til oppgave å utarbeide, i samråd med ESB og ENISA, en felles rapport som undersøker muligheten for å opprette et felles EU-knutepunkt.

56) For å oppnå et høyt nivå av digital operasjonell motstandsdyktighet, og i tråd med både de relevante internasjonale standardene (for eksempel G7 Fundamental Elements for Threat-Led Penetration Testing) og med de rammeverkene som anvendes i Unionen, som for eksempel TIBER-EU, bør finansielle enheter regelmessig teste sine IKT-systemer og ansatte som har IKT-relatert ansvar, med hensyn til hvor effektiv deres kapasitet er for forebygging, påvisning, respons og gjenoppretting, for å påvise og håndtere potensielle IKT-sårbarheter. For å gjenspeile de forskjellene som eksisterer på tvers av og innenfor de ulike finansielle delsektorene når det gjelder finansielle enheters nivå av cybersikkerhetsberedskap, bør testing omfatte et bredt spekter av verktøyer og tiltak, alt fra vurderingen av grunnleggende krav (for eksempel sårbarhetsvurderinger og -analyser, analyser av åpen kildekode, vurderinger av nettsikkerhet, mangelanalyser, fysiske sikkerhetsvurderinger, spørreskjemaer og programvareløsninger for skanning, gjennomgåelse av kildekoder dersom det er mulig, scenariobaserte tester, kompatibilitetstesting, ytelsestesting eller ende-til-ende-testing) til mer avansert testing ved hjelp av TLPT. Slike avanserte tester bør bare kreves av finansielle enheter som utfra et IKT-perspektiv er modne nok til å kunne gjennomføre dem på en rimelig måte. Den testingen av den digitale operasjonelle motstandsdyktigheten som kreves i henhold til denne forordningen, bør derfor være mer krevende for de finansielle enhetene som oppfyller kriteriene fastsatt i denne forordningen (for eksempel store, systemiske og IKT-modne kredittinstitusjoner, børser, verdipapirsentraler og sentrale motparter), enn for andre finansielle enheter. Samtidig bør testing av digital operasjonell motstandsdyktighet ved hjelp av TLPT være mer relevant for finansielle enheter som driver virksomhet innenfor sentrale delsektorer for finansielle tjenester, og som spiller en systemisk rolle (for eksempel betalinger, bankvirksomhet samt clearing og oppgjør), og mindre relevant for andre delsektorer (for eksempel kapitalforvaltere og kredittvurderingsbyråer).

57) Finansielle enheter som er involvert i virksomhet over landegrensene, og som utøver etableringsadgang eller tjenesteyting i Unionen, bør oppfylle et felles sett av krav til avansert testing (TLPT) i hjemstaten, som bør omfatte IKT-infrastrukturer i alle jurisdiksjoner der det grenseoverskridende finanskonsernet driver virksomhet i Unionen, hvilket innebærer at slike grenseoverskridende finanskonsern bare kan pådra seg relaterte IKT-testkostnader i én jurisdiksjon.

58) For å utnytte den ekspertisen som allerede er ervervet av visse vedkommende myndigheter, særlig med hensyn til gjennomføringen av TIBER-EU-rammeverket, bør denne forordningen gi medlemsstatene mulighet til å utpeke en felles offentlig myndighet som ansvarlig i finanssektoren på nasjonalt plan for alle TLPT-relaterte spørsmål eller, dersom ingen slik myndighet utpekes, å utpeke vedkommende myndigheter til å delegere utførelsen av TLPT-relaterte oppgaver til en annen nasjonal finansiell vedkommende myndighet.

59) Ettersom denne forordningen ikke krever at finansielle enheter skal dekke alle kritiske eller viktige funksjoner i én enkelt trusselbasert penetrasjonstest, bør finansielle enheter stå fritt til å bestemme hvilke og hvor mange kritiske eller viktige funksjoner som bør være omfattet av en slik test.

60) Samlet testing som definert i denne forordningen, som innebærer deltakelse av flere finansielle enheter i en TLPT, og for hvilke en tredjepartsleverandør av IKT-tjenester kan inngå kontraktsregulerte ordninger direkte med en ekstern tester, bør bare tillates dersom kvaliteten eller sikkerheten for de tjenestene som tredjepartsleverandør av IKT-tjenester leverer til kunder som er enheter som faller utenfor virkeområdet for denne forordningen, eller for fortroligheten for data som er knyttet til slike tjenester, med rimelighet kan forventes å bli negativt påvirket. Samlet testing bør også være omfattet av garantier (under ledelse av én utpekt finansiell enhet, kalibrering av antall deltakende finansielle enheter) for å sikre en streng testprosess for de involverte finansielle enhetene som oppfyller målene for TLPT i henhold til denne forordningen.

61) For å utnytte interne ressurser som er tilgjengelige på foretaksnivå, bør denne forordningen tillate bruk av interne testere for å utføre TLPT, forutsatt at tilsynsmyndigheten godkjenner det, at det ikke foreligger noen interessekonflikter, og at anvendelsen av interne og eksterne testere alternerer regelmessig (hver tredje test), samtidig som formidleren av trusseletterretninger i TLPT alltid skal være ekstern i forhold til den finansielle enheten. Ansvaret for å utføre en TLPT bør fullt ut ligge hos den finansielle enheten. Erklæringer fra myndighetene bør utelukkende ha til formål å sikre gjensidig anerkjennelse og bør ikke utelukke eventuelle oppfølgingstiltak som er nødvendige for å håndtere den IKT-risikoen som den finansielle enheten er eksponert for, og de bør heller ikke ses på som en tilsynsmessig godkjenning av en finansiell enhets kapasitet til å styre og begrense IKT-risiko.

62) For å sikre en forsvarlig overvåking av IKT-tredjepartsrisiko i finanssektoren er det nødvendig å fastsette en rekke prinsippbaserte regler for å veilede finansielle enheter når de overvåker risiko som oppstår i forbindelse med funksjoner som er utkontraktert til tredjepartsleverandører av IKT-tjenester, særlig for IKT-tjenester som støtter kritiske eller viktige funksjoner, samt mer generelt i forbindelse med avhengighet av IKT-tredjeparter.

63) For å håndtere kompleksiteten i de ulike kildene til IKT-risiko, samtidig som det tas hensyn til mangfoldet av leverandører av teknologiske løsninger som muliggjør en smidig levering av finansielle tjenester, bør denne forordningen omfatte et bredt spekter av tredjepartsleverandører av IKT-tjenester, herunder leverandører av skytjenester, programvare, dataanalysetjenester og leverandører av datasentertjenester. Ettersom finansielle enheter på en effektiv og sammenhengende måte bør identifisere og styre alle typer risiko, herunder i forbindelse med IKT-tjenester som anskaffes innenfor et finanskonsern, bør det likeledes presiseres at foretak som er en del av et finanskonsern og hovedsakelig leverer IKT-tjenester til morforetaket, eller til datterforetak eller filialer av morforetaket, samt finansielle enheter som leverer IKT-tjenester til andre finansielle enheter, også bør anses som tredjepartsleverandører av IKT-tjenester i henhold til denne forordningen. Endelig, på bakgrunn av at markedet for betalingstjenester i stadig større grad blir avhengig av komplekse tekniske løsninger, og med hensyn til nye typer betalingstjenester og betalingsrelaterte løsninger, bør deltakere i økosystemet for betalingstjenester som leverer betalingsbehandlingstjenester, eller som driver betalingsinfrastrukturer, også anses som tredjepartsleverandører av IKT-tjenester i henhold til denne forordningen, med unntak av sentralbanker når de driver betalings- eller verdipapiroppgjørssystemer, og offentlige myndigheter når de leverer IKT-relaterte tjenester i forbindelse med utførelsen av statlige funksjoner.

64) En finansiell enhet bør til enhver tid fortsatt være fullt ansvarlig for å overholde sine forpliktelser i henhold til denne forordningen. Finansielle enheter bør anvende en forholdsmessig tilnærming i forbindelse med overvåkingen av de risikoene som oppstår hos tredjepartsleverandører av IKT-tjenester, gjennom å ta behørig hensyn til karakteren på og omfanget av, kompleksiteten hos og betydningen av sin IKT-relaterte avhengighet, tjenestenes kritiske verdi eller betydningen av de prosessene eller funksjonene som er omfattet av de kontraktsregulerte ordningene, og, i siste instans, på grunnlag av en grundig vurdering av en eventuell potensiell innvirkning på kontinuiteten og kvaliteten til finansielle tjenester på individuelt nivå og på konsernnivå, alt etter hva som er relevant.

65) Gjennomføringen av en slik overvåking bør følge en strategisk tilnærming til IKT-tredjepartsrisiko som formaliseres ved at den finansielle enhetens ledelsesorgan vedtar en sær-

lig strategi for IKT-tredjepartsrisiko, som tar utgangspunkt i en løpende screening av all avhengighet av IKT-tredjeparter. For å øke tilsynsmyndighetens bevissthet om avhengighet av IKT-tredjeparter og ytterligere støtte arbeidet i forbindelse med overvåkingsrammeverket som fastsatt i henhold til denne forordningen, bør alle finansielle enheter være forpliktet til å føre et register over opplysninger om alle kontraktsregulerte ordninger som gjelder bruken av IKT-tjenester levert av tredjepartsleverandører av IKT-tjenester. Finansielle tilsynsmyndigheter bør kunne anmode om tilgang til hele registret eller be om bestemte avsnitt av registeret, og dermed innhente vesentlige opplysninger for å få en bredere forståelse av finansielle enheters IKT-avhengighet.

66) En grundig analyse før kontraktinngåelse bør underbygge og gå forut for den formelle inngåelsen av kontraktsregulerte ordninger, særlig gjennom å fokusere på elementer som kritisk verdi eller betydningen av de tjenestene som støttes av den påtenkte IKT-kontrakten, de nødvendige tilsynsgodkjenningene eller andre forhold, den mulige konsentrasjonsrisikoen som følger med, samt å anvende tilbørlig aktsomhet i prosessen med utvelgelse og vurdering av tredjepartsleverandører av IKT-tjenester og vurdering av potensielle interessekonflikter. I forbindelse med kontraktsregulerte ordninger som gjelder kritiske eller viktige funksjoner, bør finansielle enheter ta hensyn hvorvidt tredjepartsleverandører av IKT-tjenester bruker de nyeste og høyeste standardene om informasjonssikkerhet. Oppsigelse av kontraktsregulerte ordninger kan som et minimum være forårsaket av en rekke omstendigheter som viser mangler hos tredjepartsleverandøren av IKT-tjenester, særlig vesentlige overtredelser av lover eller kontraktsvilkår, omstendigheter som avslører en potensiell endring i utførelsen av de funksjonene som er fastsatt i kontraktsregulerte ordninger, tegn på svakheter hos tredjepartsleverandøren av IKT-tjenester i den samlede IKT-risikostyringen eller omstendigheter som tyder på at den berørte vedkommende myndigheten ikke er i stand til å føre effektivt tilsyn med den finansielle enheten.

67) For å håndtere den systemiske virkningen av den konsentrasjonsrisikoen som er forbundet med IKT-tredjeparter, fremmer denne forordningen en balansert løsning ved hjelp av en fleksibel og gradvis tilnærming til en slik konsentrasjonsrisiko, ettersom innføringen av strenge tak eller strenge begrensninger kan hindre utøvelsen av virksomhet og begrense kontraktsfriheten. Finansielle enheter bør foreta en grundig vurdering av sine påtenkte kontraktsregulerte ordninger for å fastslå sannsynligheten for at en slik risiko oppstår, herunder ved hjelp av inngående analyser av underleverandøravtaler, særlig når de inngås med tredjepartsleverandører av IKT-tjenester som er etablert i et tredjeland. På det nåværende tidspunktet, og med henblikk på å finne en rimelig balanse mellom nødvendigheten av å bevare kontraktsfriheten og å sikre den finansielle stabiliteten, anses det ikke som hensiktsmessig å fastsette regler om strenge tak og strenge begrensninger for eksponeringer mot IKT-tredjeparter. I forbindelse med overvåkingsrammeverket bør en hovedovervåker som er utpekt i henhold til denne forordningen, med hensyn til kritiske tredjepartsleverandører av IKT-tjenester, være særlig oppmerksom på å oppnå full forståelse for omfanget av gjensidig avhengighet, påvise særlige tilfeller der en høy grad av konsentrasjon av kritiske tredjepartsleverandører av IKT-tjenester i Unionen sannsynligvis vil legge press på stabiliteten og integriteten i Unionens finanssystem, og opprettholde en dialog med kritiske tredjepartsleverandører av IKT-tjenester der denne spesifikke risikoen er identifisert.

68) For regelmessig å vurdere og overvåke hvorvidt en tredjepartsleverandør av IKT-tjenester har evnen til å levere tjenester på en sikker måte til en finansiell enhet, og uten at dette har negative virkninger på en finansiell enhets digitale operasjonelle motstandsdyktighet, bør flere viktige kontraktsmessige elementer med tredjepartsleverandører av IKT-tjenester harmoniseres. En slik harmonisering bør omfatte minst de områdene som er svært viktige for at den finansielle enheten skal kunne gjennomføre en fullstendig overvåking av de risikoene som kan oppstå gjennom tredjepartsleverandøren av IKT-tjenester, sett i lys av en finansiell enhets behov for å sikre sin digitale motstandsdyktighet ettersom den er helt avhengig av de mottatte IKT-tjenestenes stabilitet, funksjonalitet, tilgjengelighet og sikkerhet.

69) Når finansielle enheter og tredjepartsleverandører av IKT-tjenester reforhandler kontraktsregulerte ordninger med henblikk på oppnå samsvar med kravene i denne forord-

ningen, bør de sikre at de viktige kontraktsbestemmelsene som er fastsatt i denne forordningen, er omfattet.

70) Definisjonen av «kritisk eller viktig funksjon» i denne forordningen omfatter de «kritiske funksjonene» som er definert i artikkel 2 nr. 1 punkt 35) i europaparlaments- og rådsdirektiv 2014/59/EU[20]. Funksjoner som anses som kritiske i henhold til direktiv 2014/59/EU, er derfor tatt med i definisjonen av kritiske funksjoner i henhold til denne forordningen.

71) Uavhengig av hvor kritisk eller viktig den funksjonen som støttes av IKT-tjenestene, er, bør kontraktsregulerte ordninger særlig inneholde en spesifikasjon av de fullstendige beskrivelsene av funksjoner og tjenester, av stedene der slike funksjoner leveres, og hvor dataene skal behandles, samt beskrivelser av tjenestenivå. Andre grunnleggende elementer for å muliggjøre en finansiell enhets overvåking av IKT-tredjepartsrisiko er kontraktsbestemmelser som spesifiserer hvordan adgang, tilgjengelighet, integritet, sikkerhet og vern av personopplysninger sikres av tredjepartsleverandøren av IKT-tjenester, bestemmelser som fastsetter de relevante garantiene for å muliggjøre tilgang til, gjenoppretting og tilbakeføring av data ved insolvens, krisehåndtering eller opphør av virksomheten til tredjepartsleverandøren av IKT-tjenester, samt bestemmelser som krever at tredjepartsleverandøren av IKT-tjenester skal yte bistand i tilfelle av IKT-hendelser i forbindelse med tjenestene som leveres, uten ekstra kostnad eller til en kostnad som er fastsatt på forhånd, bestemmelser om forpliktelsen for tredjepartsleverandøren av IKT-tjenester til å samarbeide fullt ut med vedkommende myndigheter og krisehåndteringsmyndigheter i den finansielle enheten og bestemmelser om oppsigelsesrett og tilhørende minste oppsigelsesfrist for kontraktsregulerte ordninger i samsvar med forventningene til vedkommende myndigheter og krisehåndteringsmyndigheter.

72) I tillegg til slike kontraktsbestemmelser, og med henblikk på å sikre at finansielle enheter fortsatt har full kontroll over all utvikling som skjer på tredjepartsnivå, og som kan svekke deres IKT-sikkerhet, bør kontraktene om levering av IKT-tjenester som støtter kritiske eller viktige funksjoner, også inneholde bestemmelser om følgende: En fullstendig beskrivelse av tjenestenivået, med nøyaktige kvantitative og kvalitative ytelsesmål, for å muliggjøre uten unødig forsinkelse egnede korrigerende tiltak dersom de avtalte tjenestenivåene ikke overholdes, relevante oppsigelsesfrister og rapporteringsforpliktelser for tredjepartsleverandøren av IKT-tjenester for hendelser som kan ha en vesentlig innvirkning på hvorvidt tredjepartsleverandøren av IKT-tjenester har evnen til å levere de respektive IKT-tjenestene på en effektiv måte, et krav om at tredjepartsleverandøren av IKT-tjenester skal gjennomføre og teste beredskapsplaner for virksomheten og innføre IKT-sikkerhetstiltak, IKT-verktøyer og IKT-retningslinjer som muliggjør sikker levering av tjenester, samt delta og samarbeide fullt ut i den TLPT-en som utføres av den finansielle enheten.

73) Kontrakter om levering av IKT-tjenester som støtter kritiske eller viktige funksjoner, bør også inneholde bestemmelser som gir den finansielle enheten, eller en utpekt tredjepart, rett til tilgang, inspeksjon og revisjon, og rett til å ta kopier som avgjørende verktøyer i de finansielle enhetenes løpende overvåking av de resultatene som tredjepartsleverandøren av IKT-tjenester oppnår, kombinert med sistnevntes fulle samarbeid i forbindelse med inspeksjonene. Tilsvarende bør den finansielle enhetens vedkommende myndighet ha rett til, som følge av varsler, å inspisere og foreta revisjon av tredjepartsleverandøren av IKT-tjenester, med forbehold om vern av fortrolige opplysninger.

74) Slike kontraktsregulerte ordninger bør også inneholde særskilte exit-strategier som særlig muliggjør obligatoriske overgangsperioder der tredjepartsleverandører av IKT-tjenester bør fortsette å levere de relevante tjenestene med henblikk på å redusere risikoen for forstyrrelser i den finansielle enheten, eller for å gi sistnevnte mulighet til å bytte til andre tredjepartsleverandører av IKT-tjenester på en effektiv måte, eller alternativt bytte til interne løsninger som er forenlige med den leverte IKT-tjenestens kompleksitet. Finansielle enheter som er omfattet av direktiv 2014/59/EU, bør dessuten sikre

[20] Europaparlaments- og rådsdirektiv 2014/59/EU av 15. mai 2014 om fastsettelse av en ramme for gjenoppretting og krisehåndtering av kredittinstitusjoner og verdipapirforetak og om endring av rådsdirektiv 82/891/EØF, europaparlaments- og rådsdirektiv 2001/24/EF, 2002/47/EF, 2004/25/EF, 2005/56/EF, 2007/36/EF, 2011/35/EU, 2012/30/EU og 2013/36/EU og europaparlaments- og rådsforordning (EU) nr. 1093/2010 og (EU) nr. 648/2012 (EUT L 173 av 12.6.2014, s. 190).

at de relevante kontraktene for IKT-tjenester er robuste og kan håndheves fullt ut ved krisehåndtering av disse finansielle enhetene. I samsvar med krisehåndteringsmyndighetenes forventninger bør disse finansielle enhetene derfor sikre at de relevante kontraktene for IKT-tjenester er motstandsdyktige mot krisehåndtering. Så lenge disse finansielle enhetene fortsetter å oppfylle sine betalingsforpliktelser, bør de blant annet sikre at de relevante kontraktene for IKT-tjenester inneholder bestemmelser om at de ikke kan sies opp, ikke kan oppheves midlertidig og ikke kan endres på grunn av omstrukturering eller krisehåndtering.

75) Videre kan frivillig bruk av standardavtalevilkår som offentlige myndigheter eller Unionens institusjoner har utarbeidet, særlig bruken av kontraktsvilkår som Kommisjonen har utarbeidet for skytjenester, gi de finansielle enhetene og tredjepartsleverandørene av IKT-tjenester mer trygghet gjennom å øke rettssikkerheten når det gjelder bruken av skytjenester i finanssektoren, i fullt samsvar med de kravene og forventningene som er fastsatt i unionsregelverket for finansielle tjenester. Utarbeidingen av standardavtalevilkår bygger på tiltak som allerede var planlagt i handlingsplanen for FinTech fra 2018, som kunngjorde Kommisjonens hensikt om å fremme og tilrettelegge for utarbeidingen av standardavtalevilkår for finansielle enheters utkontraktering av skytjenester, basert på den tverrsektorielle innsatsen fra berørte parter på området for skytjenester, som Kommisjonen har bidratt til med deltakelse fra finanssektoren.

76) For å fremme tilnærming og effektivitet med hensyn til tilsynsstrategier når det gjelder styring av IKT-tredjepartsrisiko i finanssektoren, samt for å styrke den digitale operasjonelle motstandsdyktigheten i finansielle enheter som er avhengige av kritiske tredjepartsleverandører av IKT-tjenester for levering av IKT-tjenester som støtter leveringen av finansielle tjenester, og dermed bidra til å bevare stabiliteten i Unionens finanssystem og integriteten på det indre marked for finansielle tjenester, bør kritiske tredjepartsleverandører av IKT-tjenester være underlagt Unionens overvåkingsrammeverk. Selv om opprettelsen av overvåkingsrammeverket er begrunnet i merverdien av å treffe tiltak på unionsplan og av de særlige forholdene som gjør seg gjeldende for bruken av IKT-tjenester, og den rollen de spiller i forbindelse med levering av finansielle tjenester, bør det samtidig bemerkes at denne løsningen virker å være egnet bare innenfor rammen av denne forordningen som spesifikt omhandler digital operasjonell motstandsdyktighet i finanssektoren. Et slikt overvåkingsrammeverk bør imidlertid ikke anses som en ny modell for Unionens tilsyn på andre områder av finansielle tjenester og finansiell virksomhet.

77) Overvåkingsrammeverket bør bare få anvendelse på kritiske tredjepartsleverandører av IKT-tjenester. Det bør derfor være en utpekingsordning som tar hensyn til omfanget og arten av finanssektorens avhengighet av slike tredjepartsleverandører av IKT-tjenester. Denne ordningen bør innebære et sett av kvantitative og kvalitative kriterier for å fastsette parametrer for kritisk verdi som grunnlag for inkludering i overvåkingsrammeverket. For å sikre at denne vurderingen er nøyaktig, og uavhengig av foretaksstrukturen til tredjepartsleverandøren av IKT-tjenester, bør slike kriterier, når det gjelder en tredjepartsleverandør av IKT-tjenester som er en del av et større konsern, ta hensyn til hele konsernstrukturen hos tredjepartsleverandøren av IKT-tjenester. På den ene side bør kritiske tredjepartsleverandører av IKT-tjenester som ikke automatisk utpekes i henhold til disse kriteriene, ha mulighet til å delta i overvåkingsrammeverket på frivillig basis, men på den annen side bør tredjepartsleverandører av IKT-tjenester som allerede er omfattet av overvåkingsrammer som støtter utførelsen av oppgavene til Det europeiske system av sentralbanker som nevnt i artikkel 127 nr. 2 i TEUV, unntas.

78) På samme måte bør finansielle enheter som leverer IKT-tjenester til andre finansielle enheter, selv om de tilhører kategorien av tredjepartsleverandører av IKT-tjenester i henhold til denne forordningen, også unntas fra overvåkingsrammeverket ettersom de allerede er omfattet av tilsynsordninger som er opprettet gjennom det relevante unionsregelverket for finansielle tjenester. Dersom det er relevant, bør vedkommende myndigheter i forbindelse med sin tilsynsvirksomhet ta hensyn til den IKT-risikoen som finansielle enheter som leverer IKT-tjenester, utgjør for finansielle enheter. På samme måte bør det på grunn av de eksisterende ordningene for risikooovervåking på konsernnivå innføres samme unntak for tredjepartsleverandører av

IKT-tjenester som leverer tjenester hovedsakelig til enheter i sitt egen konsern. Tredjepartsleverandører av IKT-tjenester som utelukkende leverer IKT-tjenester i én medlemsstat til finansielle enheter som bare er aktive i denne medlemsstaten, bør også unntas fra utpekingsordningen på grunn av sin begrensede virksomhet og manglende innvirkning over landegrensene.

79) Den digitale omstillingen av finansielle tjenester har ført til et helt enestående nivå når det gjelder bruk og avhengighet av IKT-tjenester. Ettersom det er blitt utenkelig å levere finansielle tjenester uten bruk av skytjenester, programvareløsninger og datarelaterte tjenester, har Unionens finansielle økosystem blitt uløselig forbundet med visse IKT-tjenester som leveres av tredjepartsleverandører av IKT-tjenester. Noen av disse leverandørene er innovatører når det gjelder å utvikle og anvende IKT-basert teknologi, og spiller en viktig rolle i leveringen av finansielle tjenester eller er blitt integrert i verdikjeden for finansielle tjenester. De er dermed blitt avgjørende for stabiliteten og integriteten i Unionens finanssystem. Denne utbredte avhengigheten av tjenester levert av kritiske tredjepartsleverandører av IKT-tjenester, i kombinasjon med den gjensidige avhengigheten mellom informasjonssystemene til ulike markedsoperatører, skaper en direkte og potensielt alvorlig risiko for Unionens system for finansielle tjenester og for kontinuiteten i leveringen av finansielle tjenester dersom kritiske tredjepartsleverandører av IKT-tjenester skulle bli påvirket av driftsforstyrrelser eller alvorlige cyberhendelser. Cyberhendelser har en særegen evne til å formere seg og spre seg i hele finanssystemet i et betydelig raskere tempo enn andre typer risikoer som overvåkes i finanssektoren, og kan strekke seg over sektorer og utover geografiske grenser. De har potensial til å utvikle seg til en systemisk krise der tilliten til finanssystemet uthules på grunn av forstyrrelser av funksjoner som støtter realøkonomien, eller på grunn av betydelige finansielle tap som når et nivå som finanssystemet ikke kan klare, eller som krever omfattende tiltak for å absorbere kraftige sjokk. For å hindre at disse scenarioene inntreffer og dermed setter Unionens finansielle stabilitet og integritet i fare, er det viktig å sikre tilnærming av tilsynspraksis for IKT-tredjepartsrisiko i finanssektoren, særlig gjennom nye regler som gjør det mulig for Unionen å ha oversyn med kritiske tredjepartsleverandører av IKT-tjenester.

80) Overvåkingsrammeverket avhenger for en stor del av graden av samarbeid mellom hovedovervåkeren og den kritiske tredjepartsleverandøren av IKT-tjenester som leverer tjenester til finansielle enheter, som påvirker leveransen av finansielle tjenester. Vellykket overvåking er blant annet basert på hovedovervåkerens evne til effektivt å gjennomføre overvåkingsoppdrag og inspeksjoner for å vurdere de reglene, kontrollene og prosessene som brukes av de kritiske tredjepartsleverandørene av IKT-tjenester, samt å vurdere den potensielle kumulative virkningen av deres aktiviteter på den finansielle stabiliteten og finanssystemets integritet. Samtidig er det svært viktig at kritiske tredjepartsleverandører av IKT-tjenester følger hovedovervåkerens anbefalinger og imøtekommer dennes betenkeligheter. Ettersom manglende samarbeid fra en kritisk tredjepartsleverandør av IKT-tjenester som leverer tjenester som påvirker leveringen av finansielle tjenester, som for eksempel avslag på å gi tilgang til sine lokaler eller å sende inn opplysninger, til slutt vil frata hovedovervåkeren dens viktige verktøyer for å vurdere IKT-tredjepartsrisiko og kan ha en negativ innvirkning på finanssystemets finansielle stabilitet og integritet, er det også nødvendig å innføre en passende sanksjonsordning.

81) På denne bakgrunn bør hovedovervåkerens behov for å ilegge overtredelsesgebyr for å tvinge kritiske tredjepartsleverandører av IKT-tjenester til å oppfylle forpliktelsene om åpenhet og tilgang som fastsatt i denne forordningen, ikke trues av vanskeligheter som oppstår som følge av håndhevingen av disse overtredelsesgebyrene i forbindelse med kritiske tredjepartsleverandører av IKT-tjenester som er etablert i tredjeland. For å sikre at slike sanksjoner kan håndheves, og for å muliggjøre en rask innføring av framgangsmåter som opprettholder retten til forsvar for de kritiske tredjepartsleverandørene av IKT-tjenester i forbindelse med utpekingsordningen og utstedelsen av anbefalinger, bør det kreves at disse kritiske tredjepartsleverandørene av IKT-tjenester som leverer tjenester til finansielle enheter, som påvirker leveringen av finansielle tjenester, skal være forpliktet til å opprettholde en tilstrekkelig virksomhet i Unionen. På grunn av tilsynets karakter og man-

gelen på sammenlignbare ordninger i andre jurisdiksjoner finnes det ingen egnede alternative ordninger for å nå dette målet gjennom et effektivt samarbeid med finansielle tilsynsmyndigheter i tredjeland om overvåkingen av virkninger av de digitale operasjonelle risikoene som systemviktige tredjepartsleverandører av IKT-tjenester, som anses som kritiske tredjepartsleverandører av IKT-tjenester etablert i tredjeland, utgjør. For å fortsette å levere IKT-tjenester til finansielle enheter i Unionen bør derfor en tredjepartsleverandør av IKT-tjenester som er etablert i et tredjeland, og som er utpekt som kritisk i samsvar med denne forordningen, senest tolv måneder etter utpekingen, treffe alle nødvendige tiltak for å sikre sin registrering som foretak i Unionen gjennom å opprette et datterforetak som definert i gjeldende unionsregelverk, nærmere bestemt i europaparlaments- og rådsdirektiv 2013/34/EU[21].

82) Kravet om å opprette et datterforetak i Unionen bør ikke hindre den kritiske tredjepartsleverandøren av IKT-tjenester fra å levere IKT-tjenester og tilhørende teknisk støtte fra anlegg og infrastruktur som ligger utenfor Unionen. Denne forordningen innfører ikke noen plikt om datalokalisering ettersom den ikke krever at datalagring eller databehandling skal finne sted i Unionen.

83) Kritiske tredjepartsleverandører av IKT-tjenester bør kunne tilby IKT-tjenester fra hvor som helst i verden, ikke nødvendigvis eller ikke bare fra lokaler i Unionen. Tilsynsvirksomheten bør først gjennomføres i lokaler som ligger i Unionen, og gjennom samhandling med enheter lokalisert i Unionen, herunder datterforetak etablert av kritiske tredjepartsleverandører av IKT-tjenester i henhold til denne forordningen. Slike tiltak i Unionen kan imidlertid være utilstrekkelige for at hovedovervåkeren fullt ut og på en effektiv måte skal kunne utføre sine oppgaver i henhold til denne forordningen. Hovedovervåkeren bør derfor også kunne utøve sin relevante myndighet i tredjeland. Utøvelsen av denne myndigheten i tredjeland bør gjøre det mulig for hovedovervåkeren å undersøke de fasilitetene fra hvilke IKT-tjenestene eller de tekniske supporttjenestene faktisk leveres eller forvaltes av den kritiske tredjepartsleverandøren av IKT-tjenester, og bør gi hovedovervåkeren omfattende og operasjonell forståelse av IKT-risikostyringen hos den kritiske tredjepartsleverandøren av IKT-tjenester. Hovedovervåkerens mulighet, i egenskap av unionsbyrå, til å utøve myndighet utenfor Unionens territorium bør være behørig avgrenset av relevante vilkår, særlig samtykke fra den berørte kritiske tredjepartsleverandøren av IKT-tjenester. På samme måte bør de berørte myndighetene i tredjelandet underrettes om, og ikke ha innvendinger mot, at hovedovervåkerens virksomhet utøves på tredjelandets eget territorium. For å sikre en effektiv gjennomføring, og uten at det berører den respektive myndigheten til Unionens institusjoner og medlemsstatene, må imidlertid slik myndighet også være fullt forankret i inngåelsen av ordninger om administrativt samarbeid med de berørte myndighetene i det berørte tredjelandet. Denne forordningen bør derfor gjøre det mulig for de europeiske tilsynsmyndighetene å inngå ordninger om administrativt samarbeid med de berørte myndighetene i tredjeland som ikke på annen måte bør skape rettslige forpliktelser for Unionen og dens medlemsstater.

84) For å lette kommunikasjonen med hovedovervåkeren og for å sikre tilstrekkelig representasjon, bør kritiske tredjepartsleverandører av IKT-tjenester som er en del av et konsern, utpeke en juridisk person som sitt koordineringspunkt.

85) Overvåkingsrammeverket bør ikke berøre medlemsstatenes myndighet til å gjennomføre sine egne overvåkings- eller monitoreringsoppdrag med hensyn til tredjepartsleverandører av IKT-tjenester som ikke er utpekt som kritiske i henhold til denne forordningen, men som anses som viktige på nasjonalt plan.

86) For å utnytte den institusjonelle flerlagsarkitekturen på området finansielle tjenester bør Felleskomiteen for de europeiske tilsynsmyndighetene fortsette å sikre en samlet koordinering på tvers av sektorer i alle spørsmål som gjelder IKT-risiko, i samsvar med sine oppgaver når det gjelder cybersikkerhet. Dette arbeidet bør støttes av en ny underkomité («overvåkingssforumet») som utfører forberedende arbeid både for de enkelte beslutningene rettet til kritiske tredjepartsleverandører av IKT-tjenester, og for utste-

[21] Europaparlaments- og rådsdirektiv 2013/34/EU av 26. juni 2013 om årsregnskaper, konsernregnskaper og tilhørende rapporter for visse typer foretak, om endring av europaparlaments- og rådsdirektiv 2006/43/EF og om oppheving av rådsdirektiv 78/660/EØF og 83/349/EØF (EUT L 182 av 29.6.2013, s. 19).

delse av kollektive anbefalinger, særlig i forbindelse med referansemåling av overvåkingsprogrammene for kritiske tredjepartsleverandører av IKT-tjenester, og identifisering av beste praksis for håndtering av spørsmål om IKT-konsentrasjonsrisiko.

87) For å sikre at kritiske tredjepartsleverandører av IKT-tjenester overvåkes på en hensiktsmessig og effektiv måte på unionsplan, fastsetter denne forordningen at hver og en av de tre europeiske tilsynsmyndighetene kan utpekes som hovedovervåker. Den individuelle tildelingen av en kritisk tredjepartsleverandør av IKT-tjenester til en av de tre europeiske tilsynsmyndighetene bør være et resultat av en vurdering av den overveiende andelen av finansielle enheter som driver virksomhet i finanssektorene, som den europeiske tilsynsmyndigheten har ansvaret for. Denne tilnærmingen bør føre til en balansert fordeling av oppgaver og ansvar mellom de tre europeiske tilsynsmyndighetene i forbindelse med utøvelsen av overvåkingsfunksjonene og bør på beste måte utnytte de menneskelige ressursene og den tekniske ekspertisen som finnes i hver av de tre europeiske tilsynsmyndighetene.

88) Hovedovervåkere bør tildeles nødvendig myndighet til å foreta undersøkelser, gjennomføre stedlige inspeksjoner og eksterne inspeksjoner i lokaler og på driftssteder hos kritiske tredjepartsleverandører av IKT-tjenester samt å innhente fullstendige og oppdaterte opplysninger. Denne myndigheten bør gjøre det mulig for hovedovervåkeren å få reell innsikt i typen, omfanget og virkningen av IKT-tredjepartsrisikoen for finansielle enheter og til syvende og sist for Unionens finanssystem. Å gi de europeiske tilsynsmyndighetene den ledende overvåkerrollen er en forutsetning for å forstå og håndtere den systemiske dimensjonen av IKT-risiko i finanssektoren. Den innvirkningen som kritiske tredjepartsleverandører av IKT-tjenester har på Unionens finanssektor, og de potensielle problemene som skyldes den derav følgende IKT-konsentrasjonsrisikoen, krever en kollektiv tilnærming på unionsplan. Samtidig gjennomføring av flere revisjoner og tilgangsrettigheter som utføres separat av mange vedkommende myndigheter med liten eller ingen innbyrdes koordinering, vil forhindre finansielle tilsynsmyndigheter i å få en fullstendig og omfattende oversikt over IKT-tredjepartsrisiko i Unionen, samtidig som det innebærer redundans, byrde og kompleksitet for kritiske tredjepartsleverandører av IKT-tjenester, dersom de er gjenstand for mange anmodninger om overvåking og inspeksjon.

89) Ettersom utpekingen som kritisk har en betydelig innvirkning, bør denne forordningen sikre at rettighetene til kritiske tredjepartsleverandører av IKT-tjenester overholdes gjennom hele gjennomføringen av overvåkingsrammeverket. Før slike leverandører utpekes som kritiske, bør de for eksempel ha rett til å sende en begrunnet uttalelse til hovedovervåkeren som inneholder alle opplysninger som er relevante for den vurderingen som gjelder utpekingen. Ettersom hovedovervåkeren bør ha myndighet til å legge fram anbefalinger om spørsmål som gjelder IKT-risiko og egnede tiltak for håndtering av disse, som omfatter myndigheten til å motsette seg visse kontraktsregulerte ordninger som i siste instans påvirker stabiliteten til den finansielle enheten eller finanssystemet, bør kritiske tredjepartsleverandører av IKT-tjenester også gis mulighet til, før disse anbefalingene ferdigstilles, å gi forklaringer på hvilken innvirkning de foreslåtte løsningene i anbefalingene forventes å ha på kunder som er enheter som faller utenfor virkeområdet for denne forordningen, og til å utarbeide løsninger for å begrense risikoene. Kritiske tredjepartsleverandører av IKT-tjenester som er uenige med anbefalingene, bør sende inn en begrunnet redegjørelse for sin hensikt om ikke å slutte seg til anbefalingen. Dersom en slik begrunnet redegjørelse ikke sendes inn, eller dersom den anses å være utilstrekkelig, bør hovedovervåkeren sende ut en kunngjøring som kort beskriver problemet med manglende overholdelse.

90) De vedkommende myndighetene bør på behørig vis la oppgaven med å kontrollere at anbefalinger fra hovedovervåkeren faktisk overholdes, inngå i deres oppdrag med hensyn til tilsyn med finansielle enheter. De vedkommende myndighetene bør kunne kreve at finansielle enheter treffer ytterligere tiltak for å styre de risikoene som er identifisert i hovedovervåkerens anbefalinger, og bør i god tid utstede meldinger om dette. Dersom hovedovervåkeren retter anbefalinger til kritiske tredjepartsleverandører av IKT-tjenester som er underlagt tilsyn i henhold til direktiv (EU) 2022/2555, bør de vedkommende myndighetene, på frivillig grunnlag og før de vedtar ytterligere tiltak, kunne høre de vedkommende myndighetene i henhold til det

nevnte direktivet for å fremme en koordinert strategi for håndtering av de aktuelle kritiske tredjepartsleverandørene av IKT-tjenester.

91) Utøvelsen av overvåkingen bør styres av tre operasjonelle prinsipper som har til formål å sikre a) tett koordinering mellom de europeiske tilsynsmyndighetene i deres roller som hovedovervåker gjennom et felles overvåkingsnettverk, b) samsvar med det rammeverket som er fastsatt i henhold til direktiv (EU) 2022/2555 (gjennom en frivillig høring av organer i henhold til det nevnte direktivet for å unngå overlapping av tiltak rettet mot kritiske tredjepartsleverandører av IKT-tjenester), og c) aktsomhet for å minimere den potensielle risikoen for forstyrrelser i tjenester levert av kritiske tredjepartsleverandører av IKT-tjenester til kunder som er enheter som faller utenfor virkeområdet for denne forordningen.

92) Overvåkingsrammeverket bør ikke erstatte eller på noen måte eller i noen del anvendes i stedet for kravet om at finansielle enheter selv skal styre de risikoene som følger av anvendelsen av tredjepartsleverandører av IKT-tjenester, herunder deres forpliktelse til å opprettholde en løpende overvåking av kontraktsregulerte ordninger som er inngått med kritiske tredjepartsleverandører av IKT-tjenester. Overvåkingsrammeverket bør heller ikke berøre de finansielle enhetenes fulle ansvar for å overholde og oppfylle alle rettslige forpliktelser fastsatt i denne forordningen og i det relevante regelverket for finansielle tjenester.

93) For å unngå dobbeltbestemmelser og overlappinger bør vedkommende myndigheter avstå fra å treffe individuelle tiltak som tar sikte på å overvåke risiko hos den kritiske tredjepartsleverandøren av IKT-tjenester, og bør i den forbindelse stole på den relevante hovedovervåkerens vurdering. Alle tiltak bør under alle omstendigheter koordineres og avtales på forhånd med hovedovervåkeren som ledd i utførelsen av oppgaver innenfor overvåkingsrammeverket.

94) For å fremme tilnærming på internasjonalt plan når det gjelder anvendelse av beste praksis for gjennomgåelse og overvåking av den digitale risikostyringen som foretas av tredjepartsleverandører av IKT-tjenester, bør de europeiske tilsynsmyndighetene oppfordres til å inngå samarbeidsordninger med relevante tilsyns- og reguleringsmyndigheter i tredjeland.

95) For å utnytte den spesifikke kompetansen, de tekniske ferdighetene og ekspertisen til personale som spesialiserer seg på operasjonell risiko og IKT-risiko hos de vedkommende myndighetene, de tre europeiske tilsynsmyndighetene og, på frivillig grunnlag, de vedkommende myndighetene i henhold til direktiv (EU) 2022/2555, bør hovedovervåkeren benytte seg av nasjonal tilsynskapasitet og -kunnskap og opprette særskilte granskningsgrupper for hver kritisk tredjepartsleverandør av IKT-tjenester, for å samle tverrfaglige grupper til støtte for utarbeiding og gjennomføring av overvåkingsvirksomhet, herunder generelle undersøkelser og inspeksjoner av kritiske tredjepartsleverandører av IKT-tjenester, samt for eventuell nødvendig oppfølging av dem.

96) Mens kostnader som oppstår som følge av overvåkingsoppgaver vil bli fullt ut finansiert av avgifter pålagt kritiske tredjepartsleverandører av IKT-tjenester, er det imidlertid sannsynlig at de europeiske tilsynsmyndighetene vil pådra seg, før overvåkingsrammeverket får anvendelse, kostnader for gjennomføring av særskilte IKT-systemer som støtter den kommende overvåkingen, ettersom særskilte IKT-systemer må utvikles og innføres på forhånd. Denne forordningen inneholder bestemmelser om en hybrid finansieringsmodell, der overvåkingsrammeverket som sådan vil være fullt ut finansiert gjennom avgifter, mens utviklingen av de europeiske tilsynsmyndighetenes IKT-systemer vil bli finansiert gjennom bidrag fra Unionen og de nasjonale vedkommende myndighetene.

97) De vedkommende myndighetene bør ha all nødvendig tilsyns-, undersøkelses- og sanksjonsmyndighet for å sikre at de utøver sine oppgaver i henhold til denne forordningen. De bør i prinsippet offentliggjøre kunngjøringer om de administrative sanksjonene de pålegger. Ettersom finansielle enheter og tredjepartsleverandører av IKT-tjenester kan etableres i ulike medlemsstater og overvåkes av ulike vedkommende myndigheter, bør anvendelsen av denne forordningen lettes ved på den ene side et nært samarbeid mellom berørte vedkommende myndigheter, herunder Den europeiske sentralbank, med hensyn til særlige oppgaver som den er tildelt i henhold til rådsforordning (EU) nr. 1024/2013, og ved på den annen side høring av de europeiske tilsynsmyndighetene gjennom gjensidig utveksling av opplysninger og leve-

ring av bistand i forbindelse med den relevante tilsynsvirksomheten.

98) For ytterligere å kvantifisere og kvalifisere kriteriene for utpeking av tredjepartsleverandører av IKT-tjenester som kritiske og for å harmonisere overvåkingsavgiftene bør myndigheten til å vedta rettsakter i samsvar med artikkel 290 i TEUV delegeres til Kommisjonen for å utfylle denne forordningen med nærmere spesifisering av den systemiske virkningen som en svikt eller en driftsstans hos en tredjepartsleverandør av IKT-tjenester skulle kunne få på de finansielle enhetene som den leverer IKT-tjenester til, antall globale systemviktige institusjoner eller andre systemviktige institusjoner som er avhengige av den aktuelle tredjepartsleverandøren av IKT-tjenester, antall tredjepartsleverandører av IKT-tjenester som er aktive på et gitt marked, kostnadene ved å overføre data og IKT-arbeidsbelastningen til andre tredjepartsleverandører av IKT-tjenester, samt størrelsen på avgiftsbeløpene og hvordan de skal betales. Det er særlig viktig at Kommisjonen gjennomfører hensiktsmessige høringer under sitt forberedende arbeid, herunder på ekspertnivå, og at disse høringene gjennomføres i samsvar med prinsippene fastsatt i den tverrinstitusjonelle avtalen av 13. april 2016 om bedre regelverksutforming[22]. For å sikre lik deltakelse ved utarbeidingen av delegerte rettsakter er det særlig viktig at Europaparlamentet og Rådet mottar alle dokumenter samtidig som medlemsstatenes eksperter, og deres eksperter bør ha systematisk adgang til møter i Kommisjonens ekspertgrupper som er med på utarbeidingen av delegerte rettsakter.

99) Tekniske reguleringsstandarder bør sikre en ensartet harmonisering av kravene fastsatt i denne forordningen. De europeiske tilsynsmyndighetene bør i egenskap av organ med høyt spesialisert sakkunnskap derfor få i oppdrag å utarbeide utkast til tekniske reguleringsstandarder som ikke innebærer politiske valg, med sikte på framlegging for Kommisjonen. Det bør utvikles tekniske reguleringsstandarder på områdene IKT-risikostyring, rapportering av alvorlige IKT-relaterte hendelser, testing, samt i forbindelse med sentrale krav til en forsvarlig overvåking av IKT-tredjepartsrisiko. Kommisjonen og de europeiske tilsynsmyndighetene bør sikre at disse standardene og kravene kan anvendes av alle finansielle enheter på en måte som står i forhold til deres størrelse og generelle risikoprofil, samt til arten, omfanget og kompleksiteten av deres tjenester, aktiviteter og drift. Kommisjonen bør gis myndighet til å vedta slike tekniske reguleringsstandarder ved hjelp av delegerte rettsakter i henhold til artikkel 290 i TEUV og i samsvar med artikkel 10–14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

100) For å gjøre det lettere å sammenligne rapporter om alvorlige IKT-relaterte hendelser og alvorlige betalingsrelaterte operasjonelle hendelser eller sikkerhetshendelser, samt for å sikre åpenhet om kontraktsregulerte ordninger for bruk av IKT-tjenester som leveres av tredjepartsleverandører av IKT-tjenester, bør de europeiske tilsynsmyndighetene utarbeide utkast til tekniske gjennomføringsstandarder som fastsetter standardiserte maler, skjemaer og framgangsmåter, slik at finansielle enheter kan rapportere en alvorlig IKT-relatert hendelse og en alvorlig betalingsrelatert operasjonell hendelse eller sikkerhetshetshendelse, samt standardiserte maler for registrering av opplysninger. Når de europeiske tilsynsmyndighetene utarbeider disse standardene, bør de ta hensyn til den finansielle enhetens størrelse og generelle risikoprofil, samt til arten, omfanget og kompleksiteten av dens tjenester, aktiviteter og drift. Kommisjonen bør gis myndighet til å vedta slike tekniske gjennomføringsstandarder ved hjelp av en gjennomføringsrettsakt i henhold til artikkel 291 i TEUV og i samsvar med artikkel 15 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

101) Ettersom det allerede er fastsatt ytterligere krav gjennom delegerte rettsakter og gjennomføringsrettsakter basert på tekniske reguleringsstandarder og tekniske gjennomføringsstandarder i europaparlaments- og rådsforordning (EF) nr. 1060/2009[23], (EU) nr. 648/2012[24], (EU) nr. 600/2014[25] og (EU) nr. 909/2014[26], er det hensiktsmessig å gi de

[22] EUT L 123 av 12.5.2016, s. 1.

[23] Europaparlaments- og rådsforordning (EF) nr. 1060/2009 av 16. september 2009 om kredittvurderingsbyråer (EUT L 302 av 17.11.2009, s. 1).

[24] Europaparlaments- og rådsforordning (EU) nr. 648/2012 av 4. juli 2012 om OTC-derivater, sentrale motparter og transaksjonsregistre (EUT L 201 av 27.7.2012, s. 1).

[25] Europaparlaments- og rådsforordning (EU) nr. 600/2014 av 15. mai 2014 om markeder for finansielle instrumenter og om endring av forordning (EU) nr. 648/2012 (EUT L 173 av 12.6.2014, s. 84).

europeiske tilsynsmyndighetene mandat til, enten individuelt eller i fellesskap gjennom Felleskomiteen, å legge fram tekniske reguleringsstandarder og tekniske gjennomføringsstandarder for Kommisjonen for vedtakelse av delegerte rettsakter og gjennomføringsrettsakter om overføring og oppdatering av eksisterende regler om IKT-risikostyring.

102) Ettersom denne forordningen, sammen med europaparlaments- og rådsdirektiv (EU) 2022/2556[27], innebærer en konsolidering av bestemmelser om IKT-risikostyring i flere forordninger og direktiver i Unionens regelverk for finansielle tjenester, herunder forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 og (EU) nr. 909/2014, og europaparlaments- og rådsforordning (EU) 2016/1011[28], bør disse forordningene endres for å sikre fullt samsvar og tydeliggjøre at gjeldende IKT-risikorelaterte bestemmelser er fastsatt i denne forordningen.

103) Derfor bør virkeområdet for de relevante artiklene knyttet til operasjonell risiko, for hvilke delegerte rettsakter og gjennomføringsrettsakter skal vedtas i henhold til den myndigheten som er fastsatt i forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011, begrenses slik at alle bestemmelser som omfatter aspekter av digital operasjonell motstandsdyktighet, og som i dag inngår i disse forordningene, overføres til denne forordningen.

104) Den potensielle systemrisikoen på cyberområdet knyttet til bruken av IKT-infrastrukturer som muliggjør drift av betalingssystemer og levering av betalingsbehandlingstjenester, bør håndteres på behørig vis på unionsplan gjennom harmoniserte regler om digital motstandsdyktighet. Kommisjonen bør derfor raskt vurdere behovet for å gjennomgå virkeområdet for denne forordningen, samtidig som en slik gjennomgåelse tilpasses til resultatet av den omfattende gjennomgåelsen som er planlagt i henhold til direktiv (EU) 2015/2366. Mange storstilte angrep i løpet av det siste tiåret viser hvordan betalingssystemer er blitt utsatt for cybertrusler. Med en sentral plassering i betalingstjenestekjeden og sterke innbyrdes forbindelser til finanssystemet som en helhet har betalingssystemer og betalingsbehandlingstjenester fått en avgjørende betydning for finansmarkedenes virkemåte i Unionen. Cyberangrep på slike systemer kan forårsake alvorlige driftsforstyrrelser med direkte konsekvenser for viktige økonomiske funksjoner, som for eksempel tilrettelegging av betalinger og indirekte virkninger på relaterte økonomiske prosesser. Inntil det er innført en harmonisert ordning og tilsyn med operatører av betalingssystemer og behandlingsenheter på unionsplan, kan medlemsstatene, med sikte på å anvende en lignende markedspraksis, la seg inspirere av de kravene til digital operasjonell motstandsdyktighet som er fastsatt i denne forordningen, når de anvender regler på operatører av betalingssystemer og behandlingsenheter som er underlagt tilsyn i deres egne jurisdiksjoner.

105) Ettersom målet for denne forordningen, som er å oppnå et høyt nivå av digital operasjonell motstandsdyktighet for regulerte finansielle enheter, ikke kan nås i tilstrekkelig grad av medlemsstatene ettersom det krever harmonisering av flere ulike regler i unionsretten og nasjonal rett, og derfor på grunn av tiltakets omfang og virkninger bedre kan nås på unionsplan, kan Unionen treffe tiltak i samsvar med nærhetsprinsippet som fastsatt i artikkel 5 i traktaten om Den europeiske union. I samsvar med forholdsmessighetsprinsippet fastsatt i den nevnte artikkelen går denne forordningen ikke lenger enn det som er nødvendig for å nå dette målet.

106) EUs datatilsyn er blitt rådspurt i samsvar med artikkel 42 nr. 1 i europaparlaments- og rådsforordning (EU) 2018/1725[29] og avga uttalelse 10. mai 2021[30].

---

[26] Europaparlaments- og rådsforordning (EU) nr. 909/2014 av 23. juli 2014 om forbedring av verdipapiroppgjør 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 (EUT L 257 av 28.8.2014, s. 1).

[27] Europaparlaments- og rådsdirektiv (EU) 2022/256 av 14. desember 2022 om endring av direktiv 2009/65/EF, 2009/138/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 og (EU) 2016/2341 med hensyn til digital operasjonell motstandsdyktighet i finanssektoren (se EUT L 333 av 27.12.2022, s. 153).

[28] Europaparlaments- og rådsforordning (EU) 2016/1011 av 8. juni 2016 om indekser som brukes som referanseverdier for finansielle instrumenter og finansielle kontrakter eller for å måle investeringsfonds resultater, og om endring av direktiv 2008/48/EF og 2014/17/EU og forordning (EU) nr. 596/2014 (EUT L 171 av 29.6.2016, s. 1).

[29] Europaparlaments- og rådsforordning (EU) 2018/1725 av 23. oktober 2018 om vern av fysiske personer i forbindelse med behandling av personopplysninger i Unionens institusjoner, organer, kontorer og byråer og om fri utveksling av slike opplysninger samt om oppheving av forordning (EF) nr. 45/2001 og beslutning nr. 1247/2002/EF (EUT L 295 av 21.11.2018, s. 39).

[30] EUT C 229 av 15.6.2021, s. 16.

VEDTATT DENNE FORORDNINGEN:

Kapittel I

Alminnelige bestemmelser

Artikkel 1

Formål

1. For å oppnå et høyt felles nivå av digital operasjonell motstandsdyktighet fastsetter denne forordningen ensartede krav til sikkerheten i nettverks- og informasjonssystemer som støtter finansielle enheters forretningsprosesser på følgende måte:
   a) Krav som får anvendelse på finansielle enheter i forbindelse med
      i) risikostyring i forbindelse med informasjons- og kommunikasjonsteknologi (IKT),
      ii) rapportering av alvorlige IKT-relaterte hendelser og underretning på frivillig grunnlag om betydelige cybertrusler til de vedkommende myndighetene,
      iii) rapportering av alvorlige betalingsrelaterte operasjonelle hendelser eller sikkerhetshendelser til de vedkommende myndighetene fra finansielle enheter som nevnt i artikkel 2 nr. 1 bokstav a)–d),
      iv) testing av digital operasjonell motstandsdyktighet,
      v) utveksling av opplysninger og etterretninger i forbindelse med cybertrusler og sårbarheter,
      vi) tiltak for forsvarlig styring av IKT-tredjepartsrisiko.
   b) Krav i forbindelse med kontraktsregulerte ordninger inngått mellom tredjepartsleverandører av IKT-tjenester og finansielle enheter.
   c) Regler om opprettelse og gjennomføring av tilsynsrammen for kritiske tredjepartsleverandører av IKT-tjenester når de leverer tjenester til finansielle enheter.
   d) Krav om samarbeid mellom vedkommende myndigheter og regler om vedkommende myndigheters tilsyn og håndheving i forbindelse med alle forhold som er omfattet av denne forordningen.
2. Når det gjelder finansielle enheter som er identifisert som vesentlige eller viktige enheter i henhold til nasjonale regler som innarbeider artikkel 3 i direktiv (EU) 2022/2555, skal denne forordningen anses som en sektorspesifikk unionsrettsakt med hensyn til artikkel 4 i det nevnte direktivet.
3. Denne forordningen berører ikke medlemsstatenes ansvar for vesentlige statlige funksjoner som gjelder offentlig sikkerhet, forsvar og nasjonal sikkerhet i samsvar med unionsretten.

Artikkel 2

Virkeområde

1. Med forbehold for nr. 3 og 4 får denne forordningen anvendelse på følgende enheter:
   a) Kredittinstitusjoner
   b) Betalingsinstitusjoner, herunder betalingsinstitusjoner som er unntatt i henhold til direktiv (EU) 2015/2366.
   c) Ytere av kontoopplysningstjenester.
   d) E-pengeforetak, herunder e-pengeforetak som er unntatt i henhold til direktiv 2009/110/EF.
   e) Verdipapirforetak.
   f) Tilbydere av kryptoeiendeler som er meddelt tillatelse i henhold til europaparlaments- og rådsforordning om markeder for kryptoeiendeler, og om endring av forordning (EU) nr. 1093/2010 og (EU) nr. 1095/2010 og direktiv 2013/36/EU og (EU) 2019/1937 («forordningen om markeder for kryptoeiendeler») og utstedere av kryptoeiendeler,
   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 forsikringsformidlere som har forsikringsformidling som tilleggsvirksomhet.
   p) Tjenestepensjonsforetak.
   q) Kredittvurderingsbyråer.
   r) Administratorer av kritiske referanseverdier.
   s) Tilbydere av folkefinansieringstjenester.
   t) Verdipapiriseringsregistre.
   u) Tredjepartsleverandører av IKT-tjenester.
2. I denne forordningen skal enheter nevnt i nr. 1 bokstav a)–t) samlet kalles «finansielle enheter».

3. Denne forordningen får ikke anvendelse på
   a) forvaltere av alternative investeringsfond som nevnt i artikkel 3 nr. 2 i direktiv 2011/61/EF,
   b) forsikrings- og gjenforsikringsforetak som nevnt i artikkel 4 i direktiv 2009/138/EF,
   c) tjenestepensjonsforetak som forvalter pensjonsordninger som til sammen ikke har mer enn 15 medlemmer i alt,
   d) fysiske eller juridiske personer som er unntatt i henhold til artikkel 2 og 3 i direktiv 2014/65/EU,
   e) forsikringsformidlere, gjenforsikringsformidlere og forsikringsformidlere som har forsikringsformidling som tilleggsvirksomhet, som er svært små, små eller mellomstore bedrifter,
   f) postgirokontorer som nevnt i artikkel 2 nr. 5 punkt 3) i direktiv 2013/36/EU.
4. Medlemsstatene kan unnta enheter nevnt i artikkel 2 nr. 5 punkt 4)–23) i direktiv 2013/36/EU som befinner seg på deres respektive territorier, fra denne forordningens virkeområde. Dersom en medlemsstat gjør bruk av denne muligheten, skal den underrette Kommisjonen om dette og om eventuelle senere endringer. Kommisjonen skal offentliggjøre opplysningene på sitt nettsted eller på en annen lett tilgjengelig måte.

Artikkel 3

Definisjoner

I denne forordningen menes med

1) «digital operasjonell motstandsdyktighet» en finansiell enhets evne til å bygge opp, sikre og gjennomgå sin operasjonelle integritet og pålitelighet gjennom å sikre, enten direkte eller indirekte gjennom bruk av tjenester levert av tredjepartsleverandører av IKT-tjenester, hele spekteret av IKT-relatert kapasitet som er nødvendig for å håndtere sikkerheten i de nettverks- og informasjonssystemene som en finansiell enhet bruker, og som støtter fortløpende levering av finansielle tjenester og deres kvalitet, herunder i forbindelse med forstyrrelser,
2) «nettverks- og informasjonssystem» et nettverks- og informasjonssystem som definert i artikkel 6 punkt 1) i direktiv (EU) 2022/2555,
3) «eldre IKT-system» et IKT-system som har nådd slutten av sin livssyklus (end-of-life), og som av teknologiske eller kommersielle årsaker ikke er egnet til oppgraderinger eller utbedringer, eller som ikke lenger støttes av sin tredjepartsleverandør av IKT-tjenester, men som fortsatt er i bruk og støtter den finansielle enhetens funksjoner,
4) «sikkerhet i nettverks- og informasjonssystemer» sikkerhet i nettverks- og informasjonssystemer som definert i artikkel 6 punkt 2) i direktiv (EU) 2022/2555,
5) «IKT-risiko» enhver omstendighet som med rimelighet kan identifiseres i forbindelse med bruk av nettverks- og informasjonssystemer som, dersom den oppstår, kan svekke sikkerheten i nettverks- og informasjonssystemer, i verktøyer eller prosesser som er teknologiavhengige, i funksjoner og prosesser eller i forbindelse med levering av tjenester gjennom å skape negative virkninger i det digitale eller fysiske miljøet,
6) «informasjonsressurs» en samling av opplysninger, både materielle og immaterielle, som det er verdt å beskytte,
7) «IKT-ressurs» en programvare- eller maskinvareressurs i nettverks- og informasjonssystemene som brukes av den finansielle enheten,
8) «IKT-relatert hendelse» én enkelt hendelse eller en rekke tilknyttede hendelser som ikke er planlagt av den finansielle enheten, og som går ut over sikkerheten i nettverks- og informasjonssystemene, og har en negativ innvirkning på tilgjengeligheten, autentisiteten, integriteten eller fortroligheten til dataene eller på de tjenestene som leveres av den finansielle enheten,
9) «betalingsrelatert operasjonell hendelse eller sikkerhetshendelse» én enkelt hendelse eller en rekke tilknyttede hendelser som ikke er planlagt av de finansielle enhetene nevnt i artikkel 2 nr. 1 bokstav a)–d), uansett om de er IKT-relaterte eller ikke, og som har en negativ innvirkning på tilgjengeligheten, autentisiteten, integriteten eller fortroligheten til betalingsrelaterte opplysninger, eller på de betalingsrelaterte tjenestene som leveres av den finansielle enheten,
10) «alvorlig IKT-relatert hendelse» en IKT-relatert hendelse som har en stor negativ innvirkning på nettverks- og informasjonssystemene som støtter den finansielle enhetens kritiske eller viktige funksjoner,
11) «alvorlig betalingsrelatert operasjonell hendelse eller sikkerhetshendelse» en betalingsrelatert operasjonell hendelse eller sikkerhetshendelse som har stor negativ innvirkning på de betalingsrelaterte tjenestene som leveres,

12) «cybertrussel» cybertrussel som definert i artikkel 2 punkt 8) i forordning (EU) 2019/881,
13) «betydelig cybertrussel» en cybertrussel hvis tekniske egenskaper tilsier at den kan føre til en alvorlig IKT-relatert hendelse eller en alvorlig betalingsrelatert operasjonell hendelse eller sikkerhetshendelse,
14) «cyberangrep» en ondsinnet IKT-relatert hendelse forårsaket av en trusselaktørs forsøk på å ødelegge, eksponere, endre, deaktivere, stjele eller få uautorisert tilgang til eller uautorisert bruk av en eiendel,
15) «trusseletterretning» opplysninger som er aggregert, omdannet, analysert, tolket eller beriket for å skape den sammenhengen som kreves for beslutningstaking, og for å muliggjøre relevant og tilstrekkelig forståelse med henblikk på å redusere virkningene av en IKT-relatert hendelse eller en cybertrussel, herunder de tekniske detaljene om et cyberangrep, de ansvarlige for angrepet og deres framgangsmåte og motiv,
16) «sårbarhet» en svakhet, mottakelighet eller feil i en eiendel, et system, en prosess eller en kontroll som kan utnyttes,
17) «trusselbasert penetrasjonstesting (TLPT)» et rammeverk som etterligner de taktikkene, teknikkene og framgangsmåtene som brukes av virkelige trusselaktører og oppfattes som en ekte cybertrussel, og som gir en kontrollert, skreddersydd og etterretningsbasert («red team») test av de kritiske produksjonssystemene som er i drift hos den finansielle enheten,
18) «IKT-tredjepartsrisiko» en IKT-risiko som kan oppstå for en finansiell enhet i forbindelse med dens bruk av IKT-tjenester levert av tredjepartsleverandører av IKT-tjenester eller av underleverandører til slike leverandører, herunder gjennom ordninger for utkontraktering,
19) «tredjepartsleverandør av IKT-tjenester» et foretak som leverer IKT-tjenester,
20) «konsernintern leverandør av IKT-tjenester» et foretak som er en del av et finanskonsern, og som hovedsakelig leverer IKT-tjenester til finansielle enheter innenfor samme konsern eller til finansielle enheter som tilhører samme institusjonelle beskyttelsesordning, herunder til deres morforetak, datterforetak, filialer eller andre enheter som er under felles eierskap eller kontroll,
21) «IKT-tjenester» digitale tjenester og datatjenester som fortløpende leveres gjennom IKT-systemer til en eller flere interne eller eksterne brukere, herunder maskinvare som en tjeneste og maskinvaretjenester som omfatter maskinvareleverandørens levering av teknisk støtte via oppdateringer av programvare eller fastvare, med unntak av tradisjonelle analoge telefonitjenester,
22) «kritisk eller viktig funksjon» en funksjon hvis forstyrrelser i vesentlig grad vil forringe en finansiell enhets finansielle inntjening, eller soliditeten eller kontinuiteten i dens tjenester og aktiviteter, eller som, dersom den aktuelle funksjonen avbrytes, er mangelfull eller mislykkes, i vesentlig grad kan forringe en finansiell enhets oppfyllelse av de vilkårene og forpliktelsene som er forbundet med dens tillatelse, eller av dens øvrige forpliktelser i henhold til gjeldende regelverk for finansielle tjenester,
23) «kritisk tredjepartsleverandør av IKT-tjenester» en tredjepartsleverandør av IKT-tjenester som er klassifisert som kritisk i samsvar med artikkel 31,
24) «tredjepartsleverandør av IKT-tjenester som er etablert i et tredjeland» en tredjepartsleverandør av IKT-tjenester som er en juridisk person som er etablert i et tredjeland, og som har inngått en kontraktsregulert ordning med en finansiell enhet om levering av IKT-tjenester,
25) «datterforetak» et datterforetak i henhold til artikkel 2 punkt 10) og artikkel 22 i direktiv 2013/34/EU,
26) «konsern» et konsern som definert i artikkel 2 punkt 11) i direktiv 2013/34/EU,
27) «morforetak» et morforetak i henhold til artikkel 2 punkt 9) og artikkel 22 i direktiv 2013/34/EU,
28) «IKT-underleverandør som er etablert i et tredjeland» en IKT-underleverandør som er en juridisk person som er etablert i et tredjeland, og som har inngått en kontraktsregulert ordning enten med en tredjepartsleverandør av IKT-tjenester eller med en tredjepartsleverandør av IKT-tjenester som er etablert i et tredjeland,
29) «IKT-konsentrasjonsrisiko» en eksponering mot enkelte eller flere tilknyttede kritiske tredjepartsleverandører av IKT-tjenester som skaper en grad av avhengighet av slike leverandører, slik at manglende tilgjengelighet, feil eller annen type svikt hos en slik leverandør kan sette en finansiell enhets evne til å levere kritiske eller viktige funksjoner i fare, eller føre til at den rammes av andre former for negative virkninger, herunder store tap, eller

sette den finansielle stabiliteten i Unionen som helhet i fare,

30) «ledelsesorgan» et ledelsesorgan som definert i artikkel 4 nr. 1 punkt 36) i direktiv 2014/65/EU, artikkel 3 nr. 1 punkt 7) i direktiv 2013/36/EU, artikkel 2 nr. 1 bokstav s) i europaparlaments- og rådsdirektiv 2009/65/EF[31], artikkel 2 nr. 1 punkt 45) i forordning (EU) nr. 909/2014, artikkel 3 nr. 1 punkt 20) i forordning (EU) 2016/1011 og i den relevante bestemmelsen i forordningen om markeder for kryptoeiendeler, eller tilsvarende personer som i praksis leder enheten eller har nøkkelfunksjoner i samsvar med relevant unionsrett eller nasjonal rett,
31) «kredittinstitusjon» en kredittinstitusjon som definert i artikkel 4 nr. 1 punkt 1) i europaparlaments- og rådsforordning (EU) nr. 575/2013[32],
32) «institusjon unntatt i henhold til direktiv 2013/36/EU» en enhet som nevnt i artikkel 2 nr. 5 punkt 4)–23) i direktiv 2013/36/EU,
33) «verdipapirforetak» et verdipapirforetak som definert i artikkel 4 nr. 1 punkt 1) i direktiv 2014/65/EU,
34) «lite verdipapirforetak uten innbyrdes forbindelser» et verdipapirforetak som oppfyller vilkårene i artikkel 12 nr. 1 i europaparlaments- og rådsforordning (EU) 2019/2033[33],
35) «betalingsinstitusjon» en betalingsinstitusjon som definert i artikkel 4 nr. 4 i direktiv (EU) 2015/2366,
36) «betalingsinstitusjon som er unntatt i henhold til direktiv (EU) 2015/2366» en betalingsinstitusjon som er unntatt i henhold til artikkel 32 nr. 1 i direktiv (EU) 2015/2366,
37) «yter av kontoopplysningstjenester» en yter av kontoopplysningstjenester som nevnt i artikkel 33 nr. 1 i direktiv (EU) 2015/2366,
38) «e-pengeforetak» et e-pengeforetak som definert i artikkel 2 punkt 1) i europaparlaments- og rådsdirektiv 2009/110/EF,
39) «e-pengeforetak som er unntatt i henhold til direktiv 2009/110/EF» et e-pengeforetak som er omfattet av et unntak som omhandlet i artikkel 9 nr. 1 i direktiv 2009/110/EF,
40) «sentral motpart» en sentral motpart som definert i artikkel 2 punkt 1) i forordning (EU) nr. 648/2012,
41) «transaksjonsregister» et transaksjonsregister som definert i artikkel 2 punkt 2) i forordning (EU) nr. 648/2012,
42) «verdipapirsentral» en verdipapirsentral som definert i artikkel 2 nr. 1 punkt 1) i forordning (EU) nr. 909/2014,
43) «handelsplass» en handelsplass som definert i artikkel 4 nr. 1 punkt 24) i direktiv 2014/65/EU,
44) «forvalter av alternative investeringsfond» en forvalter av alternative investeringsfond som definert i artikkel 4 nr. 1 bokstav b) i direktiv 2011/61/EU,
45) «forvaltningsselskap» et forvaltningsselskap som definert i artikkel 2 nr. 1 bokstav b) i direktiv 2009/65/EF,
46) «leverandør av datarapporteringstjenester» en leverandør av datarapporteringstjenester i henhold til forordning (EU) nr. 600/2014, som nevnt i artikkel 2 nr. 1 punkt 34)–36) i samme forordning,
47) «forsikringsforetak» et forsikringsforetak som definert i artikkel 13 punkt 1) i direktiv 2009/138/EF,
48) «gjenforsikringsforetak» et gjenforsikringsforetak som definert i artikkel 13 punkt 4) i direktiv 2009/138/EF,
49) «forsikringsformidler» en forsikringsformidler som definert i artikkel 2 nr. 1 punkt 3) i europaparlaments- og rådsforordning (EU) 2016/97[34],
50) «forsikringsformidler som har forsikringsformidling som tilleggsvirksomhet» en forsikringsformidler som har forsikringsformidling som tilleggsvirksomhet, som definert i artikkel 2 nr. 1 punkt 4) i direktiv (EU) 2016/97,
51) «gjenforsikringsformidler» en gjenforsikringsformidler som definert i artikkel 2 nr. 1 punkt 5) i direktiv (EU) 2016/97,
52) «tjenestepensjonsforetak» et tjenestepensjonsforetak som definert i artikkel 6 punkt 1) i direktiv (EU) 2016/2341,

---

31 Europaparlaments- og rådsdirektiv 2009/65/EF av 13. juli 2009 om samordning av lover og forskrifter om foretak for kollektiv investering i omsettelige verdipapirer (UCITS) (EUT L 302 av 17.11.2009, s. 32).

32 Europaparlaments- og rådsforordning (EU) nr. 575/2013 av 26. juni 2013 om tilsynskrav for kredittinstitusjoner og om endring av forordning (EU) nr. 648/2012 (EUT L 176 av 27.6.2013, s. 1).

33 Europaparlaments- og rådsforordning (EU) 2019/2033 av 27. november 2019 om tilsynskrav for verdipapirforetak og om endring av forordning (EU) nr. 1093/2010, (EU) nr. 575/2013, (EU) nr. 600/2014 og (EU) nr. 806/2014 (EUT L 314 av 5.12.2019, s. 1).

34 Europaparlaments- og rådsdirektiv (EU) 2016/97 av 20. januar 2016 om forsikringsdistribusjon (EUT L 26 av 2.2.2016, s. 19).

53) «lite tjenestepensjonsforetak» et tjenestepensjonsforetak som forvalter pensjonsordninger som til sammen har mindre enn 100 medlemmer,
54) «kredittvurderingsbyrå» et kredittvurderingsbyrå som definert i artikkel 3 nr. 1 bokstav b) i forordning (EF) nr. 1060/2009,
55) «tilbyder av kryptoeiendelstjenester» en tilbyder av kryptoeiendelstjenester som definert i den relevante bestemmelsen i forordningen om markeder for kryptoeiendeler,
56) «utsteder av kryptoeiendeler» en utsteder av kryptoeiendeler som definert i den relevante bestemmelsen i forordningen om markeder for kryptoeiendeler,
57) «administrator av kritiske referanseverdier» en administrator av kritiske referanseverdier som definert i artikkel 3 nr. 1 punkt 25) i forordning (EU) 2016/1011,
58) «tilbyder av folkefinansieringstjenester» en tilbyder av folkefinansieringstjenester som definert i artikkel 2 nr. 1 bokstav e) i europaparlaments- og rådsforordning (EU) 2020/1503[35],
59) «verdipapiriseringsregister» et verdipapiriseringsregister som definert i artikkel 2 punkt 23) i europaparlaments- og rådsforordning (EU) 2017/2402[36],
60) «svært liten bedrift» en finansiell enhet, som ikke er en handelsplass, en sentral motpart, et transaksjonsregister eller en verdipapirsentral, og som sysselsetter færre enn ti personer og har en årsomsetning og/eller en samlet årsbalanse som ikke overstiger 2 millioner euro,
61) «hovedovervåker» den europeiske tilsynsmyndigheten som er utpekt i samsvar med artikkel 31 nr. 1 bokstav b) i denne forordningen,
62) «felleskomité» den komiteen som er nevnt i artikkel 54 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010,
63) «liten bedrift» en finansiell enhet som sysselsetter ti eller flere personer, men færre enn 50 personer, og som har en årsomsetning og/eller en samlet årsbalanse som overstiger 2 millioner euro, men som ikke overstiger 10 millioner euro,
64) «mellomstor bedrift» en finansiell enhet som ikke er en liten bedrift, og som sysselsetter færre enn 250 personer og har en årsomsetning som ikke overstiger 50 millioner euro og/eller en årsbalanse som ikke overstiger 43 millioner euro,
65) «offentlig myndighet» enhver offentlig myndighet eller andre enheter innen offentlig forvaltning, herunder nasjonale sentralbanker.

Artikkel 4

Forholdsmessighetsprinsippet

1. Finansielle enheter skal gjennomføre reglene fastsatt i kapittel II i samsvar med forholdsmessighetsprinsippet, samtidig som det tas hensyn til deres størrelse og generelle risikoprofil samt til arten, omfanget og kompleksiteten av deres tjenester, aktiviteter og drift.
2. I tillegg skal finansielle enheters anvendelse av kapittel III, IV og V avsnitt I, stå i et rimelig forhold til deres størrelse og generelle risikoprofil, samt til arten, omfanget og kompleksiteten av deres tjenester, aktiviteter og drift, slik det er spesifisert i de relevante reglene i disse kapitlene.
3. De vedkommende myndighetene skal vurdere finansielle enheters anvendelse av forholdsmessighetsprinsippet når de gjennomgår sammenhengen i rammeverket for IKT-risikostyring på grunnlag av de rapportene som framlegges på anmodning fra vedkommende myndigheter i henhold til artikkel 6 nr. 5 og artikkel 16 nr. 2.

Kapittel II

IKT-risikostyring

Avsnitt I

Artikkel 5

Styring og organisering

1. Finansielle enheter skal ha innført et intern rammeverk for styring og kontroll som sikrer en effektiv og forsvarlig styring av IKT-risiko, i samsvar med artikkel 6 nr. 4, for å oppnå et høyt nivå av digital operasjonell motstandsdyktighet.
2. Ledelsesorganet i den finansielle enheten skal definere, godkjenne, føre tilsyn med og ha ansvar for gjennomføringen av alle ordninger knyttet til rammeverket for IKT-risikostyring nevnt i artikkel 6 nr. 1.

   Ved anvendelse av første ledd skal organet

---

35 Europaparlaments- og rådsforordning (EU) 2020/1503 av 7. oktober 2020 om europeiske tilbydere av folkefinansieringstjenester til næringsvirksomhet og om endring av forordning (EU) 2017/1129 og direktiv (EU) 2019/1937 (EUT L 347 av 20.10.2020, s. 1).

36 Europaparlaments- og rådsforordning (EU) 2017/2402 av 12. desember 2017 om fastsettelse av en generell ramme for verdipapirisering og en særskilt ramme for enkel, gjennomsiktig og standardisert verdipapirisering, og om endring av direktiv 2009/65/EF, 2009/138/EF og 2011/61/EU og forordning (EF) nr. 1060/2009 og (EU) nr. 648/2012 (EUT L 347 av 28.12.2017, s. 35).

a) ha det endelige ansvaret for å styre den finansielle enhetens IKT-risiko,
b) innføre retningslinjer som tar sikte på å sikre opprettholdelse av høye standarder for tilgjengeligheten, autentisiteten, integriteten og fortroligheten til dataene,
c) fastsette klare roller og ansvarsområder for alle IKT-relaterte funksjoner og etablere hensiktsmessige styringsordninger for å sikre effektiv og rettidig kommunikasjon, samarbeid og koordinering mellom disse funksjonene,
d) ha det endelige ansvaret for å fastsette og godkjenne strategien for digital operasjonell motstandsdyktighet som nevnt i artikkel 6 nr. 8, herunder fastsette et passende risikotoleransenivå for den finansielle enhetens IKT-risiko, som nevnt i artikkel 6 nr. 8 bokstav b),
e) godkjenne, føre tilsyn med og regelmessig gjennomgå gjennomføringen av den finansielle enhetens retningslinjer for IKT-kontinuitet i virksomheten og planer for IKT-respons og -gjenoppretting som nevnt i henholdsvis artikkel 11 nr. 1 og 3, som kan vedtas som egne spesifikke retningslinjer som utgjør en integrert del av den finansielle enhetens overordnede retningslinjer for kontinuitet i virksomheten og respons- og gjenopprettingsplan,
f) godkjenne og regelmessig gjennomgå den finansielle enhetens interne IKT-revisjonsplaner, IKT-revisjoner og vesentlige endringer i dem,
g) tildele og regelmessig gjennomgå et passende budsjett for å oppfylle den finansielle enhetens behov i forbindelse med digital operasjonell motstandsdyktighet med hensyn til alle typer ressurser, herunder relevante IKT-programmer for å bevisstgjøre om IKT-sikkerhet og opplæring i digital operasjonell motstandsdyktighet nevnt i artikkel 13 nr. 6, og IKT-ferdigheter for alle ansatte,
h) godkjenne og regelmessig gjennomgå den finansielle enhetens retningslinjer for ordninger når det gjelder bruk av IKT-tjenester levert av tredjepartsleverandører av IKT-tjenester,
i) innføre, på foretaksnivå, rapporteringskanaler som gjør det mulig å bli behørig underrettet om
   i) ordninger inngått med tredjepartsleverandører av IKT-tjenester om bruk av IKT-tjenester,
   ii) alle relevante planlagte vesentlige endringer med hensyn til tredjepartsleverandører av IKT-tjenester,
   iii) potensielle virkninger av slike endringer på de kritiske eller viktige funksjonene som omfattes av disse ordningene, herunder et sammendrag av risikoanalysen for å vurdere virkningene av disse endringene, og som et minimum alvorlige IKT-relaterte hendelser og deres virkninger, samt respons- og gjenopprettingstiltak og korrigerende tiltak.

3. Andre finansielle enheter enn svært små bedrifter skal opprette en funksjon for å overvåke ordninger inngått med tredjepartsleverandører av IKT-tjenester om bruk av IKT-tjenester, eller skal utpeke et medlem av den øverste ledelsen som ansvarlig for å føre tilsyn med tilhørende risikoeksponering og relevant dokumentasjon.
4. Medlemmene av den finansielle enhetens ledelsesorgan skal hele tiden holde seg oppdatert med tilstrekkelig kunnskap og ferdigheter slik at de kan forstå og vurdere IKT-risikoen og dens innvirkning på den finansielle enhetens drift, herunder ved regelmessig å gjennomgå spesifikk opplæring som står i et rimelig forhold til den IKT-risikoen som styres.

Avsnitt II

Artikkel 6

Ramme for IKT-risikostyring

1. Finansielle enheter skal ha et forsvarlig, omfattende og veldokumentert rammeverk for IKT-risikostyring som en del av sitt overordnede risikostyringssystem, slik at de kan håndtere IKT-risiko på en rask, effektiv og grundig måte og sikre et høyt nivå av digital operasjonell motstandsdyktighet.
2. Rammeverket for IKT-risikostyring skal som et minimum omfatte strategier, retningslinjer, framgangsmåter, IKT-protokoller og -verktøyer som er nødvendige for på behørig vis og i tilstrekkelig grad å beskytte alle informasjonsressurser og IKT-ressurser, herunder programvare, maskinvare, servere, samt for å beskytte alle relevante fysiske komponenter og infrastrukturer, som for eksempel lokaler, datasentre og følsomme utpekte områder, for å sikre at alle informasjonsressurser og IKT-ressurser er tilstrekkelig beskyttet mot risiko, herunder skade og uautorisert tilgang eller bruk.

3. I samsvar med sitt rammeverk for IKT-risikostyring skal finansielle enheter minimere virkningen av IKT-risiko gjennom å innføre egnede strategier, retningslinjer, framgangsmåter, IKT-protokoller og -verktøyer. De skal gi fullstendige og oppdaterte opplysninger om IKT-risiko og om sitt rammeverk for IKT-risikostyring til de vedkommende myndighetene når de anmoder om det.
4. Andre finansielle enheter enn svært små bedrifter skal tildele ansvaret for å styre og føre tilsyn med IKT-risiko til en kontrollfunksjon og sikre et passende nivå av uavhengighet for en slik kontrollfunksjon for å unngå interessekonflikter. Finansielle enheter skal sikre et passende skille og uavhengighet av IKT-risikostyringsfunksjoner, kontrollfunksjoner og interne revisjonsfunksjoner i henhold til modellen med tre forsvarslinjer eller en intern modell for risikostyring og kontroll.
5. Rammeverket for IKT-risikostyring skal dokumenteres og gjennomgås minst én gang i året, eller regelmessig når det gjelder svært små bedrifter, samt når det forekommer alvorlige IKT-relaterte hendelser, og i henhold til tilsynsinstrukser eller konklusjoner fra relevante tester av digital operasjonell motstandsdyktighet eller fra revisjonsprosesser. Rammeverket skal forbedres kontinuerlig på grunnlag av erfaringer fra gjennomføring og overvåking. En rapport om gjennomgåelsen av rammeverket for IKT-risikostyring skal legges fram for den vedkommende myndigheten når den anmoder om det.
6. Rammeverket for IKT-risikostyring for andre finansielle enheter enn svært små bedrifter skal regelmessig være gjenstand for internrevisjon av revisorer i tråd med den finansielle enhetens revisjonsplan. Disse revisorene skal ha tilstrekkelig kunnskap, ferdigheter og ekspertise med hensyn til IKT-risiko samt være tilstrekkelig uavhengige. Hyppigheten av IKT-revisjoner og deres fokus skal stå i et rimelig forhold til den finansielle enhetens IKT-risiko.
7. De finansielle enhetene skal på grunnlag av konklusjonene fra internrevisjonen opprette en formell oppfølgingsprosess, herunder regler om rettidig verifisering og utbedring av kritiske resultater fra IKT-revisjonen.
8. Rammeverket for IKT-risikostyring skal omfatte en strategi for digital operasjonell motstandsdyktighet som fastsetter hvordan rammeverket skal gjennomføres. For dette formålet skal strategien for digital operasjonell motstandsdyktighet omfatte metoder for å håndtere IKT-risiko og oppfylle spesifikke IKT-mål gjennom å
   a) redegjøre for hvordan rammeverket for IKT-risikostyring støtter den finansielle enhetens forretningsstrategi og mål,
   b) fastsette risikotoleransenivået for IKT-risiko i samsvar med den finansielle enhetens risikovillighet og analysere toleransen mot virkninger av IKT-forstyrrelser,
   c) redegjøre for klare mål for informasjonssikkerhet, herunder nøkkelindikatorer og viktige risikoparametrer,
   d) redegjøre for IKT-referansearkitekturen og eventuelle endringer som er nødvendige for å nå spesifikke forretningsmål,
   e) beskrive de ulike ordningene som er innført for å påvise IKT-relaterte hendelser, forebygge deres innvirkning og gi beskyttelse mot den,
   f) dokumentere den nåværende situasjonen for den digitale operasjonelle motstandsdyktigheten på grunnlag av antall alvorlige IKT-relaterte hendelser som er rapportert, og effektiviteten av de forebyggende tiltakene,
   g) gjennomføre testing av digital operasjonell motstandsdyktighet i samsvar med kapittel IV i denne forordningen,
   h) utarbeide en kommunikasjonsstrategi i tilfelle av IKT-relaterte hendelser hvis offentliggjøring er påkrevd i samsvar med artikkel 14.
9. Finansielle enheter kan i forbindelse med strategien for digital operasjonell motstandsdyktighet som nevnt i nr. 8 utforme en helhetlig strategi med flere ulike leverandører av IKT-tjenester på konsern- eller enhetsnivå som viser hvor det er stor avhengighet av tredjepartsleverandører av IKT-tjenester, og forklare logikken bak den valgte sammensetningen av tredjepartsleverandører av IKT-tjenester.
10. Finansielle enheter kan i samsvar med unionsretten og nasjonal sektorspesifikk lovgivning utkontraktere oppgavene med å kontrollere overholdelsen av kravene til IKT-risikostyring til konserninterne eller eksterne foretak. Ved slik utkontraktering er den finansielle enheten fortsatt fullt ansvarlig for å kontrollere at kravene til IKT-risikostyring overholdes.

Artikkel 7

IKT-systemer, -protokoller og -verktøyer

For å håndtere og styre IKT-risiko skal de finansielle enhetene bruke og opprettholde oppdaterte IKT-systemer, -protokoller og -verktøyer som er

a) hensiktsmessige med hensyn til omfanget av transaksjoner som ligger til grunn for deres virksomhet, i samsvar med forholdsmessighetsprinsippet som nevnt i artikkel 4,
b) pålitelige,
c) utstyrt med tilstrekkelig kapasitet med henblikk på en korrekt behandling av de opplysningene som er nødvendige for å utføre aktiviteter og rettidig levering av tjenester, og for å håndtere toppbelastning med hensyn til ordre-, meldings- eller transaksjonsvolum etter behov, herunder når det innføres ny teknologi,
d) teknologisk motstandsdyktige for i tilstrekkelig grad å håndtere ytterligere behov for informasjonsbehandling som kreves under stressede markedsforhold eller andre vanskelige situasjoner.

Artikkel 8

Identifisering

1. Som en del av det rammeverket for IKT-risikostyring som er nevnt i artikkel 6 nr. 1, skal finansielle enheter identifisere, klassifisere og på en hensiktsmessig måte dokumentere alle IKT-støttede forretningsfunksjoner, roller og ansvarsområder, de informasjonsressursene og IKT-ressursene som støtter disse funksjonene, og deres roller og avhengighet med hensyn til IKT-risiko. Finansielle enheter skal ved behov og minst én gang i året vurdere hvorvidt denne klassifiseringen og all relevant dokumentasjon er tilstrekkelig.
2. Finansielle enheter skal fortløpende identifisere alle kilder til IKT-risiko, særlig risikoeksponeringen mot og fra andre finansielle enheter, og vurdere cybertrusler og IKT-sårbarheter som er relevante for deres IKT-støttede forretningsfunksjoner, informasjonsressurser og IKT-ressurser. Finansielle enheter skal regelmessig og minst én gang i året gjennomgå de risikoscenarioene som påvirker dem.
3. Andre finansielle enheter enn svært små bedrifter skal foreta en risikovurdering etter hver større endring av infrastrukturen i nettverks- og informasjonssystemene, i de prosessene eller framgangsmåtene som påvirker deres IKT-støttede forretningsfunksjoner, informasjonsressurser eller IKT-ressurser.
4. De finansielle enhetene skal identifisere alle informasjonsressurser og IKT-ressurser, herunder på eksterne steder, nettverksressurser og maskinvareutstyr, og de skal kartlegge de som anses som kritiske. De skal kartlegge konfigurasjonen til informasjonsressursene og IKT-ressursene samt forbindelsene og den gjensidige avhengigheten mellom de ulike informasjonsressursene og IKT-ressursene.
5. De finansielle enhetene skal identifisere og dokumentere alle prosesser som er avhengige av tredjepartsleverandører av IKT-tjenester, og skal identifisere innbyrdes forbindelser med tredjepartsleverandører av IKT-tjenester som leverer tjenester som støtter kritiske eller viktige funksjoner.
6. Ved anvendelse av nr. 1, 4 og 5 skal finansielle enheter føre relevante varefortegnelser og oppdatere dem regelmessig og hver gang det skjer en større endring som nevnt i nr. 3.
7. Andre finansielle enheter enn svært små bedrifter skal regelmessig og minst én gang i året foreta en særskilt IKT-risikovurdering av alle eldre IKT-systemer og i hvert tilfelle før og etter sammenkopling av teknologier, applikasjoner eller systemer.

Artikkel 9

Beskyttelse og forebygging

1. For å sikre tilstrekkelig beskyttelse av IKT-systemer og organisere mottiltak skal finansielle enheter kontinuerlig overvåke og kontrollere IKT-systemers og -verktøyers sikkerhet og virkemåte, og minimere virkningen av IKT-risiko på IKT-systemer gjennom å innføre egnede sikkerhetsverktøyer, retningslinjer og prosedyrer for IKT-sikkerhet.
2. Finansielle enheter skal utforme, anskaffe og gjennomføre IKT-relaterte sikkerhetsstrategier, -prosedyrer, -protokoller og -verktøyer som har til formål å sikre IKT-systemers motstandsdyktighet, kontinuitet og tilgjengelighet, særlig for de systemene som støtter kritiske eller viktige funksjoner, og å opprettholde høye standarder for tilgjengeligheten, autentisiteten, integriteten og fortroligheten til dataene, enten de er inaktive, i bruk eller under overføring.
3. For å nå målene nevnt i nr. 2 skal finansielle enheter bruke IKT-løsninger og -prosesser som er hensiktsmessige i samsvar med artik-

kel 4. Disse IKT-løsningene og -prosessene skal

a) sikre sikkerheten for metoden ved overføring av data,
b) minimere risikoen for korrumpering eller tap av data, uautorisert tilgang og tekniske feil som kan hemme forretningsvirksomheten,
c) forhindre mangel på tilgjengelighet, svekkelse av autentisiteten og integriteten, brudd på regler om fortrolighet og tap av data,
d) sikre at opplysningene er beskyttet mot risikoer som oppstår i forbindelse med databehandling, herunder dårlig forvaltning, prosessrelaterte risikoer og menneskelige feil.

4. Som en del av det rammeverket for IKT-risikostyring som er nevnt i artikkel 6 nr. 1, skal finansielle enheter

a) utarbeide og dokumentere retningslinjer for informasjonssikkerhet der det er fastsatt regler for å beskytte tilgjengeligheten, autentisiteten, integriteten og fortroligheten til dataene, informasjonsressurser og IKT-ressurser, herunder hos deres kunder, dersom det er relevant,
b) ved å følge en risikobasert tilnærming, innføre en forsvarlig forvaltningsstruktur for nettverk og infrastrukturer ved hjelp av passende teknikker, metoder og protokoller som kan omfatte gjennomføring av automatiserte ordninger for å isolere berørte informasjonsressurser ved cyberangrep,
c) gjennomføre retningslinjer som begrenser den fysiske eller logiske tilgangen til informasjonsressurser og IKT-ressurser til bare det som kreves for legitime og godkjente funksjoner og aktiviteter, og innføre en rekke retningslinjer, framgangsmåter og kontroller som omhandler tilgangsrettigheter, og sikre en forsvarlig forvaltning av disse,
d) gjennomføre retningslinjer og protokoller for sterke systemer for autentisering på grunnlag av relevante standarder og særskilte kontrollsystemer, og beskyttelsestiltak for kryptonøkler der data krypteres på grunnlag av resultatene av godkjente prosesser for dataklassifisering og IKT-risikovurdering,
e) gjennomføre dokumenterte retningslinjer, framgangsmåter og kontroller for håndtering av IKT-endringer, herunder endringer av programvare, maskinvare, fastvarekomponenter, systemer eller sikkerhetsparametrer, som bygger på en risikovurderingsmetode og er en integrert del av den finansielle enhetens overordnede prosess for endringsstyring, for å sikre at alle endringer av IKT-systemer registreres, testes, vurderes, godkjennes, gjennomføres og verifiseres på en kontrollert måte,
f) sørge for at det innføres hensiktsmessige og omfattende dokumenterte retningslinjer for programvareutbedringer og oppdateringer.

Ved anvendelse av første ledd bokstav b) skal finansielle enheter utforme infrastrukturen for nettilkopling på en måte som gjør det mulig å avbryte eller segmentere den øyeblikkelig for å minimere og forhindre spredning, særlig i forbindelse med innbyrdes forbundne finansielle prosesser.

Ved anvendelse av første ledd bokstav e) skal prosessen for håndtering av IKT-endringer godkjennes av passende ledelsesnivåer og omfatte spesifikke protokoller.

Artikkel 10

Påvisning

1. De finansielle enhetene skal ha ordninger for rask påvisning av anormal virksomhet i samsvar med artikkel 17, herunder problemer med IKT-nettverkets yteevne og IKT-relaterte hendelser, og for å identifisere potensielle vesentlige svake punkter («single points of failure»).

   Alle ordninger for påvisning omhandlet i første ledd skal testes regelmessig i samsvar med artikkel 25.
2. Ordningene for påvisning nevnt i nr. 1 skal muliggjøre flere kontrollnivåer, inneholde fastsatte varslingsterskler og varslingskriterier for å utløse og iverksette IKT-relaterte hendelser, herunder automatiske varslingsordninger for det relevante personalet som har ansvar for håndtering av IKT-relaterte hendelser.
3. De finansielle enhetene skal avsette tilstrekkelig med ressurser og kapasitet for å overvåke brukeraktivitet, forekomsten av IKT-avvik og IKT-relaterte hendelser, særlig cyberangrep.
4. Leverandørene av datarapporteringstjenester skal i tillegg ha systemer som på en effektiv måte kan kontrollere om handelsrapportene er fullstendige, identifisere utelatelser og åpenbare feil og anmode om at disse rapportene overføres på nytt.

Artikkel 11

Respons og gjenoppretting

1. Som en del av rammeverket for IKT-risikostyring som er nevnt i artikkel 6 nr. 1 og på grunnlag av kravene til identifisering som er fastsatt i artikkel 8, skal finansielle enheter innføre omfattende retningslinjer for IKT-kontinuitet i virksomheten, som kan vedtas som egne spesifikke retningslinjer, og som utgjør en integrert del av den finansielle enhetens overordnede retningslinjer for kontinuitet i virksomheten.
2. De finansielle enhetene skal gjennomføre retningslinjer for IKT-kontinuitet i virksomheten gjennom særskilte, hensiktsmessige og dokumenterte ordninger, planer, framgangsmåter og ordninger som tar sikte på
   a) å sikre kontinuiteten i den finansielle enhetens kritiske eller viktige funksjoner,
   b) å reagere på og løse alle IKT-relaterte hendelser raskt, riktig og effektivt på en måte som begrenser skade og prioriterer gjenopptakelse av virksomhet og gjenopprettingstiltak,
   c) å aktivere omgående særskilte planer som muliggjør begrensningstiltak, prosesser og teknologier tilpasset hver type av IKT-relatert hendelse, og som forhindrer ytterligere skader, samt skreddersydde framgangsmåter for respons og gjenoppretting som fastsatt i samsvar med artikkel 12,
   d) å beregne foreløpige virkninger, skader og tap,
   e) å fastsette kommunikasjons- og krisehåndteringstiltak som sikrer at oppdaterte opplysninger overføres til alt berørt internt personale og eksterne berørte parter i samsvar med artikkel 14, og at de rapporteres til de vedkommende myndighetene i samsvar med artikkel 19.
3. Som en del av rammeverket for IKT-risikostyring som er nevnt i artikkel 6 nr. 1, skal finansielle enheter gjennomføre tilhørende planer for IKT-respons og -gjenoppretting som, når det gjelder andre finansielle enheter enn svært små bedrifter, skal gjennomgås av uavhengige internrevisjoner.
4. De finansielle enhetene skal innføre, opprettholde og regelmessig teste hensiktsmessige planer for IKT-kontinuitet i virksomheten, særlig med hensyn til kritiske eller viktige funksjoner som er utkontraktert eller kontrahert gjennom ordninger inngått med tredjepartsleverandører av IKT-tjenester.
5. De finansielle enhetene skal som en del av sine overordnede retningslinjer for kontinuitet i virksomheten foreta en driftskonsekvensanalyse av hvor eksponerte de er mot alvorlige driftsforstyrrelser. De finansielle enhetene skal i forbindelse med driftskonsekvensanalysen vurdere potensielle virkninger av alvorlige driftsforstyrrelser ved hjelp av kvantitative og kvalitative kriterier ved anvendelse av interne og eksterne data og scenarioanalyse, alt etter hva som er relevant. Driftskonsekvensanalysen skal ta hensyn til den kritiske verdien til identifiserte og kartlagte forretningsfunksjoner, støtteprosesser, avhengighet av tredjeparter og informasjonsressurser og deres gjensidige avhengighet. De finansielle enhetene skal sikre at IKT-ressurser og IKT-tjenester utformes og anvendes helt i tråd med driftskonsekvensanalysen, særlig når det gjelder å sikre i tilstrekkelig grad alle kritiske komponenters redundans.
6. De finansielle enhetene skal som en del av sin omfattende IKT-risikostyring
   a) teste planene for IKT-kontinuitet i virksomheten og planene for IKT-respons og -gjenoppretting i forbindelse med IKT-systemer som støtter alle funksjoner minst én gang i året, samt ved eventuelle vesentlige endringer av IKT-systemer som støtter kritiske eller viktige funksjoner,
   b) teste de krisekommunikasjonsplanene som er utarbeidet i samsvar med artikkel 14.

   Ved anvendelse av første ledd bokstav a) skal andre finansielle enheter enn svært små bedrifter ta med i testplanene scenarioer for cyberangrep og overflytting mellom den primære IKT-infrastrukturen og den redundante kapasiteten, sikkerhetskopier og de redundante anleggene som er nødvendige for å oppfylle forpliktelsene fastsatt i artikkel 12.

   De finansielle enhetene skal regelmessig gjennomgå sine retningslinjer for IKT-kontinuitet i virksomheten og planer for IKT-respons og -gjenoppretting, samtidig som det tas hensyn til resultatene av de testene som er utført i samsvar med første ledd, og anbefalinger som bygger på revisjonskontroller eller tilsynskontroller.
7. Andre finansielle enheter enn svært små bedrifter skal ha en krisehåndteringsfunksjon som, dersom deres planer for IKT-kontinuitet i virksomheten eller planer for IKT-respons og -gjenoppretting aktiveres, blant annet skal inneholde tydelige framgangsmåter for å

håndtere intern og ekstern krisekommunikasjon i samsvar med artikkel 14.

8. De finansielle enhetene skal føre lett tilgjengelige registre over aktiviteter som pågår før og ved driftsforstyrrelser, når deres planer for IKT-kontinuitet i virksomheten og planer for IKT-respons og -gjenoppretting aktiveres.
9. Verdipapirsentraler skal legge fram kopier av resultatene av testene av IKT-kontinuitet i virksomheten eller av lignende aktiviteter for de vedkommende myndighetene.
10. Andre finansielle enheter enn svært små bedrifter skal på anmodning fra de vedkommende myndighetene innberette et overslag over samlede årlige kostnader og tap forårsaket av alvorlige IKT-relaterte hendelser.
11. I samsvar med artikkel 16 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010 skal de europeiske tilsynsmyndighetene gjennom Felleskomiteen innen 17. juli 2024 utarbeide felles retningslinjer for overslaget over de samlede årlige kostnadene og tapene nevnt i nr. 10.

Artikkel 12

Retningslinjer og framgangsmåter for sikkerhetskopiering og framgangsmåter og metoder for gjenskapelse og gjenoppretting

1. For å sikre gjenskapelse av IKT-systemer og data med minimal nedetid, begrensede forstyrrelser og tap skal finansielle enheter som en del av sitt rammeverk for IKT-risikostyring utarbeide og dokumentere
   a) retningslinjer og framgangsmåter for sikkerhetskopiering som angir omfanget av de dataene som skal sikkerhetskopieres, og minste hyppighet for sikkerhetskopiering, basert på opplysningenes kritiske verdi eller fortrolighetsnivået for opplysningene,
   b) framgangsmåter og metoder for gjenskapelse og gjenoppretting.
2. De finansielle enhetene skal sette opp systemer for sikkerhetskopiering som kan aktiveres i samsvar med retningslinjene og framgangsmåtene for sikkerhetskopiering, samt framgangsmåter og metoder for gjenskapelse og gjenoppretting. Aktiveringen av systemer for sikkerhetskopiering skal ikke sette sikkerheten til nettverks- og informasjonssystemene eller tilgjengeligheten, autentisiteten, integriteten eller fortroligheten til dataene i fare. Testing av framgangsmåter for sikkerhetskopiering og framgangsmåter og metoder for gjenskapelse og gjenoppretting skal gjennomføres med jevne mellomrom.
3. Når finansielle enheter gjenskaper sikkerhetskopierte data ved bruk av egne systemer, skal de bruke IKT-systemer som er fysisk og logisk atskilt fra det IKT-systemet som er kilden. IKT-systemene skal ha en sikker beskyttelse mot enhver form for uautorisert tilgang eller IKT-korrumpering og gjøre det mulig å gjenskape tjenester ved hjelp av sikkerhetskopiering av data og systemer etter behov.

   For sentrale motparter skal gjenopprettingsplaner gjøre det mulig å gjenopprette alle transaksjoner fra det tidspunktet da de ble avbrutt, slik at den sentrale motpartens virksomhet fortsatt er sikker og avviklingen kan fullføres på den planlagte datoen.

   Leverandørene av datarapporteringstjenester skal dessuten ha tilstrekkelige ressurser og fasiliteter for sikkerhetskopiering og gjenskapelse, slik at de kan tilby og opprettholde sine tjenester til enhver tid.
4. Andre finansielle enheter enn svært små bedrifter skal opprettholde redundant IKT-kapasitet med ressurser, evne og funksjoner som er tilstrekkelige for å sikre virksomhetens behov. Svært små bedrifter skal vurdere behovet for å opprettholde en slik redundant IKT-kapasitet på grunnlag av hvilken risikoprofil de har.
5. Verdipapirsentraler skal ha minst ett sekundært driftssted utstyrt med tilstrekkelige ressurser, evne, funksjoner og personalmessige ordninger for å sikre virksomhetens behov.

   Det sekundære driftsstedet skal
   a) være plassert tilstrekkelig langt fra det primære driftsstedet for å sikre at det har en annen risikoprofil, og for å forhindre at det påvirkes av den hendelsen som påvirker det primære driftsstedet,
   b) kunne sikre kontinuiteten for kritiske eller viktige funksjoner som er identiske med det primære driftsstedet, eller opprettholde det tjenestenivået som er nødvendig for å sikre at den finansielle enheten kan utføre sin kritiske virksomhet innenfor rammen av gjenopprettingsmålene,
   c) være tilgjengelig umiddelbart for den finansielle enhetens personale for å sikre kontinuiteten for kritiske eller viktige funksjoner dersom det primære driftsstedet ikke er tilgjengelig.
6. Når finansielle enheter fastsetter mål for gjenopprettingstid og gjenopprettingspunkt for hver funksjon, skal de ta hensyn til om det er en kri-

tisk eller viktig funksjon, og til den mulige samlede innvirkningen på markedets effektivitet. Slike tidsmål skal sikre at de avtalte tjenestenivåene oppnås i ekstreme scenarioer.

7. Når de finansielle enhetene gjenoppretter virksomheten etter en IKT-relatert hendelse, skal de utføre nødvendige kontroller, herunder eventuelt flere kontroller og avstemminger, for å sikre at dataintegriteten holder høyeste nivå. Disse kontrollene skal også utføres når data fra eksterne berørte parter rekonstrueres, for å sikre at alle dataene til systemene er sammenhengende.

Artikkel 13

Læring og utvikling

1. De finansielle enhetene skal sørge for å ha kapasitet og personale som kan samle inn opplysninger om sårbarheter og cybertrusler, IKT-relaterte hendelser, særlig cyberangrep, og analysere hvilken innvirkning de forventes å ha på deres digitale operasjonelle motstandsdyktighet.
2. De finansielle enhetene skal gjennomgå IKT-relaterte hendelser etter at en alvorlig IKT-relatert hendelse forstyrrer deres kjernevirksomhet, analysere årsakene til forstyrrelsen og identifisere nødvendige forbedringer av IKT-virksomheten eller av de retningslinjene for IKT-kontinuitet i virksomheten som er nevnt i artikkel 11.

   Andre finansielle enheter enn svært små bedrifter skal, på anmodning, underrette de vedkommende myndighetene om endringene som ble gjennomført etter gjennomgåelsen av IKT-relaterte hendelser som nevnt i første ledd.

   Gjennomgåelsene etter IKT-relaterte hendelser nevnt i første ledd skal avgjøre om de fastsatte framgangsmåtene ble fulgt, og om de tiltakene som ble truffet, var effektive, blant annet når det gjelder
   a) svartiden for å reagere på sikkerhetsvarsler og fastslå virkningen av IKT-relaterte hendelser og alvorlighetsgraden av dem,
   b) kvaliteten og hastigheten i forbindelse med utførelse av en kriminalteknisk analyse, dersom det anses som hensiktsmessig,
   c) effektiviteten av den finansielle enhetens håndtering av feilhendelser,
   d) effektiviteten av intern og ekstern kommunikasjon.
3. Erfaringer fra testing av den digitale operasjonelle motstandsdyktigheten som er utført i samsvar med artikkel 26 og 27, og fra faktiske IKT-relaterte hendelser, særlig cyberangrep, samt utfordringer som oppstår i forbindelse med aktiveringen av planer for IKT-kontinuitet i virksomheten og planer for IKT-respons og -gjenoppretting, skal sammen med relevante opplysninger som utveksles med motparter, og som vurderes i forbindelse med tilsynskontroller, fortløpende innarbeides i IKT-risikovurderingsprosessen. Disse resultatene skal danne grunnlag for hensiktsmessige gjennomgåelser av relevante komponenter i det rammeverket for IKT-risikostyring som er nevnt i artikkel 6 nr. 1.
4. De finansielle enhetene skal overvåke effektiviteten av gjennomføringen av den strategien for digital operasjonell motstandsdyktighet som er fastsatt i artikkel 6 nr. 8. De skal kartlegge IKT-risikoens utvikling over tid, analysere hyppigheten, typene, omfanget og utviklingen av IKT-relaterte hendelser, særlig cyberangrep og deres mønstre, med henblikk på å forstå graden av IKT-risikoeksponering, særlig når det gjelder kritiske eller viktige funksjoner, og forbedre den finansielle enhetens cybermodenhet og cyberberedskap.
5. Ledende IKT-ansatte skal minst én gang i året rapportere til ledelsesorganet om de resultatene som er nevnt i nr. 3, og legge fram anbefalinger.
6. De finansielle enhetene skal utarbeide bevisstgjøringsprogrammer om IKT-sikkerhet og opplæring i digital operasjonell motstandsdyktighet som obligatoriske moduler i sine ordninger for personalopplæring. Disse programmene og denne opplæringen skal gjelde for alle ansatte og for personer i den øverste ledelsen, og skal ha en grad av kompleksitet som tilsvarer deres oppgavers ansvarsområde. Dersom det er relevant, skal finansielle enheter også inkludere tredjepartsleverandører av IKT-tjenester i sine relevante opplæringsordninger i samsvar med artikkel 30 nr. 2 bokstav i).
7. Andre finansielle enheter enn svært små bedrifter skal overvåke den relevante teknologiske utviklingen fortløpende, også for å forstå hvilken virkning innføringen av slike nye teknologier kan få på kravene til IKT-sikkerhet og digital operasjonell motstandsdyktighet. De skal holde seg oppdatert om de seneste prosessene for IKT-risikostyring for å bekjempe aktuelle eller nye former for cyberangrep på en effektiv måte.

Artikkel 14

Kommunikasjon

1. Som en del av rammeverket for IKT-risikostyring som er nevnt i artikkel 6 nr. 1, skal finansielle enheter ha krisekommunikasjonsplaner som gjør det mulig å informere kunder og motparter samt allmennheten på en ansvarsfull måte om minst alvorlige IKT-relaterte hendelser eller sårbarheter, alt etter hva som er relevant.
2. Som en del av rammeverket for IKT-risikostyring skal finansielle enheter gjennomføre kommunikasjonsstrategier for internt ansatte og eksterne berørte parter. I kommunikasjonsstrategiene for de ansatte skal det tas hensyn til behovet for å skille mellom ansatte som deltar i IKT-risikostyring, særlig ansatte som har ansvar for respons og gjenoppretting, og ansatte som har behov for opplysninger.
3. Minst én person i den finansielle enheten skal ha i oppgave å gjennomføre kommunikasjonsstrategien for IKT-relaterte hendelser og fungere som talsperson overfor allmennheten og mediene for dette formålet.

Artikkel 15

Ytterligere harmonisering av verktøyer, metoder, framgangsmåter og retningslinjer for IKT-risikostyring

De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen og i samråd med Den europeiske unions cybersikkerhetsbyrå (ENISA) utarbeide felles utkast til tekniske reguleringsstandarder for å

a) spesifisere hvilke ytterligere elementer som skal inngå i retningslinjene, protokollene og verktøyene for IKT-sikkerhet som nevnt i artikkel 9 nr. 2, med henblikk på å garantere sikkerheten i nettverkene, sikre tilstrekkelige garantier mot inntrengning og misbruk av data, bevare tilgjengeligheten, autentisiteten, integriteten og fortroligheten til dataene, herunder krypteringsteknikker, og garantere en nøyaktig og rask dataoverføring uten større forstyrrelser og unødige forsinkelser,
b) utvikle ytterligere komponenter i den håndteringen av kontroll med tilgangsrettigheter som er nevnt i artikkel 9 nr. 4 bokstav c), og tilhørende personalpolitikk som angir tilgangsrettigheter, framgangsmåter for tildeling og tilbakekalling av rettigheter, overvåking av anormal atferd i forbindelse med IKT-risiko ved hjelp av egnede indikatorer, herunder mønstre for nettbruk, tidspunkter, IT-aktivitet og ukjent utstyr,
c) videreutvikle de ordningene som er angitt i artikkel 10 nr. 1, og som muliggjør umiddelbar påvisning av anormal virksomhet, og de kriteriene som er fastsatt i artikkel 10 nr. 2, for å utløse IKT-relaterte prosesser for påvisning av og håndtering av hendelser,
d) spesifisere nærmere komponentene i de retningslinjene for IKT-kontinuitet i virksomheten som er nevnt i artikkel 11 nr. 1,
e) spesifisere nærmere testingen av IKT-kontinuitet i virksomheten som nevnt i artikkel 11 nr. 6 for å sikre at slik testing tar behørig hensyn til scenarioer der kvaliteten på leveringen av en kritisk eller viktig funksjon forverres til et uakseptabelt nivå eller mislykkes, og tar behørig hensyn til den potensielle virkningen av insolvens eller andre feil forårsaket av en eventuell berørt tredjepartsleverandør av IKT-tjenester og, dersom det er relevant, de politiske risikoene i de respektive leverandørenes jurisdiksjoner,
f) spesifisere nærmere komponentene i planene for IKT-respons og -gjenoppretting som nevnt i artikkel 11 nr. 3,
g) spesifisere nærmere innholdet i og formatet for rapporten om gjennomgåelse av rammeverket for IKT-risikostyring som nevnt i artikkel 6 nr. 5.

Når de europeiske tilsynsmyndighetene utarbeider disse utkastene til tekniske reguleringsstandarder, skal de ta hensyn til den finansielle enhetens størrelse og generelle risikoprofil, samt til arten, omfanget og kompleksiteten av dens tjenester, aktiviteter og drift, samtidig som de skal ta behørig hensyn til eventuelle særtrekk som følge av den særskilte arten av aktiviteter i ulike sektorer for finansielle tjenester.

De europeiske tilsynsmyndighetene skal legge fram disse utkastene til tekniske reguleringsstandarder for Kommisjonen innen 17. januar 2024.

Kommisjonen delegeres myndighet til å utfylle denne forordningen ved å vedta de tekniske reguleringsstandardene som er nevnt i første ledd, i samsvar med artikkel 10–14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Artikkel 16

Forenklet rammeverk for IKT-risikostyring

1. Artikkel 5–15 i denne forordningen får ikke anvendelse på små verdipapirforetak uten innbyrdes forbindelser, betalingsinstitusjoner som er unntatt i henhold til direktiv (EU) 2015/2366, foretak som er unntatt i henhold til direktiv 2013/36/EU, og for hvilke medlemsstatene har besluttet ikke å anvende den muligheten som er nevnt i artikkel 2 nr. 4 i denne forordningen, e-pengeforetak som er unntatt i henhold til direktiv 2009/110/EF, og små tjenestepensjonsforetak.

   Med forbehold for første ledd skal enhetene som er oppført i første ledd,

   a) innføre og opprettholde et forsvarlig og dokumentert rammeverk for IKT-risikostyring som spesifiserer de ordningene og tiltakene som skal muliggjøre en rask, effektiv og omfattende styring av IKT-risiko, herunder for beskyttelse av relevante fysiske komponenter og infrastrukturer,
   b) kontinuerlig overvåke alle IKT-systemers sikkerhet og virkemåte,
   c) minimere virkningen av IKT-risiko gjennom bruk av forsvarlige, robuste og oppdaterte IKT-systemer, -protokoller og -verktøyer som er egnet til å støtte utførelsen av deres aktiviteter og levering av tjenester og i tilstrekkelig grad beskytte tilgjengeligheten, autentisiteten, integriteten og fortroligheten til dataene i nettverks- og informasjonssystemene,
   d) gjøre det mulig raskt å identifisere og oppdage kilder til IKT-risiko og avvik i nettverks- og informasjonssystemene, og raskt håndtere IKT-relaterte hendelser,
   e) identifisere stor avhengighet av tredjepartsleverandører av IKT-tjenester,
   f) sikre kontinuiteten for kritiske eller viktige funksjoner gjennom planer for kontinuitet i virksomheten og respons- og gjenopprettingstiltak, som minst omfatter tiltak for sikkerhetskopiering og gjenoppretting,
   g) regelmessig teste planene og tiltakene nevnt i bokstav f), samt effektiviteten av kontrollene som er gjennomført i samsvar med bokstav a) og c),
   h) gjennomføre, alt etter hva som er relevant, de relevante operasjonelle konklusjonene som følger av de testene som er nevnt i bokstav g), og av analysen etter hendelsen i IKT-risikovurderingsprosessen, og etter behov og IKT-risikoprofil utarbeide bevisstgjøringsprogrammer om IKT-sikkerhet og opplæring i digital operasjonell motstandsdyktighet for de ansatte og ledelsen.

2. Rammeverket for IKT-risikostyring nevnt i nr. 1 andre ledd bokstav a) skal dokumenteres og gjennomgås regelmessig og når det forekommer alvorlige IKT-relaterte hendelser i samsvar med tilsynsinstruksene. Rammeverket skal forbedres kontinuerlig på grunnlag av erfaringer fra gjennomføring og overvåking. En rapport om gjennomgåelsen av rammeverket for IKT-risikostyring skal legges fram for den vedkommende myndigheten når den anmoder om det.
3. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen og i samråd med ENISA utarbeide felles utkast til tekniske reguleringsstandarder for å

   a) spesifisere nærmere hvilke elementer som skal inngå i rammeverket for IKT-risikostyring nevnt i nr. 1 andre ledd bokstav a),
   b) spesifisere nærmere elementene i forbindelse med systemer, protokoller og verktøyer for å minimere virkningen av IKT-risiko som nevnt i nr. 1 andre ledd bokstav c), med henblikk på å garantere sikkerheten i nettverkene, sikre tilstrekkelige garantier mot inntrengning og misbruk av data og bevare tilgjengeligheten, autentisiteten, integriteten og fortroligheten til dataene,
   c) spesifisere nærmere komponentene i planene for IKT-kontinuitet i virksomheten som nevnt i nr. 1 andre ledd bokstav f),
   d) spesifisere nærmere reglene om testing av planer for kontinuitet i virksomheten og sikre at de kontrollene som er nevnt i nr. 1 andre ledd bokstav g), er effektive, og sikre at det ved slik testing tas behørig hensyn til scenarioer der kvaliteten på leveringen av en kritisk eller viktig funksjon forverres til et uakseptabelt nivå eller mislykkes,
   e) spesifisere nærmere innholdet i og formatet for rapporten om gjennomgåelsen av rammeverket for IKT-risikostyring som nevnt i nr. 2.

   Når de europeiske tilsynsmyndighetene utarbeider disse utkastene til tekniske reguleringsstandarder, skal de ta hensyn til den finansielle enhetens størrelse og generelle risikoprofil, samt til arten, omfanget og kompleksiteten av dens tjenester, aktiviteter og drift.

   De europeiske tilsynsmyndighetene skal legge fram disse utkastene til tekniske reguleringsstandarder for Kommisjonen innen 17. januar 2024.

Kommisjonen delegeres myndighet til å utfylle denne forordningen ved å vedta de tekniske reguleringsstandardene som er nevnt i første ledd, i samsvar med artikkel 10–14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Kapittel III

Håndtering, klassifisering og rapportering av IKT-relaterte hendelser

Artikkel 17

Prosess for håndtering av IKT-relaterte hendelser

1. De finansielle enhetene skal fastsette, opprette og gjennomføre en prosess for håndtering av IKT-relaterte hendelser for å påvise, håndtere og innberette IKT-relaterte hendelser.
2. De finansielle enhetene skal registrere alle IKT-relaterte hendelser og betydelige cybertrusler. De finansielle enhetene skal opprette hensiktsmessige framgangsmåter og prosesser for å sikre en ensartet og integrert overvåking, håndtering og oppfølging av IKT-relaterte hendelser, for å sikre at de grunnleggende årsakene identifiseres, dokumenteres og håndteres for å hindre at slike hendelser inntreffer.
3. Som ledd i prosessen for håndtering av IKT-relaterte hendelser nevnt i nr. 1
   a) innføres indikatorer for tidlig varsling,
   b) fastsettes framgangsmåter for å identifisere, spore, logge, kategorisere og klassifisere IKT-relaterte hendelser, alt etter deres prioritet og alvorlighetsgrad og i henhold til hvor kritiske de berørte tjenestene er, i samsvar med kriteriene fastsatt i artikkel 18 nr. 1,
   c) tildeles roller og ansvarsområder som må aktiveres for ulike IKT-relaterte hendelsestyper og IKT-relaterte scenarioer,
   d) utarbeides planer for kommunikasjon til ansatte, eksterne berørte parter og medier i samsvar med artikkel 14 og planer for underretning av kunder, planer for interne eskaleringsprosedyrer, herunder IKT-relaterte kundeklager, samt planer for formidling av opplysninger til finansielle enheter som opptrer som motparter, alt etter hva som er relevant,
   e) sikres det at alvorlige IKT-relaterte hendelser som et minimum blir rapportert til den relevante øverste ledelsen, og at ledelsesorganet som et minimum underrettes om alvorlige IKT-relaterte hendelser, med en redegjørelse for virkningene, tiltakene og ytterligere kontroller som skal fastsettes som følge av slike IKT-relaterte hendelser,
   f) treffes det framgangsmåter for tiltak i forbindelse med IKT-relaterte hendelser for å begrense virkningene og sikre at tjenestene raskt blir operasjonelle og sikre.

Artikkel 18

Klassifisering av IKT-relaterte hendelser og cybertrusler

1. De finansielle enhetene skal klassifisere IKT-relaterte hendelser og fastsette deres innvirkning på grunnlag av følgende kriterier:
   a) Antallet og/eller betydningen av kunder eller finansielle motparter som er berørt, og, dersom det er relevant, mengden eller antallet av transaksjoner som er berørt av den IKT-relaterte hendelsen, og om den IKT-relaterte hendelsen har påvirket omdømmet.
   b) Varigheten av den IKT-relaterte hendelsen, herunder tjenestens nedetid.
   c) Den geografiske spredningen med hensyn til områdene som påvirkes av den IKT-relaterte hendelsen, særlig dersom den påvirker mer enn to medlemsstater.
   d) Datatap som den IKT-relaterte hendelsen medfører, når det gjelder tilgjengeligheten, autentisiteten, integriteten eller fortroligheten til dataene.
   e) De berørte tjenestenes kritiske verdi, herunder den finansielle enhetens transaksjoner og virksomhet.
   f) De økonomiske virkningene, særlig direkte og indirekte kostnader og tap, av den IKT-relaterte hendelsen i både absolutte og relative tall.
2. De finansielle enhetene skal klassifisere cybertrusler som betydelige på grunnlag av de utsatte tjenestenes kritiske verdi, herunder den finansielle enhetens transaksjoner og virksomhet, antallet og/eller betydningen av kunder eller finansielle motparter som rammes, og den geografiske spredningen av de områdene som er utsatt for risiko.
3. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen og i samråd med ESB og ENISA utarbeide felles utkast til tekniske reguleringsstandarder som spesifiserer følgende nærmere:
   a) Kriteriene fastsatt i nr. 1, herunder vesentlighetsterskler for å fastslå alvorlige IKT-

relaterte hendelser eller, dersom det er relevant, alvorlige betalingsrelaterte operasjonelle hendelser eller sikkerhetshendelser, som er omfattet av rapporteringsforpliktelsen fastsatt i artikkel 19 nr. 1.

b) Kriteriene som skal anvendes av vedkommende myndigheter for å vurdere betydningen av alvorlige IKT-relaterte hendelser eller, dersom det er relevant, av alvorlige betalingsrelaterte operasjonelle hendelser eller sikkerhetshendelser, for berørte vedkommende myndigheter i andre medlemsstater, og de nærmere opplysningene i rapportene om alvorlige IKT-relaterte hendelser eller, dersom det er relevant, alvorlige betalingsrelaterte operasjonelle hendelser eller sikkerhetshendelser, som skal deles med andre vedkommende myndigheter i henhold til artikkel 19 nr. 6 og 7.

c) Kriteriene fastsatt i nr. 2 i denne artikkelen, herunder høye vesentlighetsterskler for å fastslå betydelige cybertrusler.

4. Når de europeiske tilsynsmyndighetene utarbeider det felles utkastet til tekniske reguleringsstandarder nevnt i nr. 3 i denne artikkelen, skal de ta hensyn til kriteriene fastsatt i artikkel 4 nr. 2, samt til internasjonale standarder, veiledninger og spesifikasjoner som ENISA har utarbeidet og offentliggjort, herunder, dersom det er relevant, spesifikasjoner for andre økonomiske sektorer. Ved anvendelse av kriteriene angitt i artikkel 4 nr. 2 skal de europeiske tilsynsmyndighetene ta behørig hensyn til behovet for at svært små, små og mellomstore bedrifter mobiliserer tilstrekkelige ressurser og kapasitet til å sikre at IKT-relaterte hendelser håndteres raskt.

De europeiske tilsynsmyndighetene skal framlegge disse utkastene til tekniske reguleringsstandarder for Kommisjonen innen 17. januar 2024.

Kommisjonen delegeres myndighet til å utfylle denne forordningen ved å vedta de tekniske reguleringsstandardene som er nevnt i nr. 3 i denne artikkelen, i samsvar med artikkel 10–14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Artikkel 19

Rapportering av alvorlige IKT-relaterte hendelser og frivillig underretning om betydelige cybertrusler

1. De finansielle enhetene skal rapportere alvorlige IKT-relaterte hendelser til den berørte vedkommende myndigheten nevnt i artikkel 46 i samsvar med nr. 4 i denne artikkelen.

Dersom en finansiell enhet er underlagt tilsyn av mer enn én nasjonal vedkommende myndighet som nevnt i artikkel 46, skal medlemsstatene utpeke én enkelt vedkommende myndighet som berørt vedkommende myndighet med ansvar for å ivareta de funksjonene og oppgavene som er fastsatt i denne artikkelen.

Kredittinstitusjoner som er klassifisert som betydelige i samsvar med artikkel 6 nr. 4 i forordning (EU) nr. 1024/2013, skal rapportere alvorlige IKT-relaterte hendelser til den relevante nasjonale vedkommende myndigheten som er utpekt i samsvar med artikkel 4 i direktiv 2013/36/EU, og som umiddelbart skal sende denne rapporten til Den europeiske sentralbank (ESB).

Med henblikk på første ledd skal finansielle enheter, etter å ha innhentet og analysert alle relevante opplysninger, utarbeide den første underretningen og de rapportene som er nevnt i nr. 4 i denne artikkelen ved bruk av malene nevnt i artikkel 20, og legge dem fram for den vedkommende myndigheten. Dersom det teknisk sett er umulig å sende inn den første underretningen ved bruk av malen, skal de finansielle enhetene meddele den vedkommende myndigheten om dette på annet vis.

Den første underretningen og rapportene nevnt i nr. 4 skal omfatte alle opplysninger som er nødvendige for at den vedkommende myndigheten skal kunne fastslå betydningen av den alvorlige IKT-relaterte hendelsen og vurdere mulige virkninger over landegrensene.

Uten at det berører den finansielle enhetens rapportering i henhold til første ledd til den berørte vedkommende myndigheten, kan medlemsstatene i tillegg bestemme at visse eller alle finansielle enheter også skal sende inn den første underretningen og hver rapport som er nevnt i nr. 4 i denne artikkelen ved bruk av malene nevnt i artikkel 20, til de vedkommende myndighetene eller enhetene for håndtering av digitale hendelser (CSIRT-enheter) som er utpekt eller etablert i samsvar med direktiv (EU) 2022/2555.

2. De finansielle enhetene kan på frivillig grunnlag underrette den berørte vedkommende myndigheten om betydelige cybertrusler når de anser trusselen som relevant for finanssystemet, tjenestebrukerne eller kundene. Den berørte vedkommende myndigheten kan gi slike opplysninger til andre relevante myndigheter som nevnt i nr. 6.

Kredittinstitusjoner som er klassifisert som betydelige i samsvar med artikkel 6 nr. 4 i forordning (EU) nr. 1024/2013, kan på frivillig grunnlag underrette om betydelige cybertrusler til den relevante nasjonale vedkommende myndigheten, som er utpekt i samsvar med artikkel 4 i direktiv 2013/36/EU, og som umiddelbart skal sende meldingen til Den europeiske sentralbank (ESB).

Medlemsstatene kan bestemme at disse finansielle enhetene som på frivillig grunnlag underretter i samsvar med første ledd, også kan videresende denne underretningen til de CSIRT-enhetene som er utpekt eller opprettet i samsvar med direktiv (EU) 2022/2555.

3. Dersom en alvorlig IKT-relatert hendelse inntreffer og har innvirkning på kundenes finansielle interesser, skal finansielle enheter uten unødig opphold og så snart de får kjennskap til den, informere sine kunder om den alvorlige IKT-relaterte hendelsen og om hvilke tiltak som er truffet for å begrense skadevirkningene av en slik hendelse.

   I tilfelle av en betydelig cybertrussel skal finansielle enheter, dersom det er relevant, informere de av kundene som potensielt er berørt av eventuelle egnede beskyttelsestiltak, som sistnevnte kan overveie å treffe.

4. De finansielle enhetene skal innen de tidsfristene som skal fastsettes i samsvar med artikkel 20 første ledd bokstav a) ii), legge fram følgende for den berørte vedkommende myndigheten:
   a) En første underretning.
   b) En foreløpig rapport etter den første underretningen nevnt i bokstav a) så snart statusen til den opprinnelige hendelsen har endret seg vesentlig, eller håndteringen av den alvorlige IKT-relaterte hendelsen har endret seg på grunnlag av nye tilgjengelige opplysninger, etterfulgt av, alt etter hva som er relevant, oppdaterte underretninger hver gang en relevant statusoppdatering er tilgjengelig, samt på særskilt anmodning fra den vedkommende myndigheten.
   c) En sluttrapport, når analysen av de grunnleggende årsakene er fullført, uavhengig av om de avbøtende tiltakene allerede er gjennomført, og når tallene for de faktiske virkningene foreligger og kan erstatte estimatene.

5. De finansielle enhetene kan i samsvar med unionsretten og nasjonal sektorspesifikk lovgivning utkontraktere rapporteringsforpliktelsene i henhold til denne artikkelen til en tredjepartsleverandør av tjenester. Ved en slik utkontraktering bærer den finansielle enheten det fulle ansvaret for å oppfylle kravene til rapportering av hendelser.

6. Når den vedkommende myndigheten mottar den første underretningen og hver rapport som nevnt i nr. 4, skal den til rett tid gi opplysninger om den alvorlige IKT-relaterte hendelsen til følgende mottakere, alt etter hva som er relevant, på grunnlag av deres respektive kompetanse:
   a) EBA, ESMA eller EIOPA.
   b) ESB når det gjelder finansielle enheter som nevnt i artikkel 2 nr. 1 bokstav a), b) og d).
   c) De vedkommende myndighetene, felles kontaktpunktene eller CSIRT-enhetene som er utpekt eller opprettet i samsvar med direktiv (EU) 2022/2555.
   d) De krisehåndteringsmyndighetene som nevnt i artikkel 3 i direktiv 2014/59/EU og Det felles krisehåndteringsråd med hensyn til de enhetene som er nevnt i artikkel 7 nr. 2 i europaparlaments- og rådsforordning (EU) nr. 806/2014[37], og med hensyn til enheter og grupper som nevnt i artikkel 7 nr. 4 bokstav b) og nr. 5 i forordning (EU) nr. 806/2014, dersom slike opplysninger gjelder hendelser som utgjør en risiko for å sikre kritiske funksjoner i henhold til artikkel 2 nr. 1 punkt 35) i direktiv 2014/59/EU.
   e) Andre relevante offentlige myndigheter i henhold til nasjonal rett.

7. Etter å ha mottatt opplysningene i samsvar med nr. 6 skal EBA, ESMA eller EIOPA og ESB, i samråd med ENISA og i samarbeid med den berørte vedkommende myndigheten, vurdere om den alvorlige IKT-relaterte hendelsen er relevant for vedkommende myndigheter i andre medlemsstater. Etter denne vurderingen skal EBA, ESMA eller EIOPA så snart som mulig underrette berørte vedkommende myndigheter i andre medlemsstater om dette. ESB skal underrette medlemmene av Det europeiske system av sentralbanker om spørsmål som har betydning for betalingssystemet. På grunnlag av denne underretningen skal de vedkommende myndighetene, dersom det er

---

[37] Europaparlaments- og rådsforordning (EU) nr. 806/2014 av 15. juli 2014 om fastsettelse av ensartede regler og en ensartet framgangsmåte for krisehåndtering av kredittinstitusjoner og visse verdipapirforetak innenfor rammen av en felles krisehåndteringsordning og et felles krisehåndteringsfond og om endring av forordning (EU) nr. 1093/2010 (EUT L 225 av 30.7.2014, s. 1).

relevant, treffe alle nødvendige tiltak for å ivareta finanssystemets umiddelbare stabilitet.

8. Underretningen som skal utarbeides av ESMA i henhold til nr. 7 i denne artikkelen, skal ikke berøre den vedkommende myndighetens ansvar for omgående å oversende nærmere opplysninger om den alvorlige IKT-relaterte hendelsen til den berørte myndigheten i vertsstaten, dersom en verdipapirsentral har betydelig virksomhet over landegrensene i vertsstaten, den alvorlige IKT-relaterte hendelsen sannsynligvis vil få alvorlige konsekvenser for vertsstatens finansmarkeder og det finnes samarbeidsordninger mellom vedkommende myndigheter som gjelder tilsyn med finansielle enheter.

Artikkel 20

Harmonisering av rapporteringsinnhold og -maler

De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen og i samråd med ENISA og ESB utarbeide

a) felles utkast til tekniske reguleringsstandarder for å
   i) fastsette innholdet i rapportene om alvorlige IKT-relaterte hendelser for å gjenspeile kriteriene fastsatt i artikkel 18 nr. 1 og innarbeide ytterligere elementer, som for eksempel nærmere opplysninger for å fastsette hvorvidt rapporteringen er relevant for andre medlemsstater, og hvorvidt den utgjør en alvorlig betalingsrelatert operasjonell hendelse eller sikkerhetshendelse,
   ii) fastsette fristene for den første underretningen og for hver rapport nevnt i artikkel 19 nr. 4,
   iii) fastsette innholdet i underretningen om betydelige cybertrusler.

   Når de europeiske tilsynsmyndighetene utarbeider disse utkastene til tekniske reguleringsstandarder, skal de ta hensyn til den finansielle enhetens størrelse og generelle risikoprofil samt til arten, omfanget og kompleksiteten av dens tjenester, aktiviteter og drift, og særlig med henblikk på å sikre at ulike tidsfrister i henhold til dette nummeret bokstav a) ii), alt etter hva som er relevant, kan gjenspeile særtrekk ved finanssektorene, uten at det berører opprettholdelsen av en konsekvent strategi for rapportering av IKT-relaterte hendelser i henhold til denne forordningen og direktiv (EU) 2022/2555. De europeiske tilsynsmyndighetene skal, dersom det er relevant, gi en begrunnelse dersom de avviker fra de metodene som er anvendt i forbindelse med det nevnte direktivet,

b) felles utkast til tekniske gjennomføringsstandarder for å fastsette standardskjemaer, standardmaler og standard framgangsmåter som de finansielle enhetene skal benytte for å rapportere en alvorlig IKT-relatert hendelse og for å underrette om en betydelig cybertrussel.

De europeiske tilsynsmyndighetene skal legge fram de felles utkastene til tekniske reguleringsstandarder som nevnt i første ledd bokstav a) og de felles utkastene til tekniske gjennomføringsstandarder som nevnt i første ledd bokstav b) for Kommisjonen innen 17. juli 2024.

Kommisjonen gis myndighet til å utfylle denne forordningen ved å vedta de felles tekniske reguleringsstandardene som er nevnt i første ledd bokstav a) i samsvar med artikkel 10–14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Kommisjonen gis myndighet til å vedta de felles tekniske gjennomføringsstandardene som er nevnt i første ledd bokstav b), i samsvar med artikkel 15 i henholdsvis forordning (EU) nr. 1093/2010, forordning (EU) nr. 1094/2010 og forordning (EU) nr. 1095/2010.

Artikkel 21

Sentralisering av rapportering av alvorlige IKT-relaterte hendelser

1. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen og i samråd med ESB og ENISA utarbeide en felles rapport som vurderer muligheten for ytterligere sentralisering av rapportering av hendelser gjennom opprettelse av et felles EU-knutepunkt for finansielle enheters rapportering av alvorlige IKT-relaterte hendelser. Den felles rapporten skal inneholde en undersøkelse av ulike måter for å lette strømmen av rapportering av IKT-relaterte hendelser, redusere tilknyttede kostnader og underbygge tematiske analyser med sikte på å øke den tilsynsmessige tilnærmingen.
2. Den felles rapporten nevnt i nr. 1 skal inneholde minst følgende:
   a) Forutsetninger for opprettelse av et felles EU-knutepunkt.
   b) Fordeler, begrensninger og risikoer, herunder risikoer forbundet med den høye konsentrasjonen av følsomme opplysninger.

c) Den nødvendige kapasiteten til å sikre interoperabilitet med hensyn til andre relevante rapporteringsordninger.
d) Elementer av den operasjonelle styringen.
e) Vilkår for medlemskap.
f) Tekniske ordninger for at finansielle enheter og nasjonale vedkommende myndigheter skal få tilgang til det felles EU-knutepunktet.
g) En foreløpig vurdering av finansielle kostnader som påløper ved opprettelse av den operasjonelle plattformen, som støtter det felles EU-knutepunktet, herunder den nødvendige ekspertisen.

3. De europeiske tilsynsmyndighetene skal legge fram rapporten nevnt i nr. 1 for Europaparlamentet, Rådet og Kommisjonen innen 17. januar 2025.

Artikkel 22

Tilbakemelding fra tilsynsmyndighetene

1. Uten at det berører de tekniske opplysningene, rådene eller tiltakene og den påfølgende oppfølgingen som CSIRT-enhetene, dersom det er relevant, i henhold til direktiv (EU) 2022/255 kan gi i samsvar med nasjonal rett, skal den vedkommende myndigheten, ved mottak av den første underretningen og hver rapport som nevnt i artikkel 19 nr. 4, bekrefte mottaket og, dersom det er mulig, innen rimelig tid gi relevant og forholdsmessig tilbakemelding eller veiledning på høyt nivå til den finansielle enheten, særlig ved å gjøre tilgjengelig alle relevante anonymiserte opplysninger og etterretninger om lignende trusler, og kan drøfte hvilke tiltak som har fått anvendelse på den finansielle enheten, og måter for å minimere og begrense de negative virkningene i finanssektoren. Uten at det berører tilbakemeldingen fra tilsynsmyndigheten, skal finansielle enheter fortsatt ha det fulle ansvaret for håndteringen og konsekvensene av IKT-relaterte hendelser som rapporteres i henhold til artikkel 19 nr. 1.
2. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen, i anonymisert og aggregert form, årlig rapportere om alvorlige IKT-relaterte hendelser, hvis nærmere opplysninger skal gis av vedkommende myndigheter i samsvar med artikkel 19 nr. 6, og som minst skal angi antallet av alvorlige IKT-relaterte hendelser, deres art og innvirkning på finansielle enheters eller kunders virksomhet, samt de utbedringstiltakene som er truffet, og kostnader som er påløpt.

De europeiske tilsynsmyndighetene skal utstede varsler og utarbeide statistikk på høyt nivå for å støtte vurderinger av IKT-trusler og IKT-sårbarhet.

Artikkel 23

Betalingsrelaterte operasjonelle hendelser eller sikkerhetshendelser knyttet til kredittinstitusjoner, betalingsinstitusjoner, ytere av kontoopplysningstjenester og e-pengeforetak

Kravene fastsatt i dette kapittelet får også anvendelse på betalingsrelaterte operasjonelle hendelser eller sikkerhetshendelser og på alvorlige betalingsrelaterte operasjonelle hendelser eller sikkerhetshendelser når det gjelder kredittinstitusjoner, betalingsinstitusjoner, ytere av kontoopplysningstjenester og e-pengeforetak.

Kapittel IV

Testing av digital operasjonell motstandsdyktighet

Artikkel 24

Generelle krav til testing av digital operasjonell motstandsdyktighet

1. Med henblikk på å vurdere beredskapen til å håndtere IKT-relaterte hendelser, til å identifisere svakheter, mangler og hull i den digitale operasjonelle motstandsdyktigheten og til å gjennomføre korrigerende tiltak omgående, skal andre finansielle enheter enn svært små bedrifter, samtidig som det tas hensyn til kriteriene fastsatt i artikkel 4 nr. 2, utarbeide, opprettholde og gjennomgå et forsvarlig og omfattende program for testing av den digitale operasjonelle motstandsdyktigheten som en integrert del av rammeverket for IKT-risikostyring som nevnt i artikkel 6.
2. Programmet for testing av digital operasjonell motstandsdyktighet skal omfatte en rekke vurderinger, tester, metoder, framgangsmåter og verktøyer som skal anvendes i samsvar med artikkel 25 og 26.
3. Når andre finansielle enheter enn svært små bedrifter gjennomfører det programmet for testing av digitale operasjonell motstandsdyktighet som er nevnt i nr. 1 i denne artikkelen, skal de følge en risikobasert tilnærming som tar hensyn til kriteriene fastsatt i artikkel 4 nr. 2, samtidig som det tas behørig hensyn til IKT-risikoens utvikling, eventuelle spesifikke risikoer som den berørte finansielle enheten er eller kan bli eksponert for, informa-

sjonsressursenes og tjenestenes kritiske verdi samt alle andre faktorer som den finansielle enheten anser som hensiktsmessige.

4. Andre finansielle enheter enn svært små bedrifter skal sikre at testene utføres av uavhengige parter, enten interne eller eksterne. Når testene utføres av en intern tester, skal finansielle enheter avsette tilstrekkelige ressurser og sikre at interessekonflikter unngås når testen utformes og gjennomføres.
5. Andre finansielle enheter enn svært små bedrifter skal fastsette framgangsmåter og retningslinjer for å prioritere, klassifisere og avhjelpe alle problemer som dukker opp under gjennomføringen av testene, og skal fastsette interne valideringsmetoder for å sikre at alle identifiserte svakheter, mangler eller hull avhjelpes fullt ut.
6. Andre finansielle enheter enn svært små bedrifter skal minst én gang i året sikre at det gjennomføres hensiktsmessige tester av alle IKT-systemer og -applikasjoner som støtter kritiske eller viktige funksjoner.

Artikkel 25

Testing av IKT-verktøyer og -systemer

1. Programmet for testing av digital operasjonell motstandsdyktighet nevnt i artikkel 24 skal, i samsvar med kriteriene fastsatt i artikkel 4 nr. 2, sikre gjennomføring av hensiktsmessige tester, som for eksempel sårbarhetsvurderinger og -analyser, analyser av åpen kildekode, vurderinger av nettsikkerhet, mangelanalyser, fysiske sikkerhetsvurderinger, spørreskjemaer og programvareløsninger for skanning, gjennomgåelse av kildekoder dersom det er mulig, scenariobaserte tester, kompatibilitetstesting, ytelsestesting, ende-til-ende-testing og penetrasjonstesting.
2. Verdipapirsentraler og sentrale motparter skal utføre sårbarhetsvurderinger før eventuell innføring eller gjeninnføring av nye eller eksisterende applikasjoner og infrastrukturkomponenter, og IKT-tjenester som støtter den finansielle enhetens kritiske eller viktige funksjoner.
3. Svært små bedrifter skal gjennomføre testene nevnt i nr. 1 ved å kombinere en risikobasert tilnærming med en strategisk planlegging av IKT-testing, samtidig som det tas behørig hensyn til behovet for å opprettholde en balansert tilnærming på den ene side mellom omfanget av ressursene og tiden som skal avsettes til IKT-testing som fastsatt i denne artikkelen, og på den annen side hastesituasjonen, risikotype og den kritiske verdien til informasjonsressursene og de leverte tjenestene, samt alle andre relevante faktorer, herunder den finansielle enhetens evne til å ta kalkulerte risikoer.

Artikkel 26

Avansert testing av IKT-verktøyer, -systemer og -prosesser basert på TLPT

1. Andre finansielle enheter enn enhetene som nevnt i artikkel 16 nr. 1 første ledd og svært små bedrifter, som er identifisert i samsvar med nr. 8 tredje ledd i denne artikkelen, skal minst hvert tredje år gjennomføre avansert testing ved hjelp av TLPT. På grunnlag av den finansielle enhetens risikoprofil og samtidig som det tas hensyn til de operasjonelle omstendighetene, kan den vedkommende myndigheten ved behov anmode den finansielle enheten om å redusere eller øke denne hyppigheten.
2. Hver trusselbasert penetrasjonstest skal omfatte flere eller alle kritiske eller viktige funksjoner hos en finansiell enhet, og skal utføres på produksjonssystemer som er i drift, og som støtter slike funksjoner.

   De finansielle enhetene skal identifisere alle relevante underliggende IKT-systemer, -prosesser og -teknologier som støtter kritiske eller viktige funksjoner og IKT-tjenester, herunder dem som støtter kritiske eller viktige funksjoner som er blitt utkontraktert eller kontrahert til tredjepartsleverandører av IKT-tjenester.

   De finansielle enhetene skal vurdere hvilke kritiske eller viktige funksjoner som må omfattes av TLPT. Resultatet av denne vurderingen skal bestemme det nøyaktige omfanget av TLPT og skal valideres av de vedkommende myndighetene.
3. Dersom tredjepartsleverandører av IKT-tjenester omfattes av TLPT, skal den finansielle enheten treffe nødvendige tiltak og sikkerhetstiltak for å sikre at slike tredjepartsleverandører av IKT-tjenester deltar i TLPT, og den skal til enhver tid ha det fulle ansvaret for å sikre at denne forordningen overholdes.
4. Med forbehold for nr. 2 første og andre ledd kan den finansielle enheten og en tredjepartsleverandør av IKT-tjenester, dersom tredjepartsleverandørens deltakelse i TLPT som nevnt i nr. 3 kan forventes å ha en negativ innvirkning på kvaliteten eller sikkerheten til

de tjenestene som tredjepartsleverandøren av IKT-tjenester leverer til kunder som er enheter som ikke er omfattet av denne forordningen, eller på fortroligheten til dataene som er knyttet til slike tjenester, skriftlig avtale at tredjepartsleverandøren av IKT-tjenester inngår kontraktsregulerte ordninger direkte med en ekstern tester med henblikk på å gjennomføre, under ledelse av én utpekt finansiell enhet, en samlet TLPT som omfatter flere finansielle enheter (felles testing), som tredjepartsleverandøren av IKT-tjenester leverer IKT-tjenester til.

Den felles testingen skal omfatte det relevante spekteret av IKT-tjenester som støtter kritiske eller viktige funksjoner, som de finansielle enhetene har kontrahert til den aktuelle tredjepartsleverandøren av IKT-tjenester. Den felles testingen skal betraktes som en TLPT utført av de finansielle enhetene som deltar i den felles testingen.

Antallet av finansielle enheter som deltar i den felles testingen, skal være behørig avpasset, samtidig som det tas hensyn til de aktuelle tjenestenes kompleksitet og type.

5. De finansielle enhetene skal, i samarbeid med tredjepartsleverandører av IKT-tjenester og andre involverte parter, herunder testere, men med unntak av de vedkommende myndighetene, anvende effektive risikostyringskontroller for å redusere risikoen for potensiell innvirkning på data, skade på eiendeler og forstyrrelser av kritiske eller viktige funksjoner, tjenester eller transaksjoner hos den finansielle enheten selv, hos dens motparter eller i finanssektoren.
6. Når testingen er avsluttet, og etter at rapporter og utbedringsplaner er godkjent, skal den finansielle enheten og, dersom det er relevant, de eksterne testerne gi den myndigheten som er utpekt i samsvar med nr. 9 eller 10, et sammendrag av de relevante resultatene, utbedringsplanene og dokumentasjonen som viser at TLPT er blitt utført i samsvar med kravene.
7. Myndighetene skal gi de finansielle enhetene en erklæring som bekrefter at testen ble utført i samsvar med de kravene som framgår av dokumentasjonen, for å gi mulighet for gjensidig anerkjennelse av trusselbaserte penetrasjonstester mellom de vedkommende myndighetene. Den finansielle enheten skal underrette den berørte vedkommende myndigheten om erklæringen, sammendraget av de relevante resultatene og utbedringsplanene.

Uten at det berører en slik erklæring, skal de finansielle enhetene alltid ha det fulle ansvaret for virkningen av de testene som er nevnt i nr. 4.

8. De finansielle enhetene skal inngå en kontrakt med testere med henblikk på å utføre en TLPT i samsvar med artikkel 27. Dersom de finansielle enhetene bruker interne testere for å utføre en TLPT, skal de inngå kontrakt med eksterne testere ved hver tredje test.

   Kredittinstitusjoner som er klassifisert som betydelige i samsvar med artikkel 6 nr. 4 i forordning (EU) nr. 1024/2013, skal bare bruke eksterne testere i samsvar med artikkel 27 nr. 1 bokstav a)–e).

   De vedkommende myndighetene skal identifisere de finansielle enhetene som er pålagt å utføre en TLPT, samtidig som det tas hensyn til kriteriene i artikkel 4 nr. 2, på grunnlag av en vurdering av følgende:
   a) Påvirkningsfaktorer, særlig i hvilket omfang de tjenestene som ytes, og de aktivitetene som utføres av den finansielle enheten, påvirker finanssektoren.
   b) Eventuelle problemer med den finansielle stabiliteten, herunder den finansielle enhetens systemiske karakter på unionsplan eller nasjonalt plan, alt etter hva som er relevant.
   c) Den finansielle enhetens spesifikke IKT-risikoprofil, grad av IKT-modenhet eller tekniske funksjoner.
9. Medlemsstatene kan utpeke en felles offentlig myndighet i finanssektoren som ansvarlig for TLPT-relaterte spørsmål i finanssektoren på nasjonalt plan og overdra all myndighet og alle oppgaver med henblikk på dette.
10. Dersom det ikke er utpekt noen myndighet i samsvar med nr. 9 i denne artikkelen, og uten at det berører myndigheten til å identifisere de finansielle enhetene som er pålagt å utføre en TLPT, kan en vedkommende myndighet delegere utøvelsen av visse eller alle de oppgavene som er nevnt i denne artikkelen og i artikkel 27, til en annen nasjonal myndighet i finanssektoren.
11. De europeiske tilsynsmyndighetene skal, etter avtale med ESB, utarbeide felles utkast til tekniske reguleringsstandarder i samsvar med TIBER-EU-rammeverket for å spesifisere nærmere
    a) de kriteriene som brukes ved anvendelse av nr. 8 andre ledd,
    b) kravene og standardene for anvendelse av interne testere,

c) kravene i forbindelse med
   i) omfanget av den TLPT-en som nevnt i nr. 2,
   ii) den testmetoden og den tilnærmingen som skal følges i hver enkelt fase av testingen,
   iii) resultatene av testingen og avslutnings- og utbedringsfaser,
d) den typen av tilsynssamarbeid og annet relevant samarbeid som er nødvendig for gjennomføring av TLPT, og for å lette gjensidig anerkjennelse av en slik testing når det gjelder finansielle enheter som driver virksomhet i mer enn én medlemsstat, slik at det sikres et passende nivå av tilsynsmessig deltakelse og en fleksibel gjennomføring for å ta hensyn til særtrekk ved finansielle delsektorer eller lokale finansmarkeder.

Når de europeiske tilsynsmyndighetene utarbeider disse utkastene til tekniske reguleringsstandarder, skal de ta behørig hensyn til eventuelle særtrekk som oppstår som følge av den særskilte arten av aktiviteter i ulike sektorer for finansielle tjenester.

De europeiske tilsynsmyndighetene skal legge fram disse utkastene til tekniske reguleringsstandarder for Kommisjonen innen 17. juli 2024.

Kommisjonen delegeres myndighet til å utfylle denne forordningen ved å vedta de tekniske reguleringsstandardene som er nevnt i første ledd, i samsvar med artikkel 10–14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Artikkel 27

Krav til testere ved utførelse av TLPT

1. De finansielle enhetene skal bare bruke testere for å utføre en TLPT som
   a) er de mest egnede, og som har det beste omdømmet,
   b) har teknisk og organisatorisk kapasitet samt spesifikk ekspertise med hensyn til trusseletterretning, penetrasjonstesting og red team-testing,
   c) er sertifisert av et akkrediteringsorgan i en medlemsstat eller overholder formelle atferdsnormer eller etiske rammer,
   d) avgir en uavhengig forsikring eller en revisjonsberetning i forbindelse med forsvarlig risikostyring i forbindelse med utførelse av TLPT, herunder behørig beskyttelse av den finansielle enhetens fortrolige opplysninger og erstatning for den finansielle enhetens operasjonelle risikoer,
   e) er behørig og fullt ut dekket av relevante yrkesansvarsforsikringer, herunder mot risiko for forsømmelse og uaktsomhet.
2. Når de finansielle enhetene bruker interne testere, skal de i tillegg til kravene i nr. 1, sikre at følgende vilkår er oppfylt:
   a) En slik bruk er godkjent av den berørte vedkommende myndigheten eller av den felles offentlige myndigheten som er utpekt i samsvar med artikkel 26 nr. 9 og 10.
   b) Den berørte vedkommende myndigheten har verifisert at den finansielle enheten har avsatt tilstrekkelig med ressurser og sikret at interessekonflikter unngås når testen utformes og gjennomføres.
   c) Formidleren av trusseletterretninger er ikke en del av den finansielle enheten.
3. De finansielle enhetene skal sikre at kontrakter inngått med eksterne testere krever en forsvarlig forvaltning av resultatene av TLPT, og at enhver databehandling av disse, herunder enhver form for generering, lagring, aggregering, utkast, rapport, kommunikasjon eller destruksjon, ikke medfører risiko for den finansielle enheten.

Kapittel V

Styring av IKT-tredjepartsrisiko

Avsnitt I

Sentrale prinsipper for en forsvarlig styring av IKT-tredjepartsrisiko

Artikkel 28

Generelle prinsipper

1. De finansielle enhetene skal styre IKT-tredjepartsrisiko som en integrert del av IKT-risiko innenfor sitt rammeverk for IKT-risikostyring som nevnt i artikkel 6 nr. 1, og i samsvar med følgende prinsipper:
   a) De finansielle enhetene som har inngått kontraktsregulerte ordninger om bruk av IKT-tjenester for å drive sin virksomhet, skal til enhver tid ha det fulle ansvaret for å overholde og oppfylle alle forpliktelser i henhold til denne forordningen og gjeldende regelverk for finansielle tjenester.
   b) De finansielle enhetenes styring av IKT-tredjepartsrisiko skal gjennomføres med hensyn til forholdsmessighetsprinsippet, samtidig som det tas hensyn til

i) karakteren, omfanget, kompleksiteten og betydningen av IKT-relatert avhengighet,
ii) de risikoene som oppstår som følge av kontraktsregulerte ordninger om bruk av IKT-tjenester som er inngått med tredjepartsleverandører av IKT-tjenester, samtidig som det tas hensyn til den kritiske verdien eller betydningen av den aktuelle tjenesten, prosessen eller funksjonen, og den potensielle innvirkningen på kontinuiteten og tilgjengeligheten til finansielle tjenester og aktiviteter, på individuelt nivå og på konsernnivå.

2. Som en del av sitt rammeverk for IKT-risikostyring skal andre finansielle enheter enn de enhetene som er nevnt i artikkel 16 nr. 1 første ledd, og svært små bedrifter, vedta og regelmessig gjennomgå en strategi for IKT-tredjepartsrisiko, samtidig som det tas hensyn til strategien med flere ulike leverandører som nevnt i artikkel 6 nr. 9, dersom det er relevant. Strategien for IKT-tredjepartsrisiko skal omfatte retningslinjer for bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner levert av tredjepartsleverandører av IKT-tjenester, og skal gjelde på individuelt grunnlag og, dersom det er relevant, på delkonsolidert og konsolidert grunnlag. Ledelsesorganet skal, på grunnlag av en vurdering av den finansielle enhetens generelle risikoprofil og omfanget og kompleksiteten av forretningstjenestene, regelmessig gjennomgå de risikoene som er identifisert med hensyn til kontraktsregulerte ordninger om bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner.
3. Som en del av sitt rammeverk for IKT-risikostyring skal de finansielle enhetene opprettholde og oppdatere et register over opplysninger på enhetsnivå, delkonsolidert nivå og konsolidert nivå om alle kontraktsregulerte ordninger om bruk av IKT-tjenester levert av tredjepartsleverandører av IKT-tjenester.

   De kontraktsregulerte ordningene nevnt i første ledd skal være behørig dokumentert, og det skal skjelnes mellom dem som omfatter IKT-tjenester som støtter kritiske eller viktige funksjoner, og dem som ikke gjør det.

   De finansielle enhetene skal minst én gang i året rapportere til de vedkommende myndighetene om antall nye ordninger om bruk av IKT-tjenester, kategoriene av tredjepartsleverandører av IKT-tjenester, typen av kontraktsregulerte ordninger og de IKT-tjenestene og -funksjonene som leveres.

   De finansielle enhetene skal på anmodning gi den vedkommende myndigheten tilgang til det fullstendige registeret over opplysninger eller angitte deler av det, sammen med alle opplysninger som anses som nødvendige for et effektivt tilsyn med den finansielle enheten.

   De finansielle enhetene skal i god tid underrette den vedkommende myndigheten om enhver planlagt kontraktsregulert ordning om bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner, samt når en funksjon er blitt kritisk eller viktig.
4. Før de finansielle enhetene inngår en kontraktsregulert ordning om bruk av IKT-tjenester, skal de
   a) vurdere om den kontraktsregulerte ordningen omfatter bruken av IKT-tjenester som støtter en kritisk eller viktig funksjon,
   b) vurdere om tilsynsvilkårene for utkontraktering er oppfylt,
   c) identifisere og vurdere alle relevante risikoer i forbindelse med den kontraktsregulerte ordningen, herunder muligheten for at en slik kontraktsregulert ordning kan bidra til å styrke IKT-konsentrasjonsrisikoen som nevnt i artikkel 29,
   d) foreta en aktsomhetsvurdering av potensielle tredjepartsleverandører av IKT-tjenester og under alle utvelgelses- og vurderingsprosessene sikre at tredjepartsleverandøren av IKT-tjenester er egnet,
   e) identifisere og vurdere interessekonflikter som den kontraktsregulerte ordningen kan forårsake.
5. De finansielle enhetene kan bare inngå kontraktsregulerte ordninger med tredjepartsleverandører av IKT-tjenester som overholder egnede standarder om informasjonssikkerhet. Når slike kontraktsregulerte ordninger gjelder kritiske eller viktige funksjoner, skal finansielle enheter, før de inngår ordningene, ta behørig hensyn til hvorvidt tredjepartsleverandører av IKT-tjenester bruker de nyeste standardene om informasjonssikkerhet av høyeste kvalitet.
6. Når finansielle enheter utøver retten til tilgang, inspeksjon og revisjon overfor tredjepartsleverandøren av IKT-tjenester, skal de på grunnlag av en risikobasert tilnærming på forhånd fastsette hyppigheten av revisjoner og inspeksjoner samt de områdene som skal revideres, gjennom å følge allment anerkjente revisjonsstandarder i tråd med eventuelle til-

synsinstrukser om bruk og innarbeiding av slike revisjonsstandarder.

Dersom kontraktsregulerte ordninger inngått med tredjepartsleverandører av IKT-tjenester om bruk av IKT-tjenester medfører høy teknisk kompleksitet, skal den finansielle enheten kontrollere at revisorer, enten interne eller eksterne, eller et utvalg av revisorer, besitter de nødvendige ferdighetene og den nødvendige kunnskapen for å kunne utføre de relevante revisjonene og vurderingene på en effektiv måte.

7. De finansielle enhetene skal sikre at kontraktsregulerte ordninger om bruk av IKT-tjenester kan sies opp i alle følgende situasjoner:
   a) Tredjepartsleverandøren av IKT-tjenester begår en vesentlig overtredelse av gjeldende lover, forskrifter eller kontraktsvilkår.
   b) Forhold som er avdekket under overvåkingen av IKT-tredjepartsrisiko, og som anses for å kunne endre ytelsen til de funksjonene som tilbys gjennom den kontraktsregulerte ordningen, herunder vesentlige endringer som påvirker ordningen eller situasjonen for tredjepartsleverandøren av IKT-tjenester.
   c) Tredjepartsleverandøren av IKT-tjenester har vist svakheter når det gjelder sin samlede IKT-risikostyring, og særlig hvordan den sikrer tilgjengeligheten, autentisiteten, integriteten og fortroligheten til dataene, enten det dreier seg om personopplysninger eller på annen måte sensitive opplysninger eller andre opplysninger enn personopplysninger.
   d) Dersom den vedkommende myndigheten ikke lenger kan føre effektivt tilsyn med den finansielle enheten som følge av vilkårene i eller omstendighetene knyttet til respektive kontraktsregulerte ordninger.
8. For IKT-tjenester som støtter kritiske eller viktige funksjoner, skal finansielle enheter innføre exit-strategier. Exit-strategiene skal ta hensyn til risikoer som kan oppstå hos tredjepartsleverandører av IKT-tjenester, særlig en mulig svikt fra deres side, en forringelse av kvaliteten på de IKT-tjenestene som leveres, eventuelle driftsforstyrrelser på grunn av upassende eller mislykket levering av IKT-tjenester eller eventuelle vesentlige risikoer som oppstår i forbindelse med en hensiktsmessig og kontinuerlig anvendelse av den aktuelle IKT-tjenesten, eller oppsigelse av kontraktsregulerte ordninger med tredjepartsleverandører av IKT-tjenester i en av de situasjonene som er nevnt i nr. 7.

   De finansielle enhetene skal sikre at de kan si opp kontraktsregulerte ordninger uten
   a) at deres forretningsvirksomhet avbrytes,
   b) at overholdelsen av de forskriftsmessige kravene begrenses,
   c) at kontinuiteten og kvaliteten på de tjenestene som leveres til kunder, lider skade.

   Exit-planene skal være omfattende og dokumenterte, og de skal, i samsvar med kriteriene fastsatt i artikkel 4 nr. 2, være tilstrekkelig testet samt være gjennomgått regelmessig.

   De finansielle enhetene skal identifisere alternative løsninger og utarbeide overgangsplaner slik at de kan frata tredjepartsleverandøren av IKT-tjenester de kontraherte IKT-tjenestene og de relevante dataene, og på en sikker og fullstendig måte overføre dem til alternative leverandører eller reintegrere dem internt.

   De finansielle enhetene skal innføre egnede beredskapstiltak for å opprettholde kontinuitet i virksomheten dersom omstendighetene nevnt i første ledd inntreffer.
9. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen utarbeide utkast til tekniske gjennomføringsstandarder for å fastsette standardmaler for det registeret over opplysninger som er nevnt i nr. 3, herunder opplysninger som er felles for alle kontraktsregulerte ordninger om bruk av IKT-tjenester. De europeiske tilsynsmyndighetene skal framlegge disse utkastene til tekniske gjennomføringsstandarder for Kommisjonen innen 17. januar 2024.

   Kommisjonen gis myndighet til å vedta de tekniske gjennomføringsstandardene som er nevnt i første ledd, i samsvar med artikkel 15 i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

10. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen utarbeide utkast til tekniske reguleringsstandarder for nærmere å angi det detaljerte innholdet i retningslinjene nevnt i nr. 2 i forbindelse med de kontraktsregulerte ordningene om bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner som leveres av tredjepartsleverandører av IKT-tjenester.

    Når de europeiske tilsynsmyndighetene utarbeider disse utkastene til tekniske reguleringsstandarder, skal de ta hensyn til den finansielle enhetens størrelse og generelle risikoprofil, samt til arten, omfanget og kompleksiteten av dens tjenester, aktiviteter og drift. De

europeiske tilsynsmyndighetene skal legge fram disse utkastene til tekniske reguleringsstandarder for Kommisjonen innen 17. januar 2024.

Kommisjonen delegeres myndighet til å utfylle denne forordningen ved å vedta de tekniske reguleringsstandardene som er nevnt i første ledd, i samsvar med artikkel 10–14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Artikkel 29

Foreløpig vurdering av IKT-konsentrasjonsrisiko på enhetsnivå

1. Når finansielle enheter foretar identifisering og vurdering av risikoene nevnt i artikkel 28 nr. 4 bokstav c), skal de også ta hensyn til om den planlagte inngåelsen av en kontraktsregulert ordning i forbindelse med IKT-tjenester som støtter kritiske eller viktige funksjoner, vil føre til noe av følgende:
   a) Kontrakt med en tredjepartsleverandør av IKT-tjenester som ikke er lett å erstatte.
   b) Inngåelse av flere kontraktsregulerte ordninger for levering av IKT-tjenester som støtter kritiske eller viktige funksjoner, med den samme tredjepartsleverandøren av IKT-tjenester eller med tredjepartsleverandører av IKT-tjenester som har tette forbindelser til denne.

   De finansielle enhetene skal vurdere fordelene og kostnadene ved alternative løsninger, som for eksempel bruken av ulike tredjepartsleverandører av IKT-tjenester, samtidig som det tas hensyn til om og hvordan planlagte løsninger svarer til de forretningsmessige behovene og målene som er fastsatt i deres strategi for digital motstandsdyktighet.
2. Dersom de kontraktsregulerte ordningene om bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner, omfatter muligheten for at en tredjepartsleverandør av IKT-tjenester gir IKT-tjenester som støtter en kritisk eller viktig funksjon, i underentreprise til andre tredjepartsleverandører av IKT-tjenester, skal de finansielle enhetene vurdere fordeler og risiko som kan oppstå i forbindelse med en slik underentreprise, særlig når det gjelder en IKT-underleverandør som er etablert i et tredjeland.

   Dersom kontraktsregulerte ordninger gjelder IKT-tjenester som støtter kritiske eller viktige funksjoner, skal de finansielle enhetene ta behørig hensyn til de bestemmelsene i insolvensretten som får anvendelse dersom tredjepartsleverandøren av IKT-tjenester går konkurs, samt eventuelle begrensninger som kan oppstå i forbindelse med den presserende gjenopprettingen av den finansielle enhetens data.

   Dersom det inngås kontraktsregulerte ordninger om bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner, med en tredjepartsleverandør av IKT-tjenester som er etablert i et tredjeland, skal de finansielle enhetene, i tillegg til de forholdene som er nevnt i andre ledd, også vurdere overholdelsen av Unionens personvernregler og den faktiske overholdelsen av retten i dette tredjelandet

   Dersom de kontraktsregulerte ordningene om bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner, omfatter underentreprise, skal de finansielle enhetene vurdere om og hvordan potensielt lange eller komplekse kjeder av underentrepriser kan påvirke deres evne til fullt ut å overvåke de kontraherte funksjonene og den vedkommende myndighetens evne til å føre effektivt tilsyn med den finansielle enheten i denne forbindelse.

Artikkel 30

Viktige kontraktsbestemmelser

1. Rettighetene og forpliktelsene for den finansielle enheten og tredjepartsleverandøren av IKT-tjenester skal være klart fordelt og fastsatt skriftlig. Den fullstendige kontrakten skal omfatte tjenestenivåavtaler og dokumenteres i ett skriftlig dokument som partene skal ha tilgang til på papir, eller i et dokument i et annet nedlastbart, varig og tilgjengelig format.
2. De kontraktsregulerte ordningene om bruk av IKT-tjenester skal inneholde minst følgende elementer:
   a) En klar og fullstendig beskrivelse av alle funksjoner og IKT-tjenester som skal leveres av tredjepartsleverandøren av IKT-tjenester, med angivelse av om underentreprise av en IKT-tjeneste som støtter en kritisk eller viktig funksjon, eller vesentlige deler av denne, er tillatt, og, dersom dette er tilfellet, de vilkårene som gjelder for en slik underentreprise.
   b) De stedene, nærmere bestemt regioner eller land, der de funksjonene eller IKT-tjenestene som er kontrahert eller gitt i underentreprise, skal leveres, og der dataene skal behandles, herunder lagringsstedet, og kravet til tredjepartsleverandøren av IKT-tjenester om å underrette den finansielle

enheten på forhånd dersom den planlegger å endre disse stedene.

c) Bestemmelser om tilgjengelighet, autentisitet, integritet og fortrolighet i forbindelse med vern av data, herunder personopplysninger.

d) Bestemmelser om å sikre tilgang, gjenoppretting og tilbakeføring i et lett tilgjengelig format av personopplysninger og andre opplysninger enn personopplysninger, som behandles av den finansielle enheten ved insolvens, krisehåndtering eller opphør av virksomheten til tredjepartsleverandøren av IKT-tjenester, eller ved oppsigelse av kontraktsregulerte ordninger.

e) En beskrivelse av tjenestenivåer, herunder oppdateringer og revideringer av disse.

f) Forpliktelsen for tredjepartsleverandøren av IKT-tjenester om å yte bistand til den finansielle enheten uten ekstra kostnad, eller til en kostnad som fastsettes på forhånd, dersom det oppstår en IKT-hendelse som er knyttet til den IKT-tjenesten som leveres til den finansielle enheten.

g) Forpliktelsen for tredjepartsleverandøren av IKT-tjenester om å samarbeide fullt ut med den finansielle enhetens vedkommende myndigheter og krisehåndteringsmyndigheter, herunder personer som de har utpekt.

h) Oppsigelsesrett og tilhørende minste oppsigelsesfrist for oppsigelse av de kontraktsregulerte ordningene i samsvar med forventningene til vedkommende myndigheter og krisehåndteringsmyndigheter.

i) Vilkårene for deltakelse av tredjepartsleverandører av IKT-tjenester i de finansielle enhetenes bevisstgjøringsprogrammer om IKT-sikkerhet og opplæring i digital operasjonell motstandsdyktighet i samsvar med artikkel 13 nr. 6.

3. De kontraktsregulerte ordningene om bruk av IKT-tjenester som støtter kritiske eller viktige funksjoner, skal i tillegg til elementene nevnt i nr. 2 minst omfatte følgende:

a) En fullstendig beskrivelse av tjenestenivåer, herunder oppdateringer og revideringer av disse med nøyaktige kvantitative og kvalitative ytelsesmål innenfor de avtalte tjenestenivåene, slik at den finansielle enheten kan overvåke IKT-tjenester på en effektiv måte og gjøre det mulig å iverksette egnede korrigerende tiltak uten unødig forsinkelse når de avtalte tjenestenivåene ikke oppnås.

b) Oppsigelsesfrister og rapporteringsforpliktelser for tredjepartsleverandøren av IKT-tjenester overfor den finansielle enheten, herunder underretning om enhver utvikling som kan ha en vesentlig innvirkning på hvorvidt tredjepartsleverandøren av IKT-tjenester har evnen til å levere IKT-tjenester som støtter kritiske eller viktige funksjoner, på en effektiv måte og i tråd med avtalte tjenestenivåer.

c) Krav til tredjepartsleverandøren av IKT-tjenester om å gjennomføre og teste beredskapsplaner for virksomheten og innføre IKT-sikkerhetstiltak, IKT-verktøyer og IKT-retningslinjer som gir et hensiktsmessig sikkerhetsnivå for den finansielle enhetens levering av tjenester i tråd med dens regelverk.

d) Forpliktelsen for tredjepartsleverandøren av IKT-tjenester om å delta i og fullt ut samarbeide om den finansielle enhetens TLPT som nevnt i artikkel 26 og 27.

e) Retten til fortløpende å overvåke det ytelsesnivået som tredjepartsleverandøren av IKT-tjenester leverer, hvilket innebærer følgende:

i) Ubegrenset rett til tilgang, inspeksjon og revisjon for den finansielle enheten, eller en utpekt tredjepart, og for den vedkommende myndigheten, og retten til å ta kopier av relevant dokumentasjon på stedet dersom de er av avgjørende betydning for virksomheten hos tredjepartsleverandøren av IKT-tjenester, hvis faktiske utøvelse ikke hindres eller begrenses av andre kontraktsregulerte ordninger eller gjennomføringsstrategier.

ii) Retten til å komme til enighet om alternative sikkerhetsnivåer dersom andre kunders rettigheter påvirkes.

iii) Forpliktelsen for tredjepartsleverandøren av IKT-tjenester om å samarbeide fullt ut under de stedlige inspeksjonene og revisjonene som utføres av de vedkommende myndighetene, hovedovervåkeren, den finansielle enheten eller en utpekt tredjepart.

iv) Forpliktelsen om å gi nærmere opplysninger om omfanget, de framgangsmåtene som skal følges, og hyppigheten av slike inspeksjoner og revisjoner.

f) Exit-strategier, særlig innføring av en obligatorisk passende overgangsperiode,

i) under hvilken tredjepartsleverandøren av IKT-tjenester kommer til å fortsette å

levere de respektive funksjonene eller IKT-tjenestene med sikte på å redusere risikoen for forstyrrelser hos den finansielle enheten eller for å sikre en effektiv krisehåndtering og omstrukturering av denne,

ii) slik at den finansielle enheten kan bytte til en annen tredjepartsleverandør av IKT-tjenester eller bytte til interne løsninger som er forenlige med den leverte tjenestens kompleksitet.

Som unntak fra bokstav e) kan tredjepartsleverandøren av IKT-tjenester og den finansielle enheten som er en svært liten bedrift, bli enige om at den finansielle enhetens rett til tilgang, inspeksjon og revisjon kan delegeres til en uavhengig tredjepart som utpekes av tredjepartsleverandøren av IKT-tjenester, og at den finansielle enheten når som helst kan anmode tredjeparten om opplysninger og garantier i forbindelse med de resultatene som tredjepartsleverandøren av IKT-tjenester oppnår.

4. Når finansielle enheter og tredjepartsleverandører av IKT-tjenester forhandler om kontraktsregulerte ordninger, skal de vurdere å bruke standardavtalevilkår utarbeidet av offentlige myndigheter for bestemte tjenester.
5. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen utarbeide utkast til tekniske reguleringsstandarder for å spesifisere nærmere de elementene som er nevnt i nr. 2 bokstav a), og som en finansiell enhet må fastsette og vurdere når den gir IKT-tjenester som støtter kritiske eller viktige funksjoner, i underentreprise.

Når de europeiske tilsynsmyndighetene utarbeider disse utkastene til tekniske reguleringsstandarder, skal de ta hensyn til den finansielle enhetens størrelse og generelle risikoprofil, samt til arten, omfanget og kompleksiteten av dens tjenester, aktiviteter og drift.

De europeiske tilsynsmyndighetene skal legge fram disse utkastene til tekniske reguleringsstandarder for Kommisjonen innen 17. juli 2024.

Kommisjonen delegeres myndighet til å utfylle denne forordningen ved å vedta de tekniske reguleringsstandardene som er nevnt i første ledd, i samsvar med artikkel 10–14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Avsnitt II

Tilsynsramme for kritiske tredjepartsleverandører av IKT-tjenester

Artikkel 31

Utpeking av kritiske tredjepartsleverandører av IKT-tjenester

1. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen og på anmodning fra overvåkingsforumet nedsatt i henhold til artikkel 32 nr. 1
   a) utpeke tredjepartsleverandører av IKT-tjenester som er kritiske for finansielle enheter, etter en vurdering som tar hensyn til kriteriene angitt i nr. 2,
   b) oppnevne som hovedovervåker for hver kritisk tredjepartsleverandør av IKT-tjenester den europeiske tilsynsmyndigheten som er ansvarlig i samsvar med forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 eller (EU) nr. 1095/2010, for de finansielle enhetene som til sammen har den største andelen av de samlede eiendelene av verdien av de samlede eiendelene for alle de finansielle enhetene som benytter seg av tjenestene fra den relevante kritiske tredjepartsleverandøren av IKT-tjenester, slik det framgår av summen av de individuelle balansene for disse finansielle enhetene.
2. Den utpekingen som er nevnt i nr. 1 bokstav a), skal i forbindelse med IKT-tjenester levert av tredjepartsleverandøren av IKT-tjenester baseres på alle følgende kriterier:
   a) Den systemiske virkningen på stabiliteten, kontinuiteten eller kvaliteten på leveringen av finansielle tjenester dersom den berørte tredjepartsleverandøren av IKT-tjenester skulle rammes av omfattende driftsforstyrrelser, slik at denne ikke kan levere sine tjenester, samtidig som det tas hensyn til antallet av finansielle enheter og den samlede verdien av eiendeler hos de finansielle enhetene som den berørte tredjepartsleverandøren av IKT-tjenester leverer tjenester til.
   b) Den systemiske karakteren eller betydningen av de finansielle enhetene som er avhengige av den berørte tredjepartsleverandøren av IKT-tjenester, vurdert i samsvar med følgende parametrer:
      i) Antallet av globalt systemviktige institusjoner eller andre systemviktige institusjoner som er avhengige av den aktuelle

tredjepartsleverandøren av IKT-tjenester.

ii) Den gjensidige avhengigheten mellom de globalt systemviktige institusjonene eller de andre systemviktige institusjonene nevnt i punkt i) og andre finansielle enheter, herunder situasjoner der de globalt systemviktige institusjonene eller de andre systemviktige institusjonene leverer finansielle infrastrukturtjenester til andre finansielle enheter.

c) Finansielle enheters avhengighet av tjenestene som leveres av den berørte tredjepartsleverandøren av IKT-tjenester i forbindelse med kritiske eller viktige funksjoner hos finansielle enheter som i siste instans involverer den samme tredjepartsleverandøren av IKT-tjenester, uavhengig av om finansielle enheter er avhengige av disse tjenestene direkte eller indirekte, gjennom underleverandøravtaler.

d) Graden av erstattbarhet hos tredjepartsleverandøren av IKT-tjenester, samtidig som det tas hensyn til følgende parametrer:

i) Mangelen på reelle alternativer, også delvis, på grunn av det begrensede antallet av tredjepartsleverandører av IKT-tjenester som er aktive på et bestemt marked, eller markedsandelen for den berørte tredjepartsleverandøren av IKT-tjenester, eller den tekniske kompleksiteten eller den avanserte karakteren, herunder i forbindelse med eventuell proprietær teknologi, eller særtrekkene ved organisasjonen eller virksomheten til tredjepartsleverandøren av IKT-tjenester.

ii) Vanskeligheter i forbindelse med delvis eller fullstendig overføring av relevante data og arbeidsbelastninger fra den berørte tredjepartsleverandøren av IKT-tjenester til en annen tredjepartsleverandør av IKT-tjenester, enten på grunn av betydelige finansielle kostnader, tid eller andre ressurser som overføringsprosessen kan medføre, eller på grunn av økt IKT-risiko eller andre operasjonelle risikoer som den finansielle enheten kan bli eksponert for gjennom en slik overføring.

3. Dersom tredjepartsleverandøren av IKT-tjenester inngår i et konsern, skal kriteriene nevnt i nr. 2 vurderes med hensyn til de IKT-tjenestene som leveres av konsernet som helhet.

4. Kritiske tredjepartsleverandører av IKT-tjenester som er en del av et konsern, skal utpeke en juridisk person som koordineringspunkt for å sikre tilstrekkelig representasjon og kommunikasjon med hovedovervåkeren.

5. Hovedovervåkeren skal underrette tredjepartsleverandøren av IKT-tjenester om resultatet av vurderingen som fører til utpekingen nevnt i nr. 1 bokstav a). Innen 6 uker fra datoen for underretningen kan tredjepartsleverandøren av IKT-tjenester sende en begrunnet uttalelse til hovedovervåkeren med alle relevante opplysninger med henblikk på vurderingen. Hovedovervåkeren skal vurdere den begrunnede uttalelsen og kan be om ytterligere opplysninger som skal legges fram innen 30 kalenderdager etter mottak av en slik uttalelse.

Etter å ha utpekt en tredjepartsleverandør av IKT-tjenester som kritisk skal de europeiske tilsynsmyndighetene gjennom Felleskomiteen underrette tredjepartsleverandøren av IKT-tjenester om en slik utpeking og om startdatoen for når den faktisk vil være omfattet av tilsynsvirksomhet. Denne startdatoen skal ikke være senere enn én måned etter underretningen. Tredjepartsleverandøren av IKT-tjenester skal underrette de finansielle enhetene som den leverer tjenester til, om at den er utpekt som kritisk.

6. Kommisjonen gis myndighet til å vedta delegerte rettsakter i samsvar med artikkel 57 for å utfylle denne forordningen ved å spesifisere nærmere kriteriene i nr. 2 i denne artikkelen innen 17. juni 2024.

7. Den utpekingen som er nevnt i nr. 1 bokstav a), får ikke anvendelse før Kommisjonen har vedtatt en delegert rettsakt i samsvar med nr. 6.

8. Utpekingen nevnt i nr. 1 bokstav a) får ikke anvendelse på følgende:

i) Finansielle enheter som leverer IKT-tjenester til andre finansielle enheter.

ii) Tredjepartsleverandører av IKT-tjenester som er underlagt tilsynsrammer etablert for å støtte oppgavene nevnt i artikkel 127 nr. 2 i traktaten om Den europeiske unions virkemåte.

iii) Konserninterne leverandører av IKT-tjenester.

iv) Tredjepartsleverandører av IKT-tjenester som utelukkende leverer IKT-tjenester i én medlemsstat til finansielle enheter som bare er aktive i den aktuelle medlemsstaten.

9. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen opprette, offentliggjøre og oppdatere årlig listen over kritiske tredjepartsleverandører av IKT-tjenester på unionsplan.
10. Ved anvendelse av nr. 1 bokstav a) skal vedkommende myndigheter årlig og i aggregert form oversende de rapportene som er nevnt i artikkel 28 nr. 3 tredje ledd, til det overvåkingsforumet som er opprettet i henhold til artikkel 32. overvåkingsforumet skal vurdere finansielle enheters avhengighet av tredjepartsleverandører av IKT-tjenester på grunnlag av opplysninger som det mottar fra de vedkommende myndighetene.
11. Tredjepartsleverandører av IKT-tjenester som ikke er oppført på listen nevnt i nr. 9, kan anmode om å bli utpekt som kritiske i samsvar med nr. 1 bokstav a).

    Med henblikk på første ledd skal tredjepartsleverandøren av IKT-tjenester inngi en begrunnet søknad til EBA, ESMA eller EIOPA, som gjennom Felleskomiteen skal beslutte om denne tredjepartsleverandøren av IKT-tjenester skal utpekes som kritisk i samsvar med nr. 1 bokstav a).

    Beslutningen nevnt i andre ledd skal vedtas og meddeles tredjepartsleverandøren av IKT-tjenester innen seks måneder etter mottak av søknaden.
12. Finansielle enheter skal bare benytte seg av tjenestene til en tredjepartsleverandør av IKT-tjenester som er etablert i et tredjeland, og som er utpekt som kritisk i samsvar med nr. 1 bokstav a), dersom sistnevnte har etablert et datterforetak i Unionen innen tolv måneder etter utpekingen.
13. Den kritiske tredjepartsleverandøren av IKT-tjenester nevnt i nr. 12 skal underrette hovedovervåkeren om eventuelle endringer i ledelsesstrukturen i det datterforetaket som er etablert i Unionen.

Artikkel 32

Tilsynsrammens struktur

1. Felleskomiteen skal i samsvar med artikkel 57 nr. 1 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010 opprette overvåkingsforumet som en underkomité med henblikk på å støtte arbeidet som utføres i Felleskomiteen og av hovedovervåkeren nevnt i artikkel 31 nr. 1 bokstav b), på området for IKT-tredjepartsrisiko i alle finanssektorer. Overvåkingsforumet skal utarbeide utkast til felles holdninger og utkast til felles rettsakter for Felleskomiteen på dette området.

    Overvåkingsforumet skal regelmessig drøfte relevante utviklingstrekk med hensyn til IKT-risiko og -sårbarheter og fremme en konsekvent strategi for overvåking av IKT-tredjepartsrisiko på unionsplan.
2. Overvåkingsforumet skal hvert år foreta en samlet vurdering av resultatene og konklusjonene av den overvåkingsvirksomheten som utføres for alle kritiske tredjepartsleverandører av IKT-tjenester, og fremme koordineringstiltak for å øke finansielle enheters digitale operasjonelle motstandsdyktighet, fremme beste praksis for å håndtere IKT-konsentrasjonsrisiko og undersøke risikoreduserende tiltak for sektorovergripende risikooverføring.
3. Overvåkingsforumet skal legge fram omfattende referanseverdier for kritiske tredjepartsleverandører av IKT-tjenester som Felleskomiteen skal vedta som de europeiske tilsynsmyndighetenes felles holdninger i samsvar med artikkel 56 nr. 1 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.
4. Overvåkingsforumet skal bestå av følgende:
    a) Lederne for de europeiske tilsynsmyndighetene.
    b) Én representant på høyt nivå for det nåværende personalet i den berørte vedkommende myndigheten som nevnt i artikkel 46 fra hver medlemsstat.
    c) De administrerende direktørene for hver europeisk tilsynsmyndighet og én representant fra Kommisjonen, ESRB, ESB og ENISA som observatører.
    d) Dersom det er relevant, én ytterligere representant for en vedkommende myndighet som nevnt i artikkel 46 fra hver medlemsstat som observatør.
    e) Dersom det er relevant, én representant for de vedkommende myndighetene som er utpekt eller opprettet i samsvar med direktiv (EU) 2022/2555, og som er ansvarlig for tilsynet med en vesentlig eller viktig enhet som er omfattet av det nevnte direktivet, og som er utpekt som en kritisk tredjepartsleverandør av IKT-tjenester, som observatør.

    Overvåkingsforumet kan, dersom det er relevant, rådføre seg med uavhengige eksperter som er utpekt i samsvar med nr. 6.
5. Hver medlemsstat skal utpeke den berørte vedkommende myndigheten hvis ansatte skal

være den representanten på høyt nivå som er nevnt i nr. 4 første ledd bokstav b), og skal underrette hovedovervåkeren om dette.

De europeiske tilsynsmyndighetene skal offentliggjøre på sitt nettsted listen over representanter på høyt nivå fra det nåværende personalet i den berørte vedkommende myndigheten som er utpekt av medlemsstatene.

6. De uavhengige ekspertene nevnt i nr. 4 andre ledd skal utpekes av overvåkingsforumet fra en gruppe av eksperter som velges ut etter en offentlig og gjennomsiktig søknadsprosess.

   De uavhengige ekspertene skal utpekes på grunnlag av sin ekspertise om finansiell stabilitet, digital operasjonell motstandsdyktighet og IKT-sikkerhet. De skal opptre uavhengig og upartisk og utelukkende i hele Unionens interesse, og skal ikke be om eller motta instrukser fra Unionens institusjoner eller organer, medlemsstaters regjeringer eller annet offentlig eller privat organ.
7. I samsvar med artikkel 16 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010 skal de europeiske tilsynsmyndighetene innen 17. juli 2024 med henblikk på dette avsnittet utstede retningslinjer for samarbeidet mellom de europeiske tilsynsmyndighetene og de vedkommende myndighetene om de nærmere framgangsmåtene og vilkårene for tildeling og utførelse av oppgaver mellom de vedkommende myndighetene og de europeiske tilsynsmyndighetene, og de nærmere opplysningene om den utvekslingen av opplysninger som er nødvendig for at de vedkommende myndighetene skal kunne sikre oppfølgingen av de anbefalingene som er rettet til kritiske tredjepartsleverandører av IKT-tjenester i henhold til artikkel 35 nr. 1 bokstav d).
8. De kravene som er fastsatt i dette avsnittet berører ikke anvendelsen av direktiv (EU) 2022/2555 og andre unionsregler om tilsyn som gjelder for leverandører av skytjenester.
9. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen og på grunnlag av overvåkingsforumets forberedende arbeid årlig legge fram en rapport om anvendelsen av dette avsnittet for Europaparlamentet, Rådet og Kommisjonen.

Artikkel 33

Hovedovervåkerens oppgaver

1. Hovedovervåkeren, som er utpekt i samsvar med artikkel 31 nr. 1 bokstav b), skal overvåke de tildelte kritiske tredjepartsleverandørene av IKT-tjenester og skal i forbindelse med alle forhold knyttet til overvåkingen være det primære kontaktpunktet for disse kritiske tredjepartsleverandørene av IKT-tjenester.
2. Ved anvendelse av nr. 1 skal hovedovervåkeren vurdere om hver kritisk tredjepartsleverandør av IKT-tjenester har innført omfattende, forsvarlige og effektive regler, framgangsmåter, mekanismer og ordninger for å styre den IKT-risikoen som den kan utsette finansielle enheter for.

   Den vurderingen som er nevnt i første ledd, skal hovedsakelig fokusere på IKT-tjenester som leveres av den kritiske tredjepartsleverandøren av IKT-tjenester, og som støtter finansielle enheters kritiske eller viktige funksjoner. Dersom det er nødvendig for å håndtere alle relevante risikoer, skal denne vurderingen omfatte IKT-tjenester som støtter andre funksjoner enn dem som er kritiske eller viktige.
3. Vurderingen nevnt i nr. 2 skal omfatte følgende:
   a) IKT-krav som særlig skal sikre sikkerheten, tilgjengeligheten, kontinuiteten, skalerbarheten og kvaliteten på tjenestene som den kritiske tredjepartsleverandøren av IKT-tjenester leverer til finansielle enheter, samt evnen til alltid å opprettholde høye standarder for tilgjengeligheten, autentisiteten, integriteten eller fortroligheten til dataene.
   b) Den fysiske sikkerheten som bidrar til å sikre IKT-sikkerheten, herunder sikkerheten i lokaler, på anlegg og i datasentre.
   c) Risikostyringsprosessene, herunder retningslinjer for IKT-risikostyring, IKT-kontinuitet i virksomheten og planer for IKT-respons og -gjenoppretting.
   d) Styringsordninger, herunder en organisasjonsstruktur med klare, gjennomsiktige og konsekvente regler om ansvar og ansvarlighet som muliggjør effektiv IKT-risikostyring.
   e) Identifisering, overvåking og rask rapportering av vesentlige IKT-relaterte hendelser til finansielle enheter, styring og krisehåndtering av disse hendelsene, særlig cyberangrep.
   f) Ordninger for dataportabilitet, applikasjonsportabilitet og interoperabilitet som sikrer at de finansielle enhetene effektivt kan utøve sin oppsigelsesrett.
   g) Testing av IKT-systemer, IKT-infrastruktur og IKT-kontroller.

h) IKT-revisjoner.
i) Bruk av relevante nasjonale og internasjonale standarder som får anvendelse på levering av IKT-tjenester til de finansielle enhetene.

4. På grunnlag av vurderingen nevnt i nr. 2 og koordinert med det felles tilsynsnettverket som er nevnt i artikkel 34 nr. 1, skal hovedovervåkeren vedta en klar, detaljert og begrunnet individuell tilsynsplan som beskriver de årlige tilsynsmålene og de viktigste tilsynshandlingene som er planlagt for hver kritisk tredjepartsleverandør av IKT-tjenester. Denne planen skal hvert år meddeles den kritiske tredjepartsleverandøren av IKT-tjenester.

   Før tilsynsplanen vedtas, skal hovedovervåkeren oversende utkastet til tilsynsplan til den kritiske tredjepartsleverandøren av IKT-tjenester.

   Ved mottak av utkastet til tilsynsplan kan den kritiske tredjepartsleverandøren av IKT-tjenester sende inn en begrunnet uttalelse innen 15 kalenderdager som viser den forventede innvirkningen på de kundene som er enheter som faller utenfor virkeområdet for denne forordningen, og dersom det er relevant, utarbeide løsninger for å redusere risikoene.
5. Når de årlige tilsynsplanene nevnt i nr. 4 er vedtatt og meddelt de kritiske tredjepartsleverandørene av IKT-tjenester, kan vedkommende myndigheter treffe tiltak med hensyn til slike kritiske tredjepartsleverandører av IKT-tjenester bare etter avtale med hovedovervåkeren.

Artikkel 34

Operasjonell koordinering mellom hovedovervåkere

1. For å sikre en konsekvent strategi for overvåkingsvirksomhet og for å muliggjøre koordinerte generelle tilsynsstrategier og sammenhengende operasjonelle tilnærminger og arbeidsmetoder skal de tre ledende tilsynsmyndighetene som er utpekt i samsvar med artikkel 31 nr. 1 bokstav b), opprette et felles overvåkingsnettverk for seg imellom å koordinere de forberedende fasene og gjennomføringen av overvåkingsvirksomheten for de respektive kritiske tredjepartsleverandørene av IKT-tjenester som de overvåker, samt i forbindelse med eventuelle tiltak som måtte være nødvendige i henhold til artikkel 42.
2. Ved anvendelse av nr. 1 skal hovedovervåkerne utarbeide en felles overvåkingsprotokoll som angir de nærmere framgangsmåtene som skal følges for å gjennomføre den daglige koordineringen, og for å sikre raske utvekslinger og reaksjoner. Protokollen skal revideres regelmessig for å gjenspeile operasjonelle behov, særlig utviklingen av praktiske overvåkingsordninger.
3. Hovedovervåkerne kan fra gang til gang anmode ESB og ENISA om å yte teknisk rådgivning, dele praktisk erfaring eller delta i spesifikke koordineringsmøter i det felles overvåkingsnettverket.

Artikkel 35

Hovedovervåkerens myndighet

1. For å utføre de oppgavene som er fastsatt i dette avsnittet, har hovedovervåkeren følgende myndighet med hensyn til de kritiske tredjepartsleverandørene av IKT-tjenester:
   a) Å anmode om alle relevante opplysninger og dokumentasjon i samsvar med artikkel 37.
   b) Å gjennomføre generelle undersøkelser og inspeksjoner i samsvar med henholdsvis artikkel 38 og 39.
   c) Å anmode om, etter at overvåkingsvirksomheten er avsluttet, rapporter som angir hvilke tiltak som er truffet, eller hvilke avhjelpende tiltak som er iverksatt av de kritiske tredjepartsleverandørene av IKT-tjenester, i forbindelse med de anbefalingene som er nevnt i bokstav d) i dette nummeret.
   d) Å utstede anbefalinger på de områdene som er nevnt i artikkel 33 nr. 3, særlig
      i) om anvendelse av spesifikke IKT-relaterte sikkerhets- og kvalitetskrav eller -prosesser, særlig i forbindelse med utrulling av programvareutbedringer, oppdateringer, kryptering og andre sikkerhetstiltak som hovedovervåkeren anser som relevante for å sikre IKT-sikkerheten til tjenester som leveres til finansielle enheter,
      ii) om anvendelse av vilkår og betingelser, herunder den tekniske gjennomføringen av dem, i henhold til hvilke kritiske tredjepartsleverandører av IKT-tjenester leverer IKT-tjenester til finansielle enheter, som hovedovervåkeren anser som relevante for å forhindre generering av svake punkter («single points of failure»), eller at disse forsterkes, eller for å minimere eventuelle

systemiske virkninger i Unionens finanssektor i tilfelle av IKT-konsentrasjonsrisiko,

iii) om eventuelle planlagte underentrepriser, der hovedovervåkeren anser at ytterligere underentreprise, herunder underleverandøravtaler som de kritiske tredjepartsleverandørene av IKT-tjenester planlegger å inngå med tredjepartsleverandører av IKT-tjenester eller med IKT-underleverandører som er etablert i et tredjeland, kan utløse risikoer for den finansielle enhetens levering av tjenester, eller risiko for den finansielle stabiliteten, på grunnlag av undersøkelsen av de opplysningene som er samlet inn i samsvar med artikkel 37 og 38,

iv) om å avstå fra å inngå en ytterligere underleverandøravtale, der følgende kumulative vilkår er oppfylt:

– den påtenkte underleverandøren er en tredjepartsleverandør av IKT-tjenester eller en underleverandør av IKT-tjenester som er etablert i et tredjeland,

– underentreprisen gjelder den finansielle enhetens kritiske eller viktige funksjoner, og

– hovedovervåkeren anser at bruken av slik underentreprise utgjør en klar og alvorlig risiko for den finansielle stabiliteten i Unionen eller for finansielle enheter, herunder for finansielle enheters evne til å overholde tilsynskravene.

Ved anvendelse av punkt iv) i denne bokstaven skal tredjepartsleverandører av IKT-tjenester ved bruk av den malen som er nevnt i artikkel 41 nr. 1 bokstav b), overføre opplysninger om underentreprise til hovedovervåkeren.

2. Når hovedovervåkeren utøver den myndigheten som er nevnt i denne artikkelen, skal den

a) sikre regelmessig koordinering innenfor det felles overvåkingsnettverket og særlig tilstrebe konsekvente strategier, dersom det er relevant, med hensyn til overvåkingen av kritiske tredjepartsleverandører av IKT-tjenester,

b) ta behørig hensyn til det rammeverket som er fastsatt i henhold til direktiv (EU) 2022/2555, og, dersom det er nødvendig, høre de berørte vedkommende myndighetene som er utpekt eller opprettet i samsvar med det nevnte direktivet, for å unngå overlapping av tekniske og organisatoriske tiltak som kan få anvendelse på kritiske tredjepartsleverandører av IKT-tjenester i henhold til det nevnte direktivet,

c) i den grad det er mulig, tilstrebe å minimere risikoen for forstyrrelser i tjenester som leveres av kritiske tredjepartsleverandører av IKT-tjenester til kunder som er enheter som faller utenfor virkeområdet for denne forordningen.

3. Hovedovervåkeren skal høre overvåkingsovervåkingsforumet før den utøver den myndigheten som er nevnt i nr. 1.

Før hovedovervåkeren utsteder anbefalinger i samsvar med nr. 1 bokstav d), skal den gi tredjepartsleverandøren av IKT-tjenester mulighet til å legge fram, innen 30 kalenderdager, relevante opplysninger som dokumenterer den forventede innvirkningen på kunder som er enheter som faller utenfor virkeområdet for denne forordningen, og, dersom det er relevant, utarbeide løsninger for å redusere risikoene.

4. Hovedovervåkeren skal underrette det felles overvåkingsnettverket om resultatet av myndighetsutøvelsen nevnt i nr. 1 bokstav a) og b). Hovedovervåkeren skal uten unødig opphold oversende rapportene nevnt i nr. 1 bokstav c) til det felles overvåkingsnettverket og til de vedkommende myndighetene for de finansielle enhetene som bruker IKT-tjenester levert av den kritiske tredjepartsleverandøren av IKT-tjenester.

5. Kritiske tredjepartsleverandører av IKT-tjenester skal lojalt samarbeide med hovedovervåkeren og bistå denne i utførelsen av sine oppgaver.

6. Ved hel eller delvis manglende overholdelse av de tiltakene som kreves i henhold til myndighetsutøvelsen i nr. 1 bokstav a), b) og c), og etter utløpet av en periode på minst 30 kalenderdager fra den datoen da den kritiske tredjepartsleverandøren av IKT-tjenester ble underrettet om de respektive tiltakene, skal hovedovervåkeren treffe en beslutning om å ilegge en overtredelsesgebyr for å tvinge den kritiske tredjepartsleverandøren av IKT-tjenester til å overholde disse tiltakene.

7. Overtredelsesgebyret nevnt i nr. 6 skal ilegges daglig fram til overholdelse er oppnådd, og i høyst seks måneder etter underretningen om beslutningen om å ilegge den kritiske tredjepartsleverandøren av IKT-tjenester en overtredelsesgebyr.

8. Størrelsen på overtredelsesgebyret, beregnet fra den datoen som er fastsatt i beslutningen om å ilegge overtredelsesgebyret, skal utgjøre opp til 1 % av den gjennomsnittlige globale omsetningen per dag for den kritiske tredjepartsleverandøren av IKT-tjenester i foregående regnskapsår. Ved fastsettelse av størrelsen på overtredelsesgebyret skal hovedovervåkeren ta hensyn til følgende kriterier for manglende overholdelse av tiltakene nevnt i nr. 6:
   a) Den manglende overholdelsens grovhet og varighet.
   b) Hvorvidt den manglende overholdelsen er begått forsettlig eller uaktsomt.
   c) Viljen hos tredjepartsleverandøren av IKT-tjenester til å samarbeide med hovedovervåkeren.

   Ved anvendelse av første ledd skal hovedovervåkeren delta i samråd innenfor det felles overvåkingsnettverket for å sikre en konsekvent strategi.
9. Overtredelsesgebyr skal være av administrativ art og skal kunne tvangsfullbyrdes. Tvangsfullbyrdelsen skal følge de gjeldende sivile rettergangsreglene i den medlemsstaten på hvis territorium inspeksjoner og adgang skal finne sted. Domstolene i den berørte medlemsstaten skal ha domsmyndighet til å treffe beslutninger om klager knyttet til uregelmessigheter i forbindelse med tvangsfullbyrdelsen. Beløpene for overtredelsesgebyr skal overføres til Den europeiske unions alminnelige budsjett.
10. Hovedovervåkeren skal offentliggjøre alle overtredelsesgebyr som er ilagt, med mindre en slik offentliggjøring skulle kunne skape alvorlig uro på finansmarkedene eller påføre berørte parter uforholdsmessig stor skade.
11. Før hovedovervåkeren ilegger overtredelsesgebyr i henhold til nr. 6, skal den gi representantene for den kritiske tredjepartsleverandøren av IKT-tjenester som saken gjelder, mulighet til å bli hørt om de omstendighetene som overvåkingsmyndigheten har påtalt, og den skal basere sine beslutninger bare på omstendigheter som den kritiske tredjepartsleverandøren av IKT-tjenester som saken gjelder, har hatt mulighet til å uttale seg om.

    Retten til forsvar for de personene saken gjelder, skal sikres fullt ut under saksbehandlingen. Den kritiske tredjepartsleverandøren av IKT-tjenester som saken gjelder, skal ha rett til innsyn i saksmappen, med forbehold for andre personers rettmessige interesse av å bevare sine forretningshemmeligheter. Retten til innsyn i saksmappen skal ikke omfatte fortrolige opplysninger eller hovedovervåkerens interne forberedende dokumenter.

Artikkel 36

Hovedovervåkerens myndighetsutøvelse utenfor unionen

1. Dersom overvåkingsmålene ikke kan oppnås ved samhandling med datterforetaket som er opprettet i henhold til artikkel 31 nr. 12, eller ved å utøve overvåkingsvirksomhet i lokaler i Unionen, kan hovedovervåkeren utøve den myndigheten som er nevnt i følgende bestemmelser, i alle lokaler i et tredjeland og som eies eller på en eller annen måte brukes av en kritisk tredjepartsleverandør av IKT-tjenester for å levere tjenester til finansielle enheter i Unionen i forbindelse med sin forretningsvirksomhet, sine funksjoner eller tjenester, herunder alle administrative kontorer, foretakslokaler eller driftssteder, anlegg, arealer, bygninger eller andre eiendommer:
   a) I artikkel 35 nr. 1 bokstav a).
   b) I artikkel 35 nr. 1 bokstav b), i samsvar med artikkel 38 nr. 2 bokstav a), b) og d), og i artikkel 39 nr. 1 og 2 bokstav a).

      Myndigheten omhandlet i første ledd kan utøves dersom alle følgende vilkår er oppfylt:
      i) Hovedovervåkeren anser det som nødvendig å gjennomføre en inspeksjon i et tredjeland for at denne fullt ut og på en effektiv måte skal kunne utføre sine oppgaver i henhold til denne forordningen.
      ii) Inspeksjonen i et tredjeland har direkte tilknytning til levering av IKT-tjenester til finansielle enheter i Unionen.
      iii) Den berørte kritiske tredjepartsleverandøren av IKT-tjenester samtykker i at det gjennomføres en inspeksjon i et tredjeland.
      iv) Den berørte myndigheten i det berørte tredjelandet er blitt offisielt underrettet av hovedovervåkeren og har ikke gjort innsigelse mot dette.
2. Uten at det berører Unionens institusjoner og medlemsstatenes respektive myndighet, skal EBA, ESMA eller EIOPA ved anvendelse av nr. 1 inngå ordninger om administrativt samarbeid med den berørte myndigheten i det berørte tredjelandet for å gjøre det mulig for hovedovervåkeren og den gruppen som den

har utpekt til oppgaven i det aktuelle tredjelandet, å gjennomføre inspeksjoner på en smidig måte i det berørte tredjelandet. Disse samarbeidsordningene skal ikke medføre juridiske forpliktelser for Unionen og dens medlemsstater og skal heller ikke hindre medlemsstatene og deres vedkommende myndigheter i å inngå bilaterale eller multilaterale avtaler med disse tredjelandene og deres berørte myndigheter.

Disse samarbeidsordningene skal minst angi følgende opplysninger:

a) Framgangsmåtene for koordinering av den overvåkingsvirksomheten som utøves i henhold til denne forordningen, og enhver tilsvarende overvåking av IKT-tredjepartsrisiko i finanssektoren som utøves av den berørte myndigheten i det berørte tredjelandet, herunder nærmere opplysninger om oversending av sistnevntes samtykke til at hovedovervåkeren og dens utpekte gruppe kan gjennomføre generelle undersøkelser og stedlige inspeksjoner i henhold til nr. 1 første ledd, på det territoriet som er omfattet av dens jurisdiksjon.
b) Ordningen for overføring av alle relevante opplysninger mellom EBA, ESMA eller EIOPA og den berørte myndigheten i det berørte tredjelandet, særlig i forbindelse med opplysninger som hovedovervåkeren kan anmode om i henhold til artikkel 37.
c) Ordningene for rask underretning fra den berørte myndigheten i det berørte tredjelandet til EBA, ESMA eller EIOPA om tilfeller der en tredjepartsleverandør av IKT-tjenester som er etablert i et tredjeland, og som er utpekt som kritisk i samsvar med artikkel 31 nr. 1 bokstav a), anses å ha overtrådt de kravene den er forpliktet til å oppfylle i henhold til gjeldende rett i det berørte tredjelandet, når den leverer tjenester til finansinstitusjoner i dette tredjelandet, samt de avhjelpende tiltakene og sanksjonene som er anvendt.
d) Regelmessig overføring av oppdateringer om utviklingen på regulerings- og tilsynsområdet når det gjelder overvåkingen av IKT-tredjepartsrisiko for finansinstitusjoner i det berørte tredjelandet.
e) Nærmere opplysninger som ved behov gjør det mulig for én representant for den relevante myndigheten i det berørte tredjelandet å delta i de inspeksjonene som hovedovervåkeren og den utpekte gruppen gjennomfører.

3. Når hovedovervåkeren ikke er i stand til å gjennomføre overvåkningsvirksomhet utenfor Unionen som nevnt i nr. 1 og 2, skal hovedovervåkeren
   a) utøve sin myndighet i henhold til artikkel 35 på grunnlag av alle de forholdene som den kjenner til, og dokumentene som den har tilgang til,
   b) dokumentere og redegjøre for eventuelle konsekvenser av at den ikke er i stand til å gjennomføre den planlagte overvåkingsvirksomheten som nevnt i denne artikkelen.

   De potensielle konsekvensene omhandlet i bokstav b) i dette nummeret skal tas i betraktning i hovedovervåkerens anbefalinger utstedt i henhold til artikkel 35 nr. 1 bokstav d).

Artikkel 37

Anmodning om opplysninger

1. Hovedovervåkeren kan ved enkel anmodning eller ved beslutning kreve at kritiske tredjepartsleverandører av IKT-tjenester legger fram alle de opplysningene som er nødvendige for at hovedovervåkeren skal kunne utføre sine oppgaver i henhold til denne forordningen, herunder alle relevante forretningsdokumenter eller operasjonelle dokumenter, kontrakter, retningslinjer, dokumentasjon, rapporter fra revisjon av IKT-sikkerhet, IKT-relaterte hendelsesrapporter, samt alle opplysninger om parter som den kritiske tredjepartsleverandøren av IKT-tjenester har utkontraktert driftsfunksjoner eller aktiviteter til.
2. Når hovedovervåkeren sender en enkel anmodning om opplysninger i henhold til nr. 1, skal den
   a) vise til denne artikkelen som rettslig grunnlag for sin anmodning,
   b) angi formålet med anmodningen,
   c) angi nærmere hvilke opplysninger som kreves,
   d) fastsette en frist for når opplysningene skal legges fram,
   e) underrette representanten for den tredjepartsleverandøren av IKT-tjenester som anmodes om opplysninger, om at vedkommende ikke er forpliktet til å legge fram opplysningene, men at de opplysningene som legges fram frivillig som svar på anmodningen, ikke må være uriktige eller villedende.
3. Når hovedovervåkeren ved en beslutning anmoder om opplysninger i henhold til nr. 1, skal den

a) vise til denne artikkelen som rettslig grunnlag for sin anmodning,
b) angi formålet med anmodningen,
c) angi nærmere hvilke opplysninger som kreves,
d) fastsette en frist for når opplysningene skal legges fram,
e) angi de overtredelsesgebyrene som er fastsatt i artikkel 35 nr. 6, dersom de ønskede opplysningene er ufullstendige, eller dersom de ikke er lagt fram innen den tidsfristen som er nevnt i bokstav d) i dette nummeret,
f) opplyse om retten til å anke beslutningen inn for de europeiske tilsynsmyndighetenes klageinstans og til å bringe beslutningen inn for Den europeiske unions domstol («Domstolen») i samsvar med artikkel 60 og 61 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

4. Representantene for de kritiske tredjepartsleverandørene av IKT-tjenester skal legge fram de opplysningene som det anmodes om. Advokater med behørig fullmakt kan legge fram opplysningene på vegne av sine klienter. Den kritiske tredjepartsleverandøren av IKT-tjenester har det fulle ansvaret dersom opplysningene som legges fram, er ufullstendige, uriktige eller villedende.
5. Hovedovervåkeren skal umiddelbart oversende en kopi av beslutningen om å utlevere opplysninger til de vedkommende myndighetene for de finansielle enhetene som benytter seg av de tjenestene som de berørte tredjepartsleverandørene av IKT-tjenester leverer, og til det felles overvåkingsnettverket.

Artikkel 38

Generelle undersøkelser

1. For å utføre sine oppgaver i henhold til denne forordningen kan hovedovervåkeren, med bistand fra den felles granskningsgruppen omhandlet i artikkel 40 nr. 1, om nødvendig gjennomføre undersøkelser av kritiske tredjepartsleverandører av IKT-tjenester.
2. Hovedovervåkeren skal ha myndighet til å
   a) undersøke registre, data, framgangsmåter og alt annet materiale som har betydning for utførelsen av dens oppgaver, uansett hvilket medium de er lagret på,
   b) ta eller skaffe bekreftede kopier av eller utdrag fra slike registre, opplysninger, dokumenterte framgangsmåter og alt annet materiale,
   c) innkalle representanter for den kritiske tredjepartsleverandøren av IKT-tjenester og be om muntlige eller skriftlige redegjørelser for forhold eller dokumenter som berører gjenstanden for og formålet med undersøkelsen, samt registrere svarene,
   d) høre enhver fysisk eller juridisk person som samtykker i å bli hørt, for å samle inn opplysninger om gjenstanden for undersøkelsen,
   e) anmode om opplysninger om tele- og datatrafikk.
3. De tjenestemennene og andre personer som har fullmakt fra hovedovervåkeren til å gjennomføre undersøkelsen nevnt i nr. 1, skal utøve sin myndighet mot framvisning av en skriftlig tillatelse med nærmere opplysninger om gjenstanden for og formålet med undersøkelsen.

   Denne tillatelsen skal også inneholde opplysninger om de overtredelsesgebyrene som er fastsatt i artikkel 35 nr. 6, dersom dokumentasjonen, opplysningene, de dokumenterte framgangsmåtene eller alt annet materiale som kreves, eller svarene på spørsmål som er stilt til representanter for tredjepartsleverandøren av IKT-tjenester, ikke legges fram eller er ufullstendige.
4. Representantene for de kritiske tredjepartsleverandørene av IKT-tjenester er pålagt å underkaste seg undersøkelsene på grunnlag av en beslutning fra hovedovervåkeren. Beslutningen skal angi undersøkelsens gjenstand og formål, de overtredelsesgebyrene som er fastsatt i artikkel 35 nr. 6, klageadgangen i henhold til forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010 samt retten til å bringe beslutningen inn for Domstolen.
5. Hovedovervåkeren skal i god tid før undersøkelsen starter, underrette vedkommende myndigheter om de finansielle enhetene som benytter seg av IKT-tjenestene til den kritiske tredjepartsleverandøren av IKT-tjenester, om den planlagte undersøkelsen og om identiteten til de bemyndigede personene.

   Hovedovervåkeren skal underrette det felles overvåkingsnettverket om alle opplysninger som oversendes i henhold til første ledd.

Artikkel 39

Inspeksjoner

1. For å utføre sine oppgaver i henhold til denne forordningen kan hovedovervåkeren, med

bistand fra de felles granskningsgruppene som er nevnt i artikkel 40 nr. 1, innlede og gjennomføre alle nødvendige stedlige inspeksjoner i alle forretningslokaler, på arealer eller i eiendommer som tilhører tredjepartsleverandørene av IKT-tjenester, som for eksempel hovedkontorer, operasjonssentraler og sekundære lokaler, samt gjennomføre eksterne inspeksjoner.

Ved utøvelse av den myndigheten som er nevnt i første ledd, skal hovedovervåkeren rådføre seg med det felles overvåkingsnettverket.

2. De tjenestemennene og andre personer som har fullmakt fra hovedovervåkerentil å gjennomføre en stedlig inspeksjon, skal ha myndighet til å
   a) få adgang til forretningslokaler, arealer eller eiendommer og å
   b) forsegle slike forretningslokaler, regnskap eller forretningsdokumenter i det tidsrommet og i det omfanget som kreves for inspeksjonen.

   Tjenestemenn og andre personer som har fullmakt fra hovedovervåkeren, skal utøve sin myndighet mot framvisning av en skriftlig tillatelse med nærmere opplysninger om gjenstanden for og formålet med inspeksjonen og om overtredelsesgebyr omhandlet i artikkel 35 nr. 6 som får anvendelse dersom representantene for de berørte kritiske tredjepartsleverandørene av IKT-tjenester ikke underkaster seg inspeksjonen.
3. Hovedovervåkeren skal i god tid før inspeksjonen starter, underrette de vedkommende myndighetene for de finansielle enhetene som bruker denne tredjepartsleverandøren av IKT-tjenester.
4. Inspeksjonene skal omfatte alle relevante IKT-systemer, nettverk, utstyr, opplysninger og data som entes brukes til eller bidrar til leveringen av IKT-tjenester til finansielle enheter.
5. Før en planlagt stedlig inspeksjon skal hovedovervåkeren i rimelig tid underrette de kritiske tredjepartsleverandørene av IKT-tjenester, med mindre en slik underretning ikke er mulig på grunn av en nøds- eller krisesituasjon, eller dersom det ville føre til en situasjon der inspeksjonen eller revisjonen ikke lenger ville være effektiv.
6. Den kritiske tredjepartsleverandøren av IKT-tjenester skal underkaste seg stedlige inspeksjoner som er pålagt i henhold til en beslutning truffet av hovedovervåkeren. Beslutningen skal angi inspeksjonens gjenstand og formål, fastsette tidspunktet da inspeksjonen skal starte, og angi de overtredelsesgebyrene som er fastsatt i artikkel 35 nr. 6, klageadgangen i henhold til forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010 samt retten til å bringe beslutningen inn for Domstolen.
7. Dersom tjenestemenn og andre personer som har fullmakt fra hovedovervåkeren, konstaterer at en kritisk tredjepartsleverandør av IKT-tjenester gjør innsigelse mot en inspeksjon som er pålagt i henhold til denne artikkelen, skal hovedovervåkeren underrette den kritiske tredjepartsleverandøren av IKT-tjenester om konsekvensene av en slik innsigelse, herunder om muligheten for de relevante finansielle enhetenes vedkommende myndigheter til å kreve at de finansielle enhetene sier opp de kontraktsregulerte ordningene som er inngått med den aktuelle kritiske tredjepartsleverandøren av IKT-tjenester.

Artikkel 40

Løpende tilsyn

1. Når hovedovervåkeren utøver overvåkingsvirksomhet, særlig generelle undersøkelser eller inspeksjoner, skal den bistås av en felles granskningsgruppe som er opprettet for hver kritisk tredjepartsleverandør av IKT-tjenester.
2. Den felles granskningsgruppen nevnt i nr. 1 skal bestå av ansatte fra
   a) de europeiske tilsynsmyndighetene,
   b) de berørte vedkommende myndighetene som fører tilsyn med de finansielle enhetene som den kritiske tredjepartsleverandøren av IKT-tjenester leverer IKT-tjenester til,
   c) den nasjonale vedkommende myndigheten nevnt i artikkel 32 nr. 4 bokstav e), på frivillig grunnlag,
   d) én nasjonal vedkommende myndighet fra den medlemsstaten der den kritiske tredjepartsleverandøren av IKT-tjenester er etablert, på frivillig grunnlag.

   Medlemmene av den felles granskningsgruppen skal ha kunnskap om IKT-spørsmål og operasjonell risiko. Arbeidet i den felles granskningsgruppen skal koordineres av en utpekt ansatt under hovedovervåkeren («koordinatoren for hovedovervåkeren»).
3. Innen tre måneder etter at en undersøkelse eller inspeksjon er avsluttet, skal hovedovervåkeren, etter å ha hørt overvåkingsforumet, vedta anbefalinger som skal rettes til den kri-

tiske tredjepartsleverandøren av IKT-tjenester i henhold til den myndigheten som er nevnt i artikkel 35.

4. Anbefalingene nevnt i nr. 3 skal umiddelbart meddeles den kritiske tredjepartsleverandøren av IKT-tjenester og de vedkommende myndighetene for de finansielle enhetene som den leverer IKT-tjenester til.

   For å gjennomføre overvåkingsvirksomheten kan hovedovervåkeren ta hensyn til eventuelle relevante tredjepartssertifiseringer og interne eller eksterne revisjonsrapporter fra IKT-tredjeparter som er gjort tilgjengelige av den kritiske tredjepartsleverandøren av IKT-tjenester.

Artikkel 41

Harmonisering av vilkår som muliggjør utøvelse av tilsynsvirksomhet

1. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen utarbeide forslag til tekniske reguleringsstandarder for å presisere
   a) hvilke opplysninger en tredjepartsleverandør av IKT-tjenester skal gi i sin søknad om frivillig anmodning om å bli utpekt som kritisk i henhold til artikkel 31 nr. 11,
   b) innholdet, strukturen og formatet til de opplysningene som skal legges fram, offentliggjøres eller rapporteres av tredjepartsleverandører av IKT-tjenester i henhold til artikkel 35 nr. 1, herunder malen for framlegging av opplysninger om underleverandøravtaler,
   c) kriteriene for å fastsette sammensetningen av den felles granskningsgruppen som sikrer en balansert deltakelse av ansatte fra de europeiske tilsynsmyndighetene og fra de berørte vedkommende myndighetene, deres utpeking, oppgaver og arbeidsordninger.
   d) nærmere opplysninger om de vedkommende myndighetenes vurdering av de tiltakene som er truffet av kritiske tredjepartsleverandører av IKT-tjenester på grunnlag av anbefalingene fra hovedovervåkeren i henhold til artikkel 42 nr. 3.
2. De europeiske tilsynsmyndighetene skal legge fram disse utkastene til tekniske reguleringsstandarder for Kommisjonen innen 17. juli 2024.

   Kommisjonen delegeres myndighet til å utfylle denne forordningen ved å vedta de tekniske reguleringsstandardene som er nevnt i nr. 1, i samsvar med framgangsmåten fastsatt i artikkel 10–14 i forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010.

Artikkel 42

Vedkommende myndigheters oppfølging

1. Innen 60 kalenderdager etter mottak av anbefalingene utstedt av hovedovervåkeren i henhold til artikkel 35 nr. 1 bokstav d), skal kritiske tredjepartsleverandører av IKT-tjenester enten underrette hovedovervåkeren om at de har til hensikt å følge anbefalingene, eller gi en begrunnet forklaring på hvorfor de ikke følger slike anbefalinger. Hovedovervåkeren skal umiddelbart oversende disse opplysningene til de berørte finansielle enhetenes vedkommende myndigheter.
2. Hovedovervåkeren skal offentliggjøre tilfeller der en kritisk tredjepartsleverandør av IKT-tjenester unnlater å underrette hovedovervåkeren i samsvar med nr. 1, eller dersom den forklaringen som gis av den kritiske tredjepartsleverandøren av IKT-tjenester ikke anses å være tilstrekkelig. De offentliggjorte opplysningene skal opplyse om identiteten til den kritiske tredjepartsleverandøren av IKT-tjenester samt om typen og arten av den manglende overholdelsen. Slike opplysninger skal begrenses til hva som er relevant og forholdsmessig med henblikk på å sikre allmennhetens bevissthet, med mindre en slik offentliggjøring skulle kunne forvolde de involverte partene uforholdsmessig stor skade eller i alvorlig grad bringe finansmarkedenes velordnede funksjon og integritet eller stabiliteten i hele eller deler av Unionens finanssystem i fare.

   Hovedovervåkeren skal underrette tredjepartsleverandøren av IKT-tjenester om denne offentliggjøringen.
3. De vedkommende myndighetene skal underrette de relevante finansielle enhetene om de risikoene som er identifisert i anbefalingene rettet til kritiske tredjepartsleverandører av IKT-tjenester i samsvar med artikkel 35 nr. 1 bokstav d).

   Når de finansielle enhetene styrer IKT-tredjepartsrisiko skal de ta hensyn til risikoene nevnt i første ledd.
4. Dersom en vedkommende myndighet vurderer at en finansiell enhet ikke tar hensyn til, eller ikke i tilstrekkelig grad i sin styring av IKT-tredjepartsrisiko håndterer de spesifikke risikoene som er identifisert i anbefalingene, skal den underrette den finansielle enheten

om muligheten for at det innen 60 kalenderdager etter mottak av en slik underretning treffes en beslutning i samsvar med nr. 6, dersom det ikke foreligger egnede kontraktsregulerte ordninger som tar sikte på å håndtere slike risikoer.

5. De vedkommende myndighetene kan etter å ha mottatt rapportene nevnt i artikkel 35 nr. 1 bokstav c) og før de treffer en beslutning som nevnt i nr. 6 i denne artikkelen, på frivillig grunnlag høre de vedkommende myndighetene som er utpekt eller etablert i samsvar med direktiv (EU) 2022/2555, og som er ansvarlige for tilsynet med en vesentlig eller viktig enhet som er omfattet av det nevnte direktivet, og som er utpekt som en kritisk tredjepartsleverandør av IKT-tjenester.
6. De vedkommende myndighetene kan, som en siste utvei, etter underretningen og eventuelt høringen fastsatt i nr. 4 og 5 i denne artikkelen, i samsvar med artikkel 50 treffe en beslutning som krever at finansielle enheter midlertidig, enten helt eller delvis, avbryter bruken eller innføringen av en tjeneste som leveres av den kritiske tredjepartsleverandøren av IKT-tjenester, inntil de risikoene som er identifisert i anbefalingene til kritiske tredjepartsleverandører av IKT-tjenester, er blitt håndtert. De kan om nødvendig kreve at finansielle enheter helt eller delvis sier opp de relevante kontraktsregulerte ordningene som er inngått med de kritiske tredjepartsleverandørene av IKT-tjenester.
7. Dersom en kritisk tredjepartsleverandør av IKT-tjenester nekter å godta anbefalinger, basert på en annen strategi enn den som er anbefalt av hovedovervåkeren, og en slik annen strategi kan ha en negativ innvirkning på et høyt antall finansielle enheter eller en betydelig del av finanssektoren, og individuelle advarsler fra de vedkommende myndighetene ikke har ført til konsekvente strategier som begrenser den potensielle risikoen for den finansiell stabiliteten, kan hovedovervåkeren, etter å ha hørt overvåkingsforumet, avgi ikkebindende og ikke-offentlige uttalelser til de vedkommende myndighetene for å fremme konsekvente og konvergerende tilsynsmessige oppfølgingstiltak, alt etter hva som er relevant.
8. Etter å ha mottatt rapportene nevnt i artikkel 35 nr. 1 bokstav c) skal vedkommende myndigheter, når de treffer en beslutning som omhandlet i nr. 6 i denne artikkelen, ta hensyn til typen og omfanget av den risikoen som ikke er håndtert av den kritiske tredjepartsleverandøren av IKT-tjenester, samt alvorlighetsgraden av den manglende overholdelsen, samtidig som det tas hensyn til følgende kriterier:
   a) Den manglende overholdelsens grovhet og varighet.
   b) Hvorvidt manglende overholdelse har påvist alvorlige svakheter i de framgangsmåtene, de ledelsessystemene, den risikostyringen og de internkontrollene som den kritiske tredjepartsleverandøren av IKT-tjenester ivaretar.
   c) Hvorvidt økonomisk kriminalitet er blitt fremmet eller forårsaket av eller på annen måte kan tilskrives den manglende overholdelsen.
   d) Hvorvidt den manglende overholdelsen er forsettlig eller uaktsom.
   e) Hvorvidt midlertidig oppheving eller oppsigelse av de kontraktsregulerte ordningene medfører en risiko for kontinuiteten i den finansielle enhetens forretningsvirksomhet, til tross for den finansielle enhetens innsats for å unngå avbrudd i leveringen av tjenester.
   f) Dersom det er relevant, den uttalelsen som på frivillig basis er innhentet i samsvar med nr. 5 i denne artikkelen fra de vedkommende myndighetene som i samsvar med direktiv (EU) 2022/2555 er utpekt eller opprettet som ansvarlige for tilsynet med en vesentlig eller viktig enhet, som er omfattet av det nevnte direktivet, og som er utpekt som en kritisk tredjepartsleverandør av IKT-tjenester.

   De vedkommende myndighetene skal gi de finansielle enhetene den tiden som kreves for at de skal kunne tilpasse sine kontraktsregulerte ordninger med kritiske tredjepartsleverandører av IKT-tjenester for å unngå skadelige virkninger på den digitale operasjonelle motstandsdyktigheten, og slik at de kan innføre exit-strategier og overgangsplaner som nevnt i artikkel 28.
9. Den beslutningen som er nevnt i nr. 6 i denne artikkelen, skal meddeles medlemmene av overvåkingsforumet nevnt i artikkel 32 nr. 4 bokstav a), b) og c) og det felles overvåkingsnettverket.

   De kritiske tredjepartsleverandørene av IKT-tjenester som er påvirket av beslutningene fastsatt i nr. 6, skal samarbeide fullt ut med de berørte finansielle enhetene, særlig i forbindelse med prosessen med midlertidig oppheving eller oppsigelse av deres kontraktsregulerte ordninger.

10. De vedkommende myndighetene skal regelmessig underrette hovedovervåkeren om de tilnærmingene og tiltakene som de har iverksatt i forbindelse med sine tilsynsoppgaver når det gjelder finansielle enheter, samt om de kontraktsregulerte ordningene som de finansielle enhetene har inngått, når kritiske tredjepartsleverandører av IKT-tjenester ikke helt eller delvis har godkjent anbefalingene til dem fra hovedovervåkeren.
11. Hovedovervåkeren kan på anmodning gi ytterligere avklaringer når det gjelder de anbefalingene som er utstedt for å veilede de vedkommende myndighetene om oppfølgingstiltakene.

Artikkel 43

Overvåkingsavgifter

1. Hovedovervåkeren skal i samsvar med den delegerte rettsakten nevnt i nr. 2 i denne artikkelen oppkreve avgifter hos kritiske tredjepartsleverandører av IKT-tjenester som fullt ut dekker hovedovervåkerens nødvendige utgifter i forbindelse med gjennomføringen av overvåkignsoppgaver i henhold til denne forordningen, herunder godtgjøring for eventuelle kostnader som kan påløpe som følge av arbeid utført av den felles granskningsgruppen omhandlet i artikkel 40, samt kostnadene til rådgivning fra de uavhengige ekspertene omhandlet i artikkel 32 nr. 4 andre ledd, i forbindelse med forhold som hører inn under ansvarsområdet for direkte overvåkingsvirksomhet.

   Det avgiftsbeløpet som oppkreves hos en kritisk tredjepartsleverandør av IKT-tjenester, skal dekke alle kostnader som følger av utførelsen av oppgavene som er fastsatt i dette avsnittet, og skal stå i et rimelig forhold til leverandørens omsetning.
2. Kommisjonen gis myndighet til å vedta en delegert rettsakt i samsvar med artikkel 57 for å utfylle denne forordningen med hensyn til hvor høye avgiftsbeløpene skal være, og hvordan de skal betales innen 17. juli 2024.

Artikkel 44

Internasjonalt samarbeid

1. Uten at det berører artikkel 36, kan EBA, ESMA og EIOPA, i samsvar med artikkel 33 i henholdsvis forordning (EU) nr. 1093/2010, (EU) nr. 1095/2010 og (EU) nr. 1094/2010, inngå administrative ordninger med tredjelands regulerings- og tilsynsmyndigheter for å fremme internasjonalt samarbeid om IKT-tredjepartsrisiko i ulike finanssektorer, særlig ved å utvikle beste praksis for gjennomgåelse av praksis og kontroller i forbindelse med IKT-risikostyring, avbøtende tiltak og håndtering av hendelser.
2. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen hvert femte år legge fram en felles konfidensiell rapport for Europaparlamentet, Rådet og Kommisjonen, som sammenfatter resultatene av relevante drøftinger som er gjennomført med tredjelands myndigheter nevnt i nr. 1, og som fokuserer på utviklingen av IKT-tredjepartsrisiko og konsekvensene for den finansiell stabiliteten, markedsintegriteten, investorvernet og det indre markeds virkemåte.

Kapittel VI

Ordninger for utveksling av opplysninger

Artikkel 45

Ordninger for utveksling av opplysninger og etterretninger om cybertrusler

1. De finansielle enhetene kan seg imellom utveksle opplysninger og etterretninger om cybertrusler, herunder indikatorer på kompromittering, taktikker, teknikker og framgangsmåter, varsling av cybersikkerhet og konfigurasjonsverktøyer, i den grad slik utveksling av opplysninger og etterretninger

a) har som mål å forbedre finansielle enheters digitale operasjonelle motstandsdyktighet, særlig ved å øke bevisstheten om cybertrusler, begrense eller hindre cybertruslenes spredningsevne, støtte forsvarskapasiteten, metoder for påvisning av trusler, skadebegrensende strategier eller respons- og gjenopprettingsfaser,
b) finner sted innenfor betrodde grupper av finansielle enheter,
c) gjennomføres gjennom ordninger for utveksling av opplysninger som beskytter den potensielt sensitive karakteren til de opplysningene som utveksles, og som er omfattet av atferdsregler med full respekt for forretningshemmeligheter, vern av personopplysninger i samsvar med forordning (EU) 2016/679 og retningslinjer for konkurransepolitikk.

2. Ved anvendelse av nr. 1 bokstav c) skal ordningene for utveksling av opplysninger inneholde fastsatte vilkår for deltakelse og, dersom det er relevant, nærmere opplysninger om offentlige

myndigheters deltakelse og den kapasiteten de kan ha i forbindelse med ordningene for utveksling av opplysninger, om deltakelse av tredjepartsleverandører av IKT-tjenester og om operasjonelle elementer, herunder bruken av særskilte IT-plattformer.

3. De finansielle enhetene skal underrette de vedkommende myndighetene om sin deltakelse i de ordningene for utveksling av opplysninger som er nevnt i nr. 1, når deres medlemskap er godkjent, eller, alt etter hva som er relevant, ved opphør av medlemskapet når dette trer i kraft.

Kapittel VII

Vedkommende myndigheter

Artikkel 46

Vedkommende myndigheter

Med forbehold for bestemmelsene om overvåkingsrammeverket for kritiske tredjepartsleverandører av IKT-tjenester som nevnt i kapittel V avsnitt II i denne forordningen, skal overholdelse av denne forordningen sikres av følgende vedkommende myndigheter i samsvar med den myndigheten som tildeles gjennom respektive rettsakter:

a) For kredittinstitusjoner og for institusjoner som er unntatt i henhold til direktiv 2013/36/EU, den vedkommende myndigheten som er utpekt i samsvar med artikkel 4 i det nevnte direktivet, og for kredittinstitusjoner som er klassifisert som betydelige i samsvar med artikkel 6 nr. 4 i forordning (EU) nr. 1024/2013, Den europeiske sentralbank (ESB) i samsvar med den myndigheten og de oppgavene som er gitt i henhold til den nevnte forordningen.
b) For betalingsinstitusjoner, herunder betalingsinstitusjoner som er unntatt i henhold til direktiv (EU) 2015/2366, e-pengeforetak som er unntatt i henhold til direktiv 2009/110/EF, og ytere av kontoopplysningstjenester som omhandlet i artikkel 33 nr. 1 i direktiv (EU) 2015/2366, den vedkommende myndigheten som er utpekt i samsvar med artikkel 22 i direktiv (EU) 2015/2366.
c) For verdipapirforetak, den vedkommende myndigheten som er utpekt i samsvar med artikkel 4 i europaparlaments- og rådsdirektiv (EU) 2019/2034[38].
d) For tilbydere av kryptoeiendeler som er meddelt tillatelse i henhold til forordningen om markeder for kryptoeiendeler, og utstedere av kryptoeiendeler, den vedkommende myndigheten som er utpekt i samsvar med den relevante bestemmelsen i den nevnte forordningen.
e) For verdipapirsentraler, den vedkommende myndigheten som er utpekt i samsvar med artikkel 11 i forordning (EU) nr. 909/2014.
f) For sentrale motparter, den vedkommende myndigheten som er utpekt i samsvar med artikkel 22 i forordning (EU) nr. 648/2012.
g) For handelsplasser og leverandører av datarapporteringstjenester, den vedkommende myndigheten som er utpekt i samsvar med artikkel 67 i direktiv 2014/65/EU, og den vedkommende myndigheten som er definert i artikkel 2 nr. 1 punkt 18) i forordning (EU) nr. 600/2014.
h) For transaksjonsregistre, den vedkommende myndigheten som er utpekt i samsvar med artikkel 22 i forordning (EU) nr. 648/2012.
i) For forvaltere av alternative investeringsfond, den vedkommende myndigheten som er utpekt i samsvar med artikkel 44 i direktiv 2011/61/EU.
j) For forvaltningsselskaper, den vedkommende myndigheten som er utpekt i samsvar med artikkel 97 i direktiv 2009/65/EF.
k) For forsikrings- og gjenforsikringsforetak, den vedkommende myndigheten som er utpekt i samsvar med artikkel 30 i direktiv 2009/138/EF.
l) For forsikringsformidlere, gjenforsikringsformidlere og forsikringsformidlere som har forsikringsformidling som tilleggsvirksomhet, den vedkommende myndigheten som er utpekt i samsvar med artikkel 12 i direktiv (EU) 2016/97.
m) For tjenestepensjonsforetak, den vedkommende myndigheten som er utpekt i samsvar med artikkel 47 i direktiv (EU) 2016/2341.
n) For kredittvurderingsbyråer, den vedkommende myndigheten som er utpekt i samsvar med artikkel 21 i forordning (EF) nr. 1060/2009.
o) For administratorer av kritiske referanseverdier, den vedkommende myndigheten som er utpekt i samsvar med artikkel 40 og 41 i forordning (EU) 2016/1011.
p) For tilbydere av folkefinansieringstjenester, den vedkommende myndigheten som er

[38] Europaparlaments- og rådsdirektiv (EU) 2019/2034 av 27. november 2019 om tilsyn med verdipapirforetak og om endring av direktiv 2002/87/EF, 2009/65/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU og 2014/65/EU (EUT L 314 av 5.12.2019, s. 64).

utpekt i samsvar med artikkel 29 i forordning (EU) 2020/1503.

q) For verdipapiriseringsregistre, den vedkommende myndigheten som er utpekt i samsvar med artikkel 10 og artikkel 14 nr. 1 i forordning (EU) 2017/2402.

Artikkel 47

Samarbeid med strukturer og myndigheter som er opprettet ved direktiv (EU) 2022/2555

1. For å fremme samarbeid og muliggjøre tilsynsmessig utveksling mellom de vedkommende myndighetene som er utpekt i henhold til denne forordningen, og den samarbeidsgruppen som er opprettet ved artikkel 14 i direktiv (EU) 2022/2555, kan de europeiske tilsynsmyndighetene og de vedkommende myndighetene delta i samarbeidsgruppens virksomhet i saker som angår deres tilsynsvirksomhet i forbindelse med finansielle enheter. De europeiske tilsynsmyndighetene og de vedkommende myndighetene kan anmode om å bli invitert til å delta i samarbeidsgruppens virksomhet i saker som gjelder vesentlige eller viktige enheter som er omfattet av direktiv (EU) 2022/2555, og som også er utpekt som kritiske tredjepartsleverandører av IKT-tjenester i henhold til artikkel 31 i denne forordningen.
2. De vedkommende myndighetene kan, dersom det er relevant, rådføre seg og utveksle opplysninger med de felles kontaktpunktene og CSIRT-enhetene som er utpekt eller opprettet i samsvar med direktiv (EU) 2022/2555.
3. Dersom det er relevant, kan de vedkommende myndighetene anmode om en relevant teknisk uttalelse og bistand fra de vedkommende myndighetene som er utpekt eller opprettet i samsvar med direktiv (EU) 2022/2555, og inngå samarbeidsordninger, slik at det kan opprettes effektive og raske koordineringsordninger.
4. De ordningene som er nevnt i nr. 3 i denne artikkelen, kan blant annet angi framgangsmåtene for koordinering av tilsynsvirksomhet i forbindelse med vesentlige eller viktige enheter som er omfattet av direktiv (EU) 2022/2555, og som er utpekt som kritiske tredjepartsleverandører av IKT-tjenester i henhold til artikkel 31 i denne forordningen, herunder for gjennomføring, i samsvar med nasjonal rett, av undersøkelser og stedlige inspeksjoner, samt for ordninger for utveksling av opplysninger mellom de vedkommende myndighetene i henhold til denne forordningen og de vedkommende myndighetene som er utpekt eller opprettet i samsvar med det nevnte direktivet, og som omfatter tilgang til opplysninger som de sistnevnte myndighetene har anmodet om.

Artikkel 48

Samarbeid mellom myndigheter

1. De vedkommende myndighetene skal ha et nært samarbeid seg imellom og, dersom det er relevant, med hovedovervåkeren.
2. De vedkommende myndighetene og hovedovervåkeren skal i god tid utveksle alle relevante opplysninger om kritiske tredjepartsleverandører av IKT-tjenester som er nødvendige for at de skal kunne utføre sine respektive oppgaver i henhold til denne forordningen, særlig i forbindelse med identifiserte risikoer, tilnærminger og tiltak som er truffet som ledd i hovedovervåkerensovervåkingsoppgaver.

Artikkel 49

Øvelser, kommunikasjon og samarbeid mellom finanssektorer

1. De europeiske tilsynsmyndighetene kan gjennom Felleskomiteen og i samarbeid med de vedkommende myndighetene, krisehåndteringsmyndighetene nevnt i artikkel 3 i direktiv 2014/59/EU, ESB, Det felles krisehåndteringsråd når det gjelder opplysninger om enheter som er omfattet av virkeområdet for forordning (EU) nr. 806/2014, ESRB og ENISA, alt etter hva som er relevant, opprette ordninger som gjør det mulig å utveksle effektive framgangsmåter mellom ulike finanssektorer for å øke situasjonsbevisstheten og identifisere felles cybersårbarheter og -risikoer i ulike sektorer.

   De kan utarbeide krisestyrings- og beredskapsøvelser som omfatter cyberangrepsscenarioer, med henblikk på å utvikle kommunikasjonskanaler og gradvis muliggjøre en effektiv koordinert respons på unionsplan i tilfelle av en alvorlig grenseoverskridende IKT-relatert hendelse eller relatert trussel som har en systemisk virkning på Unionens finanssektor som helhet.

   Disse øvelsene kan, alt etter hva som er relevant, også omfatte testing av finanssektorens avhengighet av andre økonomiske sektorer.
2. De vedkommende myndighetene, de europeiske tilsynsmyndighetene og ESB skal

samarbeide nært med hverandre og utveksle opplysninger for å kunne utføre sine oppgaver i henhold til artikkel 47–54. De skal nøye koordinere tilsynet for å påvise og avhjelpe overtredelser av denne forordningen, utarbeide og fremme beste praksis, legge til rette for samarbeid, fremme konsekvens i tolkningen og utarbeide vurderinger på tvers av jurisdiksjoner dersom det oppstår eventuelle uenigheter.

Artikkel 50

Administrative sanksjoner og avhjelpende tiltak

1. De vedkommende myndighetene skal ha den tilsyns-, undersøkelses- og sanksjonsmyndigheten som er nødvendig for å sikre at de utfører sine oppgaver i henhold til denne forordningen.
2. Den myndigheten som er nevnt i nr. 1, skal minst omfatte myndighet til å
   a) få tilgang til alle dokumenter eller andre opplysninger i enhver form, som den vedkommende myndigheten anser for relevante for utførelsen av sine oppgaver, og få eller ta en kopi av dem,
   b) foreta stedlige inspeksjoner eller undersøkelser, som skal omfatte, men ikke er begrenset til
      i) å innkalle representanter for de finansielle enhetene og be dem om muntlige eller skriftlige redegjørelser for forhold eller dokumenter som berører gjenstanden for og formålet med undersøkelsen, samt registrere svarene,
      ii) å høre enhver fysisk eller juridisk person som går med på å bli hørt, for å samle inn opplysninger om gjenstanden for undersøkelsen,
   c) å kreve korrigerende og avhjelpende tiltak ved manglende oppfyllelse av kravene i denne forordningen.
3. Uten at det berører medlemsstatenes rett til å pålegge strafferettslige sanksjoner i samsvar med artikkel 52, skal medlemsstatene fastsette regler om egnede administrative sanksjoner og avhjelpende tiltak ved overtredelse av denne forordningen og sikre at de gjennomføres på en effektiv måte.

   Disse sanksjonene og tiltakene skal være virkningsfulle, stå i rimelig forhold til overtredelsen og virke avskrekkende.
4. Medlemsstatene skal gi vedkommende myndigheter myndighet til å anvende minst følgende administrative sanksjoner eller avhjelpende tiltak ved overtredelse av denne forordningen:
   a) Å utstede et pålegg der det kreves at den fysiske eller juridiske personen avslutter den atferden som utgjør en overtredelse av denne forordningen, og ikke gjentar slik atferd.
   b) Å kreve midlertidig eller varig opphør av enhver praksis eller atferd som den vedkommende myndigheten anser å være i strid med bestemmelsene i denne forordningen, og forhindre at praksisen eller atferden gjentas.
   c) Å treffe enhver form for tiltak, herunder av økonomisk karakter, for å sikre at finansielle enheter fortsatt oppfyller de rettslige kravene.
   d) Å kreve, i den utstrekning det er tillatt i henhold til nasjonal rett, utlevering av eksisterende opplysninger om datatrafikk som oppbevares av en teleoperatør, dersom det foreligger en begrunnet mistanke om en overtredelse av denne forordningen, og dersom disse opplysningene kan være relevante for en undersøkelse av overtredelser av denne forordningen.
   e) Å utstede kunngjøringer, herunder offentlige erklæringer som identifiserer den ansvarlige fysiske eller juridiske personen og overtredelsens art.
5. Dersom nr. 2 bokstav c) og nr. 4 får anvendelse på juridiske personer, skal medlemsstatene gi vedkommende myndigheter myndighet til å anvende de administrative sanksjonene og de avhjelpende tiltakene, med forbehold for de vilkårene som er fastsatt i nasjonal rett, på medlemmer av ledelsesorganet og på andre fysiske personer som i henhold til nasjonal rett er ansvarlige for overtredelsen.
6. Medlemsstatene skal sikre at enhver beslutning om påleggelse av administrative sanksjoner eller avhjelpende tiltak i henhold til nr. 2 bokstav c), er behørig begrunnet og kan påklages.

Artikkel 51

Utøvelse av myndigheten til å pålegge administrative sanksjoner og treffe avhjelpende tiltak

1. De vedkommende myndighetene skal utøve sin myndighet til å pålegge administrative sanksjoner og treffe avhjelpende tiltak som nevnt i artikkel 50 i samsvar med sine nasjo-

nale rettslige rammer, alt etter hva som er relevant, på følgende måte:
a) Direkte.
b) I samarbeid med andre myndigheter.
c) På eget ansvar ved delegering til andre myndigheter.
d) Ved anmodning til de vedkommende rettsmyndighetene.

2. De vedkommende myndighetene skal når de bestemmer typen av og nivået på en administrativ sanksjon eller et avhjelpende tiltak som pålegges eller treffes i henhold til artikkel 50, ta hensyn til i hvilken grad overtredelsen er begått med forsett eller skyldes uaktsomhet, og til alle andre relevante omstendigheter, herunder følgende, dersom det er relevant:
a) Overtredelsens vesentlighet, grovhet og varighet.
b) Graden av ansvar hos den fysiske eller juridiske personen som er ansvarlig for overtredelsen.
c) Den ansvarlige fysiske eller juridiske personens finansielle styrke.
d) Betydningen av den fortjenesten som er oppnådd, eller det tapet som er unngått av den ansvarlige fysiske eller juridiske personen, i den grad dette kan fastslås.
e) De tapene for tredjeparter som skyldes overtredelsen, i den grad dette kan fastslås.
f) Den ansvarlige fysiske eller juridiske personens vilje til å samarbeide med den vedkommende myndigheten, uten at det berører behovet for å sikre tilbakebetaling av den fortjenesten som den fysiske eller juridiske personens har oppnådd, eller de tapene som denne har unngått.
g) Tidligere overtredelser begått av den ansvarlige fysiske eller juridiske personen.

Artikkel 52

Strafferettslige sanksjoner

1. Medlemsstatene kan beslutte ikke å innføre administrative sanksjoner eller avhjelpende tiltak for overtredelser som er omfattet av strafferettslige sanksjoner i henhold til nasjonal rett.
2. Dersom medlemsstatene har valgt å fastsette strafferettslige sanksjoner for overtredelser av denne forordningen, skal de sikre at det er truffet hensiktsmessige tiltak slik at vedkommende myndigheter har all nødvendig myndighet til å holde kontakt med rettsmyndigheter, påtalemyndigheter eller strafferettslige myndigheter innenfor sin jurisdiksjon for å få konkrete opplysninger om strafferettslige etterforskninger eller rettssaker som er innledet på grunn av overtredelser av denne forordningen, og til å gi andre vedkommende myndigheter samt EBA, ESMA eller EIOPA de samme opplysningene, slik at de kan oppfylle sine forpliktelser om å samarbeide om anvendelsen av denne forordningen.

Artikkel 53

Underretningsplikt

Medlemsstatene skal innen 17. januar 2025 underrette Kommisjonen, ESMA, EBA og EIOPA om de lovene og forskriftene, herunder eventuelle relevante strafferettslige bestemmelser, som gjennomfører dette kapittelet. Medlemsstatene skal uten unødig opphold underrette Kommisjonen, ESMA, EBA og EIOPA om eventuelle senere endringer av dem.

Artikkel 54

Offentliggjøring av administrative sanksjoner

1. De vedkommende myndighetene skal uten unødig opphold offentliggjøre på sine offisielle nettsteder enhver avgjørelse om påleggelse av en administrativ sanksjon som ikke kan påklages, etter at mottakeren av sanksjonen er blitt underrettet om avgjørelsen.
2. Offentliggjøringen nevnt i nr. 1 skal inneholde opplysninger om overtredelsens type og art, identiteten til de ansvarlige personene og sanksjonene som er pålagt.
3. Dersom den vedkommende myndigheten etter en individuell vurdering anser at offentliggjøringen av juridiske personers identitet, eller fysiske personers identitet eller personopplysninger, vil være uforholdsmessig, herunder omfatte risikoer i forbindelse med vernet av personopplysninger, vil være til skade for finansmarkedenes stabilitet eller for en pågående strafferettslig etterforskning eller, i den grad dette kan fastslås, volde den berørte personen uforholdsmessig skade, skal den vedkommende myndigheten treffe et av følgende tiltak med hensyn til avgjørelsen om å pålegge en administrativ sanksjon:
a) Utsette offentliggjøringen av avgjørelsen inntil det ikke lenger finnes noen grunn til ikke å offentliggjøre den.
b) Offentliggjøre avgjørelsen anonymt i samsvar med nasjonal rett.
c) Avstå fra å offentliggjøre avgjørelsen dersom de alternativene som angis i bokstav a)

og b), ikke anses for å være tilstrekkelige for å sikre at finansmarkedenes stabilitet ikke på noen som helst måte bringes i fare, eller dersom en slik offentliggjøring ikke er forholdsmessig når det gjelder mindre strenge sanksjoner.

4. Når det gjelder en avgjørelse om å offentliggjøre en administrativ sanksjon i anonymisert form i samsvar med nr. 3 bokstav b), kan offentliggjøringen av de relevante opplysningene utsettes.
5. Dersom en vedkommende myndighet offentliggjør en avgjørelse om påleggelse av en administrativ sanksjon som kan påklages til de relevante rettsmyndighetene, skal de vedkommende myndighetene dessuten på sitt offisielle nettsted uten unødig opphold offentliggjøre disse opplysningene sammen med eventuelle senere opplysninger om utfallet av en slik klage på et senere tidspunkt. Enhver rettsavgjørelse om oppheving av en avgjørelse om påleggelse av en administrativ sanksjon skal også offentliggjøres.
6. De vedkommende myndighetene skal sikre at enhver offentliggjøring som nevnt i nr. 1–4, bare er tilgjengelig på deres offisielle nettsted i den tidsperioden som er nødvendig ved anvendelse av denne artikkelen. Denne perioden skal ikke overstige fem år etter offentliggjøringen.

Artikkel 55

Taushetsplikt

1. Alle fortrolige opplysninger som mottas, utveksles eller overføres i henhold til denne forordningen, skal være underlagt vilkårene for taushetsplikt som er fastsatt i nr. 2.
2. Taushetsplikten gjelder alle personer som arbeider eller har arbeidet for de vedkommende myndighetene i henhold til denne forordningen, eller for enhver myndighet, markedsaktør eller fysisk eller juridisk person som de vedkommende myndighetene har delegert myndighet til, herunder revisorer og eksperter som de vedkommende myndighetene har inngått kontrakt med.
3. Opplysninger som er omfattet av taushetsplikt, herunder utveksling av opplysninger mellom vedkommende myndigheter i henhold til denne forordningen og vedkommende myndigheter som er utpekt eller opprettet i samsvar med direktiv (EU) 2022/2555, skal ikke gis videre til noen annen person eller myndighet, unntatt når dette skjer i henhold til bestemmelser i unionsretten eller nasjonal rett.
4. Alle opplysninger som utveksles mellom de vedkommende myndighetene i henhold til denne forordningen, og som gjelder forretnings- eller driftsforhold og andre økonomiske eller personlige forhold, skal anses som fortrolige og omfattes av kravene om taushetsplikt, unntatt når den vedkommende myndigheten på det tidspunkt opplysningene meddeles, erklærer at opplysningene kan gis videre, eller når videreformidling er nødvendig i forbindelse med rettsforfølgning.

Artikkel 56

Vern av personopplysninger

1. De europeiske tilsynsmyndighetene og de vedkommende myndighetene skal bare behandle personopplysninger dersom det er nødvendig for at de skal kunne oppfylle sine respektive forpliktelser og utføre sine oppgaver i henhold til denne forordningen, særlig med hensyn til undersøkelse, inspeksjon, anmodning om opplysninger, kommunikasjon, offentliggjøring, evaluering, verifisering, vurdering og utarbeiding av tilsynsplaner. Personopplysningene skal behandles i samsvar med forordning (EU) 2016/679 eller forordning (EU) 2018/1725, alt etter hvilken som får anvendelse.
2. Med mindre annet er fastsatt i andre sektorspesifikke rettsakter, skal de personopplysningene som er nevnt i nr. 1, lagres fram til de relevante tilsynsoppgavene er utført og under alle omstendigheter i høyst 15 år, unntatt i tilfelle av pågående rettssaker som krever ytterligere lagring av slike opplysninger.

Kapittel VIII

Delegerte rettsakter

Artikkel 57

Utøvelse av delegert myndighet

1. Myndigheten til å vedta delegerte rettsakter gis Kommisjonen med forbehold for vilkårene fastsatt i denne artikkelen.
2. Myndigheten til å vedta delegerte rettsakter nevnt i artikkel 31 nr. 6 og artikkel 43 nr. 2 skal gis Kommisjonen for en periode på fem år fra 17. januar 2024. Kommisjonen skal utarbeide en rapport om den delegerte myndigheten senest ni måneder før utløpet av femårsperioden. Den delegerte myndigheten skal stilltiende forlenges med perioder av samme

varighet, med mindre Europaparlamentet eller Rådet motsetter seg slik forlengelse senest tre måneder før utløpet av hver periode.

3. Europaparlamentet eller Rådet kan når som helst tilbakekalle den delegerte myndigheten nevnt i artikkel 31 nr. 6 og artikkel 43 nr. 2. En beslutning om tilbakekalling innebærer at den delegerte myndigheten som angis i beslutningen, opphører å gjelde. Den får virkning dagen etter at beslutningen er kunngjort i Den europeiske unions tidende, eller på et senere tidspunkt angitt i beslutningen. Den berører ikke gyldigheten av delegerte rettsakter som allerede er trådt i kraft.
4. Før Kommisjonen vedtar en delegert rettsakt, skal den høre eksperter som er utpekt av hver medlemsstat i samsvar med prinsippene fastsatt i den tverrinstitusjonelle avtalen av 13. april 2016 om bedre regelverksutforming.
5. Så snart Kommisjonen vedtar en delegert rettsakt, skal den underrette Europaparlamentet og Rådet samtidig om dette.
6. En delegert rettsakt vedtatt i henhold til artikkel 31 nr. 6 og artikkel 43 nr. 2 skal tre i kraft bare dersom verken Europaparlamentet eller Rådet har gjort innsigelse mot rettsakten innen en frist på tre måneder etter at rettsakten ble meddelt Europaparlamentet eller Rådet, eller dersom Europaparlamentet og Rådet innen utløpet av denne fristen begge har underrettet Kommisjonen om at de ikke kommer til å gjøre innsigelse. På Europaparlamentets eller Rådets initiativ forlenges denne fristen med tre måneder.

Kapittel IX

Overgangs- og sluttbestemmelser

Avsnitt I

Artikkel 58

Revisjonsklausul

1. Etter høring av de europeiske tilsynsmyndighetene og ESRB skal Kommisjonen innen 17. januar 2028, alt etter hva som er relevant, utføre en revisjon og legge fram en rapport for Europaparlamentet og Rådet, eventuelt ledsaget av et forslag til regelverk. Revisjonen skal minst omfatte følgende:
   a) Kriteriene for utpeking av kritiske tredjepartsleverandører av IKT-tjenester i samsvar med artikkel 31 nr. 2.
   b) Den frivillige karakteren av underretningen om betydelige cybertrusler som er nevnt i artikkel 19.
   c) Den ordningen som er nevnt i artikkel 31 nr. 12 og hovedovervåkerens myndighet fastsatt i artikkel 35 nr. 1 bokstav d) iv) første ledd, med henblikk på å vurdere effektiviteten av disse bestemmelsene med hensyn til å sikre et effektivt tilsyn med kritiske tredjepartsleverandører av IKT-tjenester som er etablert i et tredjeland, og nødvendigheten av å etablere et datterforetak i Unionen.

      Ved anvendelse av første ledd i denne bokstaven skal revisjonen inneholde en analyse av ordningen nevnt i artikkel 31 nr. 12, herunder med hensyn til tilgangen for finansielle enheter i Unionen til tjenester fra tredjeland og tilgang til slike tjenester på markedet i Unionen, og den skal ta hensyn til den fortsatte utviklingen på markedene for de tjenestene som er omfattet av denne forordningen, finansielle enheters og finansielle tilsynsmyndigheters praktiske erfaring med hensyn til henholdsvis anvendelsen av og tilsynet med den ordningen, og enhver relevant utvikling innen regulering og tilsyn som finner sted på internasjonalt plan.
   d) Hensiktsmessigheten av å la de finansielle enhetene som er nevnt i artikkel 2 nr. 3 bokstav e), og som bruker automatiserte salgssystemer, være omfattet av denne forordningens virkeområde på bakgrunn av den framtidige markedsutviklingen når det gjelder bruken av slike systemer.
   e) Det felles tilsynsnettverkets funksjon og effektivitet når det gjelder å støtte konsekvens i tilsynet og effektivitet i utvekslingen av opplysninger innenfor overvåkingsrammeverket.
2. I forbindelse med revisjonen av direktiv (EU) 2015/2366 skal Kommisjonen vurdere behovet for økt motstandsdyktighet mot cyberangrep i betalingssystemer og betalingsbehandlingsaktiviteter og hensiktsmessigheten av å utvide virkeområdet for denne forordningen til å omfatte operatører av betalingssystemer og enheter som er involvert i betalingsbehandlingsaktiviteter. På bakgrunn av denne vurderingen skal Kommisjonen, som en del av revisjonen av direktiv (EU) 2015/2366, legge fram en rapport for Europaparlamentet og Rådet senest 17. juli 2023.

   På grunnlag av denne revisjonsrapporten og etter høring av de europeiske tilsynsmyndighetene, ESB og ESRB, kan Kommisjonen, dersom det er relevant, og som en del av det

lovforslaget som den kan vedta i henhold til artikkel 108 andre ledd i direktiv (EU) 2015/2366, legge fram et forslag for å sikre at alle operatører av betalingssystemer og enheter som er involvert i betalingsbehandlingsaktiviteter, er omfattet av et hensiktsmessig tilsyn, samtidig som det tas hensyn til sentralbankens eksisterende tilsyn.

3. Innen 17. januar 2026 skal Kommisjonen, etter høring av de europeiske tilsynsmyndighetene og Komiteen for europeiske tilsynsorganer, utføre en revisjon og oversende en rapport til Europaparlamentet og Rådet, eventuelt ledsaget av et lovforslag, om hensiktsmessigheten av strengere krav til revisorer og revisjonsselskaper med hensyn til digital operasjonell motstandsdyktighet, ved å la revisorer og revisjonsselskaper bli omfattet av denne forordningens virkeområde eller ved å endre europaparlaments- og rådsdirektiv 2006/43/EF[39].

Avsnitt II

Endringer

Artikkel 59

Endringer av forordning (EF) nr. 1060/2009

I forordning (EF) nr. 1060/2009 gjøres følgende endringer:

1) I vedlegg I avsnitt A nr. 4 skal første ledd lyde:

«Et kredittvurderingsbyrå skal ha god forvaltnings- og regnskapspraksis, internkontrollordninger, effektive framgangsmåter for risikovurdering og effektive kontroll- og sikkerhetsordninger for forvaltning av IKT-systemer i henhold til europaparlaments- og rådsforordning (EU) 2022/2554(*).

(*) Europaparlaments,- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 av 27.12.2022, s.1).»

2) I vedlegg III skal nr. 12 lyde:

«12.Kredittvurderingsbyrået overtrer artikkel 6 nr. 2, sammenholdt med vedlegg I avsnitt A nr. 4, dersom det ikke har god forvaltnings- og regnskapspraksis, internkontrollordninger, effektive framgangsmåter for risikovurdering og effektive kontroll- og sikkerhetsordninger for forvaltning av IKT-systemer i samsvar med forordning (EU) 2022/2554, eller dersom det ikke gjennomfører og opprettholder framgangsmåter for beslutningstaking eller organisasjonsstrukturer slik det kreves i det nevnte nummeret».

Artikkel 60

Endringer av forordning (EU) nr. 648/2012

I forordning (EU) nr. 648/2012 gjøres følgende endringer:

1) I artikkel 26 gjøres følgende endringer:
   a) Nr. 3 skal lyde:

«3. En sentral motpart skal opprettholde en organisasjonsstruktur som sikrer kontinuitet og regelmessighet i leveringen av tjenester og utøvelsen av virksomhet. Den skal anvende egnede og forholdsmessige systemer, ressurser og framgangsmåter, herunder IKT-systemer som forvaltes i samsvar med europaparlaments- og rådsforordning (EU) 2022/2554(*).

(*) Europaparlaments,- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 av 27.12.2022, s.1).»

   b) Nr. 6 utgår.

2) I artikkel 34 gjøres følgende endringer:
   a) Nr. 1 skal lyde:

«1. En sentral motpart skal utarbeide, gjennomføre og opprettholde egnede retningslinjer for kontinuitet i virksomheten og en katastrofeberedskapsplan som skal omfatte retningslinjer for IKT-kontinuitet i virksomheten og planer for IKT-respons- og -gjenoppretting, som er utarbeidet og gjennomført i samsvar med forordning (EU) 2022/2554, og som har som formål å sikre opprettholdelse av dens funksjoner, sikre rask gjenopptakelse av driften og oppfyllelse av den sentrale motpartens forpliktelser.»

   b) I nr. 3 skal første ledd lyde:

«3. For å sikre en ensartet anvendelse av denne artikkelen skal ESMA etter høring av ESSB-medlemmene utar-

[39] Europaparlaments- og rådsdirektiv 2006/43/EF av 17. mai 2006 om lovfestet revisjon av årsregnskap og konsernregnskap, om endring av rådsdirektiv 78/660/EØF og 83/349/EØF og om oppheving av rådsdirektiv 84/253/EØF (EUT L 157 av 9.6.2006, s. 87).

beide utkast til tekniske reguleringsstandarder med nærmere opplysninger om hva retningslinjene for kontinuitet i virksomheten og katastrofeberedskapsplanen minst skal inneholde, unntatt retningslinjer for IKT-kontinuitet i virksomheten og katastrofeberedskapsplaner.»

3) I artikkel 56 nr. 3 skal første ledd lyde:
«3. For å sikre en ensartet anvendelse av denne artikkelen skal ESMA utarbeide utkast til tekniske reguleringsstandarder med nærmere opplysninger om den søknaden om registrering som er nevnt i nr. 1, men ikke opplysninger om krav til IKT-risikostyring».
4) I artikkel 79 skal nr. 1 og 2 lyde:
«1. Et transaksjonsregister skal kartlegge kildene til operasjonell risiko og minimere dem ved å utvikle egnede systemer, kontroller og framgangsmåter, herunder IKT-systemer som forvaltes i samsvar med forordning (EU) 2022/2554.
2. Et transaksjonsregister skal utarbeide, gjennomføre og opprettholde egnede retningslinjer for kontinuitet i virksomheten og katastrofeberedskapsplan, herunder retningslinjer for IKT-kontinuitet i virksomheten og planer for IKT-respons- og -gjenoppretting utarbeidet i samsvar med (EU) 2022/2554, som har som formål å sikre opprettholdelsen av registerets funksjoner, og sikre rask gjenopptakelse av driften og oppfyllelse av transaksjonsregisterets forpliktelser.»
5) I artikkel 80 utgår nr. 1.
6) I vedlegg I avsnitt II gjøres følgende endringer:
a) Bokstav a) og b) skal lyde:
«a) Et transaksjonsregister overtrer artikkel 79 nr. 1 dersom det ikke kartlegger kildene til operasjonell risiko og minimerer dem, ved å utvikle egnede systemer, kontroller og framgangsmåter, herunder IKT-systemer som forvaltes i samsvar med forordning (EU) 2022/2554.
b) Et transaksjonsregister overtrer artikkel 79 nr. 2 dersom det ikke utarbeider, gjennomfører og opprettholder egnede retningslinjer for kontinuitet i virksomheten og en katastrofeberedskapsplan utarbeidet i samsvar med forordning (EU) 2022/2554, som har som formål å sikre opprettholdelse av registerets funksjoner, sikre rask gjenopptakelse av driften og oppfyllelse av transaksjonsregisterets forpliktelser.»
b) Bokstav c) utgår.
7) I vedlegg III gjøres følgende endringer:
a) I avsnitt II gjøres følgende endringer:
i) Bokstav c) skal lyde:
«c) En sentral motpart i kategori 2 overtrer artikkel 26 nr. 3 dersom den ikke opprettholder en organisasjonsstruktur som sikrer kontinuitet og regelmessighet i leveringen av tjenester og utøvelsen av virksomhet, eller ikke benytter hensiktsmessige og tilpassede systemer, ressurser og framgangsmåter, herunder IKT-systemer som forvaltes i samsvar med forordning (EU) 2022/2554.»
ii) Bokstav f) utgår.
b) I avsnitt III skal bokstav a) lyde:
«a) En sentral motpart i kategori 2 overtrer artikkel 34 nr. 1 dersom den ikke fastsetter, gjennomfører eller opprettholder egnede retningslinjer for kontinuitet i virksomheten og en respons- og gjenopprettingsplan utarbeidet i samsvar med forordning (EU) 2022/2554, som har som formål å sikre opprettholdelsen av den sentrale motpartens funksjoner, sikre rask gjenopptakelse av virksomheten og oppfyllelse av den sentrale motpartens forpliktelser, og som minst gjør det mulig å gjenopprette alle transaksjoner fra det tidspunktet da de ble avbrutt, slik at den sentrale motpartens drift fortsatt er sikker, og den kan gjennomføre oppgjør på den planlagte datoen.»

Artikkel 61

Endringer av forordning (EU) nr. 909/2014

I artikkel 45 i forordning (EU) nr. 909/2014 gjøres følgende endringer:

1) Nr. 1 skal lyde:
«1. En verdipapirsentral skal identifisere både interne og eksterne kilder til operasjonell risiko og begrense deres virkning ved å anvende egnede IKT-verktøyer, -prosesser og -retningslinjer som er fastsatt og forvaltet i samsvar med europaparlaments- og rådsforordning (EU) 2022/2554(*), samt ved å anvende eventuelle andre relevante verktøyer, kontroller og framgangsmåter

for andre typer av operasjonell risiko, herunder for alle de verdipapiroppgjørssystemene som den driver.

(*) Europaparlaments,- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 av 27.12.2022, s.1).»

2) Nr. 2 utgår.
3) Nr. 3 og 4 skal lyde:
«3. En verdipapirsentral skal for tjenester som den yter, og for hvert verdipapiroppgjørssystem som den driver, utarbeide, gjennomføre og opprettholde egnede retningslinjer for kontinuitet i virksomheten og en katastrofeberedskapsplan, herunder retningslinjer for IKT-kontinuitet i virksomheten og planer for IKT-respons- og -gjenoppretting utarbeidet i samsvar med forordning (EU) 2022/2554, som har som formål å sikre opprettholdelsen av dens tjenester, sikre rask gjenopptakelse av driften og oppfyllelse av verdipapirsentralens forpliktelser i tilfelle av hendelser som medfører betydelig risiko for driftsavbrudd.

4. Planen nevnt i nr. 3 skal gjøre det mulig å gjenopprette alle transaksjoner og deltakeres posisjoner fra det tidspunktet da de ble avbrutt, slik at verdipapirsentralens deltakere fortsatt kan utøve sin virksomhet på en sikker måte og oppgjøret kan gjennomføres på den planlagte datoen, herunder ved å sikre at kritiske IT-systemer umiddelbart kan gjenoppta driften fra det tidspunktet da de ble avbrutt, som fastsatt i artikkel 12 nr. 5 og 7 i forordning (EU) 2022/2554.»

4) Nr. 6 skal lyde:
«6. En verdipapirsentral skal identifisere, overvåke og håndtere de risikoene som de viktigste deltakerne i de verdipapiroppgjørssystemene som den driver, samt tjenesteytere, andre verdipapirsentraler eller andre markedsinfrastrukturer kan utgjøre for dens virksomhet. Den skal på anmodning gi vedkommende og berørte myndigheter opplysninger om enhver slik risiko som er identifisert. Den skal også umiddelbart underrette den vedkommende myndigheten og berørte myndigheter om eventuelle operasjonelle hendelser som følge av slike risikoer, med unntak av IKT-risiko».

5) I nr. 7 skal første ledd lyde:
«7. ESMA skal i nært samarbeid med ESSB-medlemmene utarbeide utkast til tekniske reguleringsstandarder med nærmere opplysninger om de operasjonelle risikoene nevnt i nr. 1 og 6, med unntak av IKT-risiko, og metodene for å utprøve, håndtere eller minimere disse risikoene, herunder retningslinjene for kontinuitet i virksomheten og katastrofeberedskapsplanene nevnt i nr. 3 og 4 samt metodene for å vurdere disse.»

Artikkel 62

Endringer av forordning (EU) nr. 600/2014

I forordning (EU) nr. 600/2014 gjøres følgende endringer:

1) I artikkel 27g gjøres følgende endringer:
a) Nr. 4 skal lyde:
«4. En godkjent offentliggjøringsordning skal oppfylle kravene til sikkerheten i nettverks- og informasjonssystemer fastsatt i europaparlaments- og rådsforordning (EU) 2022/2554(*).

(*) Europaparlaments,- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 av 27.12.2022, s.1).»
b) I nr. 8 skal bokstav c) lyde:
«c) de konkrete organisatoriske kravene fastsatt i nr. 3 og 5,»

2) I artikkel 27h gjøres følgende endringer:
a) Nr. 5 skal lyde:
«5. En leverandør av et konsolidert offentliggjøringssystem skal oppfylle kravene til sikkerheten i nettverks- og informasjonssystemer fastsatt i forordning (EU) 2022/2554.»
b) I nr. 8 skal bokstav e) lyde:
«e) de konkrete organisatoriske kravene fastsatt i nr. 4.»

3) I artikkel 27i gjøres følgende endringer:
a) Nr. 3 skal lyde:
«3. En godkjent rapporteringsordning skal oppfylle kravene til sikkerheten i nettverks- og informasjonssystemer fastsatt i forordning (EU) 2022/2554.»
b) I nr. 5 skal bokstav b) lyde:
«b) de konkrete organisatoriske kravene fastsatt i nr. 2 og 4.»

Artikkel 63

Endring av forordning (EU) 2016/1011

I artikkel 6 i forordning (EU) 2016/1011 skal nytt nummer lyde:

«6. For kritiske referanseverdier skal en administrator ha god forvaltnings- og regnskapspraksis, internkontrollordninger, effektive framgangsmåter for risikovurdering og effektive kontroll- og sikkerhetsordninger for forvaltning av IKT-systemer i samsvar med europaparlaments- og rådsforordning (EU) 2022/2554(*).

(*) Europaparlaments,- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 av 27.12.2022, s.1).»

Artikkel 64

Ikrafttredelse og anvendelse

Denne forordningen trer i kraft den 20. dagen etter at den er kunngjort i *Den europeiske unions tidende*.

Den får anvendelse fra 17. januar 2025.

Denne forordningen er bindende i alle deler og kommer direkte til anvendelse i alle medlemsstater.

Utferdiget i Strasbourg 14. desember 2022.

For Europaparlamentet	*For Rådet*
R. Metsola	M. Bek
President	*Formann*

Vedlegg 2

Europaparlaments- og rådsdirektiv (EU) 2022/2556 av 14. desember 2022 om endring av direktiv 2009/65/EF, 2009/138/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 og (EU) 2016/2341 med hensyn til digital operasjonell motstandsdyktighet i finanssektoren

EUROPAPARLAMENTET OG RÅDET FOR DEN EUROPEISKE UNION HAR

under henvisning til traktaten om Den europeiske unions virkemåte, særlig artikkel 53 nr. 1 og artikkel 114,

under henvisning til forslag fra Europakommisjonen,

etter oversending av utkast til regelverksakt til de nasjonale parlamentene,

under henvisning til uttalelse fra Den europeiske sentralbank[1],

under henvisning til uttalelse fra Den europeiske økonomiske og sosiale komité[2],

etter den ordinære regelverksprosedyren[3] og

ut fra følgende betraktninger:

1) Unionen skal på en tilstrekkelig og grundig måte håndtere digitale risikoer for alle finansielle enheter som følge av økt bruk av informasjons- og kommunikasjonsteknologi (IKT) i forbindelse med levering og forbruk av finansielle tjenester, og dermed bidra til å realisere potensialet for digital finansiering med hensyn til å styrke innovasjon og fremme konkurranse i et sikkert digitalt miljø.
2) Finansielle enheter er svært avhengige av bruken av digital teknologi i sin daglige virksomhet. Det er derfor svært viktig å sikre deres digitale aktiviteters operasjonelle motstandsdyktighet mot IKT-risiko. Dette behovet er blitt enda mer presserende på grunn av veksten i banebrytende teknologier på markedet, særlig de teknologiene som gjør det mulig å overføre og lagre digitale uttrykk for en verdi eller for en rettighet elektronisk ved bruk av desentralisert registerteknologi eller lignende teknologi (kryptoeiendeler), og for tjenester knyttet til disse eiendelene.
3) På unionsplan er kravene til styring av IKT-risiko i finanssektoren for tiden fastsatt i europaparlaments- og rådsdirektiv 2009/65/EF[4], 2009/138/EF[5], 2011/61/EU[6], 2013/36/EU[7], 2014/59/EU[8], 2014/65/EU[9], (EU) 2015/2366[10] og (EU) 2016/2341[11].

---

1 EUT C 343 av 26.8 2021, s. 1.

2 EUT C 155 av 30.4. 2021, s. 38.

3 Europaparlamentets holdning av 10. november 2022 (ennå ikke offentliggjort i EUT) og rådsbeslutning av 28. november 2022.

4 Europaparlaments- og rådsdirektiv 2009/65/EF av 13. juli 2009 om samordning av lover og forskrifter om foretak for kollektiv investering i omsettelige verdipapirer (UCITS) (EUT L 302 av 17.11.2009, s. 32).

5 Europaparlaments- og rådsdirektiv 2009/138/EF av 25. november 2009 om adgang til å starte og utøve virksomhet innen forsikring og gjenforsikring (Solvens II) (EUT L 335 av 17.12.2009, s. 1).

6 Europaparlaments- og rådsdirektiv 2011/61/EU av 8. juni 2011 om forvaltere av alternative investeringsfond og om endring av direktiv 2003/41/EF og 2009/65/EF og forordning (EF) nr. 1060/2009 og (EU) nr. 1095/2010 (EUT L 174 av 1.7.2011, s. 1).

7 Europaparlaments- og rådsdirektiv 2013/36/EU av 26. juni 2013 om adgang til å utøve virksomhet som kredittinstitusjon og om tilsyn med kredittinstitusjoner, om endring av direktiv 2002/87/EF og om oppheving av direktiv 2006/48/EF og 2006/49/EF (EUT L 176 av 27.6.2013, s. 338).

8 Europaparlaments- og rådsdirektiv 2014/59/EU av 15. mai 2014 om fastsettelse av en ramme for gjenoppretting og krisehåndtering av kredittinstitusjoner og verdipapirforetak og om endring av rådsdirektiv 82/891/EØF, europaparlaments- og rådsdirektiv 2001/24/EF, 2002/47/EF, 2004/25/EF, 2005/56/EF, 2007/36/EF, 2011/35/EU, 2012/30/EU og 2013/36/EU og europaparlaments- og rådsforordning (EU) nr. 1093/2010 og (EU) nr. 648/2012 (EUT L 173 av 12.6.2014, s. 190).

9 Europaparlaments- og rådsdirektiv 2014/65/EU av 15. mai 2014 om markeder for finansielle instrumenter og om endring av direktiv 2002/92/EF og direktiv 2011/61/EU (EUT L 173 av 12.6.2014, s. 349).

10 Europaparlaments- og rådsdirektiv (EU) 2015/2366 av 25. november 2015 om betalingstjenester i det indre marked, om endring av direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om oppheving av direktiv 2007/64/EF (EUT L 337 av 23.12.2015, s. 35).

11 Europaparlaments- og rådsdirektiv (EU) 2016/2341 av 14. desember 2016 om virksomhet i og tilsyn med tjenestepensjonsforetak (EUT L 354 av 23.12.2016, s. 37).

Disse kravene er forskjellige og i noen tilfeller ufullstendige. IKT-risikoen er i noen tilfeller bare blitt behandlet indirekte som en del av den operasjonelle risikoen, mens den i andre tilfeller ikke er blitt behandlet i det hele tatt. Disse problemene utbedres ved å vedta europaparlaments- og rådsforordning (EU) 2022/2554[12]. Disse direktivene bør derfor endres for å sikre samsvar med den nevnte forordningen. I dette direktivet vedtas en rekke endringer som er nødvendige for å skape juridisk klarhet og sammenheng med hensyn til hvordan finansielle enheter som er meddelt tillatelse og underlagt tilsyn i samsvar med de nevnte direktivene, skal anvende ulike krav til digital operasjonell motstandsdyktighet som er nødvendige for at de skal kunne utøve sin virksomhet og levere tjenester, og dermed garantere at det indre marked fungerer på en tilfredsstillende måte. Det er nødvendig å sikre at disse kravene er forenlige med markedsutviklingen, samtidig som det oppmuntres til forholdsmessighet, særlig med hensyn til størrelsen på finansielle enheter og de særskilte ordningene som de er omfattet av, med henblikk på å redusere overholdelseskostnadene.

4) Når det gjelder banktjenester, fastsetter direktiv 2013/36/EU i øyeblikket bare generelle regler om intern styring og bestemmelser om operasjonell risiko som inneholder krav til beredskapsplaner og planer for kontinuitet i virksomheten, som underforstått tjener som grunnlag for å håndtere IKT-risiko. For å håndtere IKT-risiko eksplisitt og tydelig bør imidlertid kravene til beredskapsplaner og planer for kontinuitet i virksomheten endres slik at de også omfatter planer for kontinuitet i virksomheten samt respons- og gjenopprettingsplaner vedrørende IKT-risiko i samsvar med kravene fastsatt i forordning (EU) 2022/2554. Dessuten inngår IKT-risiko bare indirekte, som en del av den operasjonelle risikoen, i tilsyns- og evalueringsprosessen (SREP) som utføres av vedkommende myndigheter, og kriteriene for vurderingen av den er i øyeblikket fastsatt i retningslinjene for IKT-risikovurdering innenfor rammen av tilsyns- og evalueringsprosessen (SREP), som er utstedt av Den europeiske tilsynsmyndighet (Den europeiske banktilsynsmyndighet) (EBA), som ble opprettet ved europaparlaments- og rådsforordning (EU) nr. 1093/2010[13]. For å skape juridisk klarhet og sikre at banktilsynsmyndighetene effektivt avdekker IKT-risiko, og overvåker finansielle enheters styring av den, i tråd med det nye rammeverket for digital operasjonell motstandsdyktighet, bør virkeområdet for tilsyns- og evalueringsprosessen (SREP) også endres slik at det uttrykkelig viser til kravene fastsatt i forordning (EU) 2022/2554, og særlig omfatter de risikoene som avdekkes i rapporter om alvorlige IKT-relaterte hendelser, og i resultatene av den testingen av digital operasjonell motstandsdyktighet som finansielle enheter utfører i samsvar med den nevnte forordningen.

5) Digital operasjonell motstandsdyktighet er nødvendig for å opprettholde en finansiell enhets kritiske funksjoner og hovedforretningsområder i tilfelle krisehåndtering, og for å unngå forstyrrelser i realøkonomien og i finanssystemet. Alvorlige operasjonelle hendelser kan hemme en finansiell enhets evne til å drive sin virksomhet og kan true krisehåndteringsmålene. Visse kontraktsregulerte ordninger om bruken av IKT-tjenester er viktige for å sikre operasjonell kontinuitet og for å levere de nødvendige opplysningene i tilfelle krisehåndtering. Med henblikk på tilpasning til målene i Unionens rammeverk for operasjonell motstandsdyktighet bør direktiv 2014/59/EU derfor endres for å sikre at det tas hensyn til opplysninger om operasjonell motstandsdyktighet i forbindelse med planlegging av krisehåndtering og vurdering av finansielle enheters muligheter til krisehåndtering.

6) I direktiv 2014/65/EU er det fastsatt strengere regler med hensyn til IKT-risiko for verdipapirforetak og handelsplasser som er involvert i algoritmehandel. Det gjelder mindre detaljerte krav for datarapporteringstjenester og transaksjonsregistre. I direktiv 2014/65/EU vises det bare i begrenset omfang til kontroll- og sikkerhetsordninger for databehandlingssystemer og bruken av hensiktsmessige systemer, ressurser og framgangsmåter for å sikre kontinuitet og regelmessighet i forbindelse med forretningstjenester. Dessuten

[12] Europaparlaments- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 av 27.12.2022, s. 1).

[13] Europaparlaments- og rådsforordning (EU) nr. 1093/2010 av 24. november 2010 om opprettelse av en europeisk tilsynsmyndighet (Den europeiske banktilsynsmyndighet), om endring av beslutning nr. 716/2009/EF og om oppheving av kommisjonsbeslutning 2009/78/EF (EUT L 331 av 15.12.2010, s. 12).

bør det nevnte direktivet harmoniseres med forordning (EU) 2022/2554 når det gjelder kontinuitet og regelmessighet i forbindelse med leveringen av investeringstjenester og utøvelsen av investeringsvirksomhet, operasjonell motstandsdyktighet, handelssystemenes kapasitet og effektivitet i forbindelse med ordninger for å sikre kontinuitet i virksomheten og risikostyring.

7) I direktiv (EU) 2015/2366 fastsettes særlige regler om IKT-relaterte sikkerhetskontroll- og begrensningsaspekter for å få tillatelse til å tilby betalingstjenester. Disse reglene om tillatelse bør endres for å bringe dem i samsvar med forordning (EU) 2022/2554. For å redusere den administrative byrden og unngå kompleksitet og overlappende rapporteringskrav bør dessuten reglene om rapportering av hendelser i det nevnte direktivet opphøre å gjelde for betalingstjenesteytere som er regulert i henhold til det nevnte direktivet, og som også er omfattet av forordning (EU) 2022/2554, slik at disse betalingstjenesteyterne kan dra nytte av en felles og fullt ut harmonisert ordning for rapportering av hendelser med hensyn til alle betalingsrelaterte operasjonelle hendelser eller sikkerhetshendelser, uavhengig av om slike hendelser er IKT-relaterte.
8) Direktiv 2009/138/EF og (EU) 2016/2341 fanger delvis opp IKT-risiko i sine generelle bestemmelser om foretaksstyring og risikostyring, hvilket innebærer at visse krav skal spesifiseres gjennom delegerte rettsakter med eller uten særskilte henvisninger til IKT-risiko. På samme måte får bare svært generelle regler anvendelse på forvaltere av alternative investeringsfond som er omfattet av direktiv 2011/61/EU, og forvaltningsselskaper som er omfattet av direktiv 2009/65/EF. Disse direktivene bør derfor tilpasses til kravene fastsatt i forordning (EU) 2022/2554 med hensyn til forvaltningen av IKT-systemer og -verktøyer.
9) I mange tilfeller er det allerede fastsatt krav til IKT-risiko i delegerte rettsakter og gjennomføringsrettsakter som er vedtatt på grunnlag av utkast til tekniske reguleringsstandarder og tekniske gjennomføringsstandarder, som er utarbeidet av den vedkommende europeiske tilsynsmyndigheten. Ettersom bestemmelsene i forordning (EU) 2022/2554 heretter utgjør det rettslige rammeverket for IKT-risiko i finanssektoren, bør visse fullmakter til å vedta delegerte rettsakter og gjennomføringsrettsakter i direktiv 2009/65/EF, 2009/138/EF, 2011/61/EU og 2014/65/EU endres for å fjerne bestemmelsene om IKT-risiko fra anvendelsesområdet for disse fullmaktene.
10) For å sikre en enhetlig gjennomføring av det nye rammeverket om digital operasjonell motstandsdyktighet i finanssektoren bør medlemsstatene anvende de internrettslig bestemmelsene som innarbeider dette direktivet fra og med anvendelsesdatoen for forordning (EU) 2022/2554.
11) Direktiv 2009/65/EF, 2009/138/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 og (EU) 2016/2341 er vedtatt på grunnlag av artikkel 53 nr. 1 eller artikkel 114 i traktaten om Den europeiske unions virkemåte (TEUV) eller begge. Endringene i dette direktivet er blitt innarbeidet i én enkelt regelverksakt ettersom gjenstanden for og målene med endringene er innbyrdes forbundet. Dette direktivet bør derfor vedtas på grunnlag av både artikkel 53 nr. 1 og artikkel 114 i TEUV.
12) Ettersom målene for dette direktivet ikke kan nås i tilstrekkelig grad av medlemsstatene, ettersom de innebærer harmonisering av krav som allerede finnes i direktivene, og derfor på grunn av tiltakets omfang og virkninger bedre kan nås på unionsplan, kan Unionen treffe tiltak i samsvar med nærhetsprinsippet som fastsatt i artikkel 5 i traktaten om Den europeiske union. I samsvar med forholdsmessighetsprinsippet fastsatt i den nevnte artikkelen går dette direktivet ikke lenger enn det som er nødvendig for å nå disse målene.
13) I samsvar med den felles politiske erklæringen fra medlemsstatene og Kommisjonen av 28. september 2011 om forklarende dokumenter[14] har medlemsstatene forpliktet seg til at de, i berettigede tilfeller, sammen med underretningen om innarbeidingstiltakene skal oversende et eller flere dokumenter som forklarer sammenhengen mellom et direktivs bestanddeler og de tilsvarende delene i de nasjonale innarbeidingsinstrumentene. Med hensyn til dette direktivet anser regelgiveren at det er berettiget å oversende slike dokumenter.

VEDTATT DETTE DIREKTIVET:

Artikkel 1

Endringer av direktiv 2009/65/EF

I artikkel 12 i direktiv 2009/65/EF gjøres følgende endringer:

[14] EUT C 369 av 17.12.2011, s. 14.

1) I nr. 1 andre ledd skal bokstav a) lyde:
«a) har gode forvaltningsmessige og regnskapsmessige rutiner, kontroll- og sikkerhetsordninger for elektronisk databehandling, herunder med hensyn til nettverks- og informasjonssystemer som opprettes og forvaltes i samsvar med europaparlaments- rådsforordning (EU) 2022/2554(*), samt tilfredsstillende ordninger for internkontroll, herunder særlig regler for de ansattes personlige transaksjoner eller for besittelse eller forvaltning av investeringer i finansielle instrumenter med henblikk på investering av egne midler, som minst sikrer at enhver transaksjon der innretningen for kollektiv investering i omsettelige verdipapirer (UCITS) er involvert, kan rekonstrueres med hensyn til opprinnelse, parter, art samt tid og sted for gjennomføringen, og at UCITS' eiendeler som forvaltes av forvaltningsselskapet, investeres i samsvar med fondsreglene eller stiftelsesdokumentene samt gjeldende lovbestemmelser,

(*) Europaparlaments- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 av 27.12.2022, s.1).»

2) Nr. 3 skal lyde:
«3. Uten at det berører artikkel 116, skal Kommisjonen ved hjelp av delegerte rettsakter i samsvar med artikkel 112a, vedta tiltak som spesifiserer
a) de framgangsmåtene og ordningene som er nevnt i nr. 1 andre ledd bokstav a), bortsett fra de framgangsmåtene og ordningene som gjelder nettverks- og informasjonssystemer,
b) de strukturene og organisatoriske krav som er nevnt i nr. 1 andre ledd bokstav b), med sikte på å redusere interessekonfliktene til et minimum.».

Artikkel 2

Endringer av direktiv 2009/138/EF

I direktiv 2009/138/EF gjøres følgende endringer:

1) I artikkel 41 skal nr. 4 lyde:
«4. Forsikrings- og gjenforsikringsforetak skal iverksette rimelige tiltak for å sikre kontinuitet og regelmessighet i utøvelsen av virksomheten, herunder utarbeiding av beredskapsplaner. For dette formålet skal foretakene anvende egnede og forholdsmessige systemer, ressurser og framgangsmåter, og skal særlig opprette og forvalte nett- og informasjonssystemer i samsvar med europaparlaments- og rådsforordning (EU) 2022/2554(*).

(*) Europaparlaments- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 av 27.12.2022, s.1).»

2) I artikkel 50 nr. 1 skal bokstav a) og b) lyde:
«a) elementene i systemene nevnt i artikkel 41, artikkel 44, særlig de områdene som er nevnt i artikkel 44 nr. 2, og artikkel 46 og 47, bortsett fra de elementene som gjelder risikostyring i forbindelse med informasjons- og kommunikasjonsteknologi,
b) funksjonene nevnt i artikkel 44 og 46-48, bortsett fra de funksjonene som gjelder risikostyring i forbindelse med informasjons- og kommunikasjonsteknologi.»

Artikkel 3

Endring av direktiv 2011/61/EU

I direktiv 2011/61/EU skal artikkel 18 lyde:

«*Artikkel 18*
Allmenne prinsipper

1. Medlemsstatene skal kreve at AIF-forvaltere til enhver tid bruker tilstrekkelige og hensiktsmessige menneskelige og tekniske ressurser for å sikre korrekt forvaltning av AIF-ene.

Samtidig som det tas hensyn til arten av AIF-er som AIF-forvalteren forvalter, skal vedkommende myndigheter i AIF-forvalterens hjemstat særlig kreve at AIF-forvalteren har god forvaltnings- og regnskapspraksis, kontroll- og sikkerhetsordninger for elektronisk databehandling, herunder når det gjelder nettverks- og informasjonssystemer som opprettes og forvaltes i samsvar med europaparlaments- og rådsforordning (EU) 2022/2554(*), samt tilfredsstillende ordninger for internkontroll, herunder særlig regler for de ansattes personlige transaksjoner eller for besittelse eller forvaltning av investeringer med henblikk på investering for egen regning, som minst sikrer at enhver transaksjon der

AIF-er er involvert, kan rekonstrueres med hensyn til opprinnelse, parter, art samt tid og sted for gjennomføringen, og at eiendeler i AIF-ene som forvaltes av AIF-forvalteren, investeres i samsvar med AIF-ets regler eller stiftelsesdokumenter samt gjeldende lovbestemmelser.

2. Kommisjonen skal gjennom delegerte rettsakter i samsvar med artikkel 56 og på vilkårene fastsatt i artikkel 57 og 58, vedta tiltak som angir de framgangsmåtene og ordningene som er nevnt i nr. 1 i denne artikkelen, bortsett fra de framgangsmåtene og ordningene som gjelder nettverks- og informasjonssystemer.

(*) Europaparlaments- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 av 27.12.2022, s. 1.»

Artikkel 4

Endringer av direktiv 2013/36/EU

I direktiv 2013/36/EU gjøres følgende endringer:

1) I artikkel 65 nr. 3 skal bokstav a) vi) lyde:
«vi) tredjeparter som de enhetene som er nevnt i nr. i)–iv), har utkontraktert funksjoner eller aktiviteter til, herunder tredjepartsleverandører av IKT-tjenester som nevnt i kapittel V i europaparlaments- og rådsforordning (EU) 2022/2554(*),

(*) Europaparlaments- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 av 27.12.2022, s. 1.»

2) I artikkel 74 nr. 1 skal første ledd lyde:
«Institusjoner skal ha solide styringsordninger, herunder en klar organisasjonsstruktur med klart definerte, gjennomsiktige og konsekvente ansvarslinjer, effektive framgangsmåter for å identifisere, styre, overvåke og rapportere de risikoene som institusjonene er eller kan bli eksponert for, forsvarlige ordninger for internkontroll, herunder forsvarlig forvaltnings- og regnskapspraksis, nettverks- og informasjonssystemer som opprettes og forvaltes i samsvar med forordning (EU) 2022/2554, og godtgjøringspolitikk og -praksis som er forenlig med og fremmer en forsvarlig og effektiv risikostyring.»

3) I artikkel 85 skal nr. 2 lyde:
«2. Vedkommende myndigheter skal sikre at institusjonene har tilstrekkelige retningslinjer og planer for beredskap og kontinuitet i virksomheten, herunder retningslinjer og planer for IKT-kontinuitet i virksomheten og planer for IKT-respons og -gjenoppretting i forbindelse med den teknologien de bruker til formidling av opplysninger, og at disse planene utarbeides, forvaltes og testes i samsvar med artikkel 11 i forordning (EU) 2022/2554, slik at institusjonene kan fortsette å drive sin virksomhet i tilfelle alvorlige driftsforstyrrelser og begrense tap som oppstår som følge av slike forstyrrelser.»

4) I artikkel 97 nr. 1 skal ny bokstav lyde:
«d) de risikoene som påvises ved testing av digital operasjonell motstandsdyktighet i samsvar med kapittel IV i forordning (EU) 2022/2554.»

Artikkel 5

Endringer av direktiv 2014/59/EU

I direktiv 2014/59/EU gjøres følgende endringer:

1) I artikkel 10 gjøres følgende endringer:
a) I nr. 7 skal bokstav c) lyde:
«c) En beskrivelse av hvordan kritiske funksjoner og hovedforretningsområder i nødvendig omfang kan atskilles juridisk og økonomisk fra andre funksjoner for å sikre kontinuitet og digital operasjonell motstandsdyktighet dersom institusjonen blir kriserammet.»
b) I nr. 7 skal bokstav q) lyde:
«q) En beskrivelse av de aktivitetene og systemene som er avgjørende for å opprettholde løpende drift av institusjonens operasjonelle prosesser, herunder nettverks- og informasjonssystemer som nevnt i europaparlaments- og rådsforordning (EU) 2022/2554(*).

(*) Europaparlaments- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 av 27.12.2022, s. 1.»

c) I nr. 9 skal nytt ledd lyde:
«EBA skal i samsvar med artikkel 10 i forordning (EU) nr. 1093/2010 gjennomgå og eventuelt oppdatere de tekniske reguleringsstandardene for blant annet å ta hen-

syn til bestemmelsene i kapittel II i forordning (EU) 2022/2554.»

2) I vedlegget gjøres følgende endringer:
   a) I avsnitt A skal punkt 16) lyde:
   «16) ordninger og tiltak som er nødvendige for å opprettholde løpende drift av institusjonens operasjonelle prosesser, herunder nettverks- og informasjonssystemer som opprettes og forvaltes i samsvar med forordning (EU) 2022/2554.»
   b) I avsnitt B gjøres følgende endringer:
      i) Punkt 14) skal lyde:
      «14) Identifisering av eierne av systemene angitt i punkt 13), tilknyttede tjenestenivåavtaler samt programvare og systemer eller lisenser, herunder per rettssubjekt, kritiske funksjoner og hovedforretningsområder, samt identifisering av kritiske tredjepartsleverandører av IKT-tjenester som definert i artikkel 3 nr. 23 i forordning (EU) 2022/2554.»
      ii) Nytt punkt skal lyde:
      «14a) Resultatene av institusjoners testing av digital operasjonell motstandsdyktighet i henhold til forordning (EU) 2022/2554.»
   c) I avsnitt C gjøres følgende endringer:
      i) Punkt 4) skal lyde:
      «4) i hvilket omfang de tjenesteavtalene som institusjonen har inngått, herunder de kontraktsregulerte ordningene om bruken av IKT-tjenester, er solide og kan håndheves dersom institusjonen krisehåndteres,»
      ii) Nytt punkt skal lyde:
      «4a) den digitale operasjonelle motstandsdyktigheten til nettverks- og informasjonssystemene som støtter institusjonens kritiske funksjoner og hovedforretningsområder, samtidig som det tas hensyn til rapporter om alvorlige IKT-relaterte hendelser og resultatene av testing av digital operasjonell motstandsdyktighet i henhold til forordning (EU) 2022/2554.»

Artikkel 6

Endringer av direktiv 2014/65/EU

I direktiv 2014/65/EU gjøres følgende endringer:

1) I artikkel 16 gjøres følgende endringer:
   a) Nr. 4 skal lyde:
   «4. Et verdipapirforetak skal treffe rimelige tiltak for å sikre kontinuitet og regelmessighet i ytingen av investeringstjenester og utøvelsen av investeringsvirksomhet. For dette formålet skal verdipapirforetaket anvende egnede og riktig avpassede systemer, herunder systemer for informasjons- og kommunikasjonsteknologi (IKT) som opprettes og forvaltes i samsvar med artikkel 7 i europaparlaments- og rådsforordning (EU) 2022/2554(*), samt egnede og riktig avpassede ressurser og framgangsmåter.

   (*) Europaparlaments- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 av 27.12.2022, s. 1.»

   b) I nr. 5 skal andre og tredje ledd lyde:
   Et verdipapirforetak skal ha god forvaltnings- og regnskapspraksis, ordninger for internkontroll og effektive framgangsmåter for risikovurdering.
   Uten at det berører vedkommende myndigheters mulighet til å kreve tilgang til kommunikasjon i samsvar med dette direktivet og forordning (EU) nr. 600/2014, skal et verdipapirforetak ha innført pålitelige sikkerhetssystemer for å garantere, i henhold til kravene i forordning (EU) 2022/2554, sikkerhet og autentisering ved informasjonsoverføringen, redusere risikoen for dataforfalskning og ulovlig tilgang og forebygge informasjonslekkasje, slik at opplysningene til enhver tid behandles på en fortrolig måte.»

2) I artikkel 17 gjøres følgende endringer:
   a) Nr. 1 skal lyde:
   «1. Et verdipapirforetak som anvender algoritmehandel, skal ha innført effektive systemer og risikokontroller som er egnede for den virksomheten det utøver, for å sikre at dets handelssystemer er motstandsdyktige og har tilstrekkelig kapasitet i samsvar med kravene fastsatt i kapittel II til forordning (EU) 2022/2554, er omfattet av egnede handelsterskler og -grenser og hindrer at det sendes feilaktige ordrer, eller at systemene på annen måte fungerer på en måte som skaper eller bidrar til uro på markedet.

Et slikt foretak skal også ha innført effektive systemer og risikokontroller for å sikre at handelssystemene ikke kan brukes til formål som er i strid med forordning (EU) nr. 596/2014 eller med reglene til en handelsplass som det er knyttet til.

Verdipapirforetaket skal ha innført effektive ordninger for kontinuitet i virksomheten for å håndtere en eventuell svikt i sine handelssystemer, herunder retningslinjer og planer for IKT-kontinuitet i virksomheten og planer for IKT-respons og -gjenoppretting som er utarbeidet i samsvar med artikkel 11 i forordning (EU) 2022/2554, og skal sikre at systemene testes fullt ut og blir behørig overvåket for å sikre at de oppfyller de generelle kravene i dette nummeret og eventuelle særlige krav i kapittel II og IV til forordning (EU) 2022/2554.»

b) I nr. 7 skal bokstav a) lyde:

«a) Nærmere opplysninger om organisatoriske krav fastsatt i nr. 1–6, bortsett fra de organisatoriske kravene som gjelder styring av IKT-risiko, som skal pålegges verdipapirforetak som yter ulike typer investeringstjenester, utøver ulike typer investeringsvirksomhet, yter tilleggstjenester eller kombinasjoner av slike, der spesifikasjonene for de organisatoriske kravene i nr. 5 skal fastsette de særlige kravene til direkte markedsadgang og sponset tilgang på en måte som sikrer at kontrollene som foretas av sponset tilgang, minst tilsvarer dem som foretas i forbindelse med direkte markedsadgang.»

3) I artikkel 47 nr. 1 gjøres følgende endringer:

a) Bokstav b) skal lyde:

«b) er tilstrekkelig utstyrt til å styre risikoene fasiliteten utsettes for, herunder til å styre IKT-risiko i samsvar med kapittel II til forordning (EU) 2022/2554, innfører egnede ordninger og systemer for å identifisere vesentlige risikoer for driften, og har innført effektive tiltak for å redusere slike risikoer,»

b) Bokstav c) utgår.

4) I artikkel 48 gjøres følgende endringer:

a) Nr. 1 skal lyde:

«1. Medlemsstatene skal kreve at et regulert marked innfører og opprettholder sin operasjonelle motstandsdyktighet i samsvar med kravene fastsatt i kapittel II i forordning (EU) 2022/2554, for å sikre at dets handelssystemer er motstandsdyktige, har tilstrekkelig kapasitet til å kunne håndtere toppbelastning med hensyn til ordre- og meldingsvolum, kan sikre ordnet handel ved alvorlig markedsstress, er testet fullt ut for å sikre at slike vilkår er oppfylt, og er omfattet av effektive ordninger for kontinuitet i virksomheten, herunder planer og retningslinjer for IKT-kontinuitet i virksomheten og planer for IKT-respons og -gjenoppretting som er utarbeidet i samsvar med artikkel 11 i forordning (EU) 2022/2554, for å sikre kontinuitet i sin virksomhet ved en eventuell svikt i sine handelssystemer.»

b) Nr. 6 skal lyde:

«6. Medlemsstatene skal kreve at et regulert marked har innført effektive systemer, framgangsmåter og ordninger, herunder krav om at medlemmer eller deltakere skal foreta egnet testing av algoritmer og skape miljøer som letter slik testing, i samsvar med kravene fastsatt i kapittel II og IV i forordning (EU) 2022/2554, for å sikre at algoritmebaserte handelssystemer ikke kan skape eller bidra til uordnede handelsvilkår på markedet, og for å håndtere eventuelle uordnede handelsvilkår som kan oppstå som følge av slike algoritmebaserte handelssystemer, herunder systemer som begrenser andelen av ikke-utførte ordrer i forhold til transaksjonene som kan gjennomføres i systemet av et medlem eller en deltaker, slik at det blir mulig å bremse ordrestrømmen dersom det er en risiko for at grensen for systemkapasiteten nås, og slik at den minste tillatte kursendringen som kan anvendes på markedet, begrenses og håndheves.»

c) I nr. 12 gjøres følgende endringer:

i) Bokstav a) skal lyde:

«a) kravene til å sikre at regulerte markeders handelssystemer er motstandsdyktige og har tilstrekkelig kapasitet, med unntak av de kravene som er knyttet til digital operasjonell motstandsdyktighet,»

ii) Bokstav g) skal lyde:

«g) kravene om å sikre tilstrekkelig testing av algoritmer, bortsett fra

testing av digital operasjonell motstandsdyktighet, for å sikre at algoritmebaserte handelssystemer, herunder systemer for høyfrekvent algoritmehandel, ikke kan skape eller bidra til uordnede handelsvilkår på markedet.»

Artikkel 7

Endringer av direktiv (EU) 2015/2366

I direktiv (EU) 2015/2366 gjøres følgende endringer:

1) I artikkel 3 skal bokstav j) lyde:
«j) tjenester som leveres av leverandører av tekniske tjenester til støtte for betalingstjenesteytingen, uten at disse på noe tidspunkt kommer i besittelse av de midlene som skal overføres, herunder behandling og lagring av data, tillitsskapende tjenester og integritetsvern, autentisering av data og enheter, levering av informasjons- og kommunikasjonsteknologi (IKT) og levering av kommunikasjonsnett, levering og vedlikehold av terminaler og innretninger som benyttes til betalingstjenester, med unntak av betalingsinitieringstjenester og kontoopplysningstjenester,»
2) I artikkel 5 nr. 1 gjøres følgende endringer:
a) I første ledd gjøres følgende endringer:
i) Bokstav e) skal lyde:
«e) en beskrivelse av søkerens ordninger for foretaksstyring og internkontroll, herunder framgangsmåter for forvaltning, risikostyring og regnskapsføring samt ordninger for bruk av IKT-tjenester i samsvar med europaparlaments- og rådsforordning (EU) 2022/2554(*), som viser at disse ordningene for foretaksstyring og internkontroll er forholdsmessige, hensiktsmessige, forsvarlige og tilstrekkelige.

(*) Europaparlaments- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 av 27.12.2022, s. 1.»

ii) Bokstav f) skal lyde:
«f) en beskrivelse av framgangsmåten som er innført for å overvåke, håndtere og følge opp sikkerhetshendelser og sikkerhetsrelaterte kundeklager, herunder en ordning for rapportering av hendelser som tar hensyn til betalingsinstitusjonens meldingsplikt i henhold til kapittel III i forordning (EU) 2022/2554,»,
iii) Bokstav h) skal lyde:
«h) en beskrivelse av ordningene for å sikre kontinuitet i virksomheten, herunder en tydelig angivelse av kritiske funksjoner, effektive retningslinjer og planer for IKT-kontinuitet i virksomheten og planer for IKT-respons og -gjenoppretting samt en prosedyre for regelmessig å teste og kontrollere slike planers egnethet og effektivitet i samsvar med forordning (EU) 2022/2554,»,
b) Tredje ledd skal lyde:
«I forbindelse med de sikkerhetskontrolltiltakene og risikoreduserende tiltakene som er nevnt i første ledd bokstav j), skal det angis hvordan de sikrer et høyt nivå av digital operasjonell motstandsdyktighet i samsvar med kapittel II i forordning (EU) 2022/2554, særlig med hensyn til teknisk sikkerhet og datavern, også for den programvaren og de IKT-systemene som brukes av søkeren eller de foretakene søkeren har satt hele eller deler av sin virksomhet ut til. Disse tiltakene skal også omfatte de sikkerhetstiltakene som er fastsatt i artikkel 95 nr. 1 i dette direktivet. I forbindelse med disse tiltakene skal det tas hensyn til de europeiske tilsynsmyndighetenes retningslinjer om sikkerhetstiltak som nevnt i artikkel 95 nr. 3 i dette direktivet, når disse foreligger.»
3) I artikkel 19 nr. 6 skal andre ledd lyde:
«Utkontraktering av viktige driftsfunksjoner, herunder IKT-systemer, kan ikke skje på en slik måte at det vesentlig forringer kvaliteten på betalingsinstitusjonens internkontroll og vedkommende myndigheters mulighet til å overvåke og spore om betalingsinstitusjonen oppfyller alle sine forpliktelser i henhold til dette direktivet.»
4) I artikkel 95 nr. 1 skal nytt ledd lyde:
«Første ledd berører ikke anvendelsen av kapittel II i forordning (EU) 2022/2554 på
a) betalingstjenesteytere nevnt i artikkel 1 nr. 1 bokstav a), b) og d) i dette direktivet,
b) ytere av kontoopplysningstjenester nevnt i artikkel 33 nr. 1 i dette direktivet,

c) betalingsinstitusjoner som er unntatt i henhold til artikkel 32 nr. 1 i dette direktivet, og
d) e-pengeforetak som er omfattet av et unntak i henhold til artikkel 9 nr. 1 i direktiv 2009/110/EF.»

5) I artikkel 96 skal nytt nummer lyde:
«7. Medlemsstatene skal sikre at nr. 1–5 i denne artikkelen ikke får anvendelse på
a) betalingstjenesteytere nevnt i artikkel 1 nr. 1 bokstav a), b) og d) i dette direktivet,
b) ytere av kontoopplysningstjenester nevnt i artikkel 33 nr. 1 i dette direktivet,
c) betalingsinstitusjoner som er unntatt i henhold til artikkel 32 nr. 1 i dette direktivet, og
d) e-pengeforetak som er omfattet av et unntak i henhold til artikkel 9 nr. 1 i direktiv 2009/110/EF.»

6) I artikkel 98 skal nr. 5 lyde:
«5. I samsvar med artikkel 10 i forordning (EU) nr. 1093/2010 skal EBA regelmessig gjennomgå og eventuelt oppdatere de tekniske reguleringsstandardene for blant annet å ta hensyn til innovasjon og teknologisk utvikling samt til bestemmelsene i kapittel II i forordning (EU) 2022/2554.»

Artikkel 8

Endring av direktiv (EU) 2016/2341

Artikkel 21 nr. 5 i direktiv (EU) 2016/2341 skal lyde:

«5. Medlemsstatene skal sikre at tjenestepensjonsforetaket treffer rimelige tiltak for å sikre kontinuitet og regelmessighet i utøvelsen av virksomheten, herunder utarbeiding av beredskapsplaner. For dette formålet skal tjenestepensjonsforetakene anvende egnede og forholdsmessige systemer, ressurser og framgangsmåter, og skal særlig opprette og forvalte nettverks- og informasjonssystemer i samsvar med europaparlaments- og rådsforordning (EU) 2022/2554(*), dersom det er relevant.

(*) Europaparlaments,- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 av 27.12.2022, s.1).»

Artikkel 9

Innarbeiding i nasjonal rett

1. Medlemsstatene skal senest 17. januar 2025 vedta og kunngjøre de bestemmelsene som er nødvendige for å etterkomme dette direktivet. De skal umiddelbart underrette Kommisjonen om dette.

De skal anvende disse bestemmelsene fra 17. januar 2025.

Når disse bestemmelsene vedtas av medlemsstatene, skal de inneholde en henvisning til dette direktivet, eller det skal vises til direktivet når de kunngjøres. Nærmere regler for henvisningen fastsettes av medlemsstatene.

2. Medlemsstatene skal oversende Kommisjonen teksten til de viktigste internrettslige bestemmelsene som de vedtar på det området dette direktivet omhandler.

Artikkel 10

Ikrafttredelse

Dette direktivet trer i kraft den 20. dagen etter at det er kunngjort i *Den europeiske unions tidende*.

Artikkel 11

Adressater

Dette direktivet er rettet til medlemsstatene.

Utferdiget i Strasbourg 14. desember 2022.

For Europaparlamentet	*For Rådet*
R. Metsola	M. Bek
President	*Formann*

Vedlegg 3

Europaparlaments- og rådsforordning (EU) 2023/1113 av 31. mai 2023 om opplysninger som skal følge overføringer av penger og visse kryptoeiendeler, og om endring av direktiv (EU) 2015/849 (omarbeiding)

EUROPAPARLAMENTET OG RÅDET FOR DEN EUROPEISKE UNION HAR

under henvisning til traktaten om Den europeiske unions virkemåte, særlig artikkel 114,

under henvisning til forslag fra Europakommisjonen,

etter oversending av utkast til regelverksakt til de nasjonale parlamentene,

under henvisning til uttalelse fra Den europeiske sentralbank[1],

under henvisning til uttalelse fra Den europeiske økonomiske og sosiale komité[2],

etter den ordinære regelverksprosedyren[3] og

ut fra følgende betraktninger:

1) Europaparlaments- og rådsforordning (EU) 2015/847[4] har blitt betydelig endret[5]. Ettersom det skal gjøres ytterligere endringer, bør forordningen av klarhetshensyn omarbeides.
2) Forordning (EU) 2015/847 ble vedtatt for å sikre ensartet anvendelse i hele Unionen av kravene som innsatsgruppen for finansielle tiltak (Financial Action Task Force – FATF) stiller til ytere av tjenester knyttet til elektronisk overføring, og særlig betalingstjenesteyteres plikt til å oversende opplysninger om betaleren og betalingsmottakeren sammen med pengeoverføringene. De seneste endringene som ble innført i juni 2019 i FATF-standardene for nye teknologier, og som har som formål å regulere virtuelle eiendeler og ytere av tjenester knyttet til virtuelle eiendeler, har medført nye og lignende forpliktelser for ytere av tjenester knyttet til virtuelle eiendeler med sikte på å gjøre det lettere å spore overføringer av virtuelle eiendeler. Som følge av disse endringene skal ytere av tjenester knyttet til virtuelle eiendeler oversende opplysninger om avsenderne og mottakerne sammen med disse overføringene. Det kreves også at ytere av tjenester knyttet til virtuelle eiendeler skal innhente, oppbevare og dele disse opplysningene med sin motpart i den andre enden av overføringen av virtuelle eiendeler, og på anmodning stille dem til rådighet for vedkommende myndigheter.
3) Ettersom forordning (EU) 2015/847 for øyeblikket bare får anvendelse på pengeoverføringer, det vil si sedler og mynter, kontopenger og elektroniske penger som definert i artikkel 2 nr. 2 i europaparlaments- og rådsdirektiv 2009/110/EF[6], bør anvendelsesområdet for forordning (EU) 2015/847 utvides slik at det også omfatter overføringer av virtuelle eiendeler.
4) Strømmer av penger fra ulovlig virksomhet som skapes gjennom overføringer av penger og virtuelle eiendeler, kan skade finanssektorens integritet, stabilitet og omdømme og utgjøre en trussel mot Unionens indre marked og den internasjonale utviklingen. Hvitvasking av penger, finansiering av terrorisme og organisert kriminalitet er fortsatt et alvorlig problem som bør håndteres på unionsplan. Soliditeten, integriteten og stabiliteten til systemet for overføringer av penger og virtuelle eiendeler, og tilliten til finanssystemet som helhet kan skades alvorlig av at kriminelle og deres medvirkende forsøker å skjule opprinnelsen til utbytte av kriminell virksomhet eller å over-

---

1 EUT C 68 av 9.2. 2022, s. 2.

2 EUT C 152 av 6.4. 2022, s. 89.

3 Europaparlamentets holdning av 20. april 2023 (ennå ikke offentliggjort i EUT) og rådsbeslutning av 16. mai 2023.

4 Europaparlaments- og rådsforordning (EU) 2015/847 av 20. mai 2015 om opplysninger som skal følge pengeoverføringer, og om oppheving av forordning (EF) nr. 1781/2006 (EUT L 141 av 5.6.2015, s. 1).

5 Se vedlegg I.

6 Europaparlaments- og rådsdirektiv 2009/110/EU av 16. september 2009 om adgang til å starte og utøve virksomhet som e-pengeforetak og om tilsyn med slik virksomhet, om endring av direktiv 2005/60/EF og 2006/48/EF og om oppheving av direktiv 2000/46/EF (EUT L 267 av 10.10.2009, s. 7).

føre penger eller virtuelle eiendeler til kriminell virksomhet eller terrorformål.

5) Med mindre det treffes visse samordningstiltak på unionsplan, vil personer som driver med hvitvasking av penger og finansiering av terrorisme, sannsynligvis prøve å utnytte den frie bevegelsen av kapital innenfor Unionens integrerte finansielle område for å fremme sin kriminelle virksomhet. Det internasjonale samarbeidet innenfor rammen av Den internasjonale innsatsgruppen for finansielle tiltak til bekjempelse av hvitvasking av penger (Financial Action Task Force, FATF) og den globale gjennomføringen av dens anbefalinger har som mål å forebygge hvitvasking av penger og finansiering av terrorisme ved overføring av penger eller virtuelle eiendeler.
6) På grunn av omfanget av de tiltakene som skal gjennomføres, bør Unionen sikre at de internasjonale standardene for bekjempelse av hvitvasking av penger og finansiering av terrorisme og spredning som FATF vedtok 16. februar 2012 og deretter reviderte 21. juni 2019 (heretter kalt «reviderte FATF-anbefalinger»), og særlig FATF-anbefaling nr. 15 om nye teknologier, FATF-anbefaling nr. 16 om elektroniske overføringer og de reviderte fortolkningsnotene til disse anbefalingene, anvendes på en ensartet måte i hele Unionen, og spesielt at det ikke forekommer noen forskjellsbehandling eller annerledes behandling av innenlandske betalinger eller overføringer av virtuelle eiendeler i en medlemsstat på den ene siden og betalinger eller overføringer av virtuelle eiendeler på tvers av landegrensene mellom medlemsstater på den andre siden. Dersom enkeltmedlemsstater treffer tiltak med hensyn til overføringer av penger og virtuelle eiendeler over landegrensene som ikke er samordnet, kan det gripe vesentlig inn i virkemåten til betalingssystemene og tjenester knyttet til virtuelle eiendeler på unionsplan og dermed skade det indre marked for finansielle tjenester.
7) For å fremme en enhetlig tilnærming internasjonalt og gjøre kampen mot hvitvasking av penger og finansiering av terrorisme mer effektiv bør Unionens videre tiltak ta hensyn til utviklingen på internasjonalt plan, særlig de reviderte FATF-anbefalingene.
8) Deres globale rekkevidde, den hastigheten som transaksjoner kan gjennomføres i, og den mulige anonymiteten som overføringen av dem gir, gjør at virtuelle eiendeler er særlig utsatt for kriminelt misbruk, også i grensekryssende situasjoner. For effektivt å håndtere de risikoene som er knyttet til misbruk av virtuelle eiendeler til hvitvasking av penger og finansiering av terrorisme, bør Unionen fremme anvendelse på globalt plan av de standardene som gjennomføres ved denne forordningen, og utvikling av den internasjonale og jurisdiksjonsoverskridende dimensjonen av regulerings- og tilsynsrammen for overføringer av virtuelle eiendeler i forbindelse med hvitvasking av penger og finansiering av terrorisme.
9) Europaparlaments- og rådsdirektiv (EU) 2015/849[7], som endret ved europaparlaments- og rådsdirektiv (EU) 2018/843[8], innførte en definisjon av virtuelle valutaer, og tilbydere av vekslingstjenester mellom virtuelle valutaer og offisielle valutaer såvel som tilbydere av oppbevaringstjenester for virtuelle valutaer ble anerkjent som enheter som er omfattet av krav om bekjempelse av hvitvasking av penger og finansiering av terrorisme i henhold til unionsretten. Den seneste internasjonale utviklingen, særlig innenfor rammen av FATF, innebærer nå et behov for å regulere ytterligere kategorier av ytere av tjenester knyttet til virtuelle eiendeler, som ennå ikke er omfattet, og å utvide den gjeldende definisjonen av virtuell valuta.
10) Definisjonen av kryptoeiendeler i europaparlaments- og rådsforordning (EU) 2023/1114[9] svarer til definisjonen av virtuelle eiendeler som fastsatt i de reviderte FATF-anbefalingene, og listen over kryptoeiendelstjenester og ytere av kryptoeiendelstjenester som er omfattet av nevnte forordning, omfatter også de yterne av tjenester knyttet til virtuelle eiendeler, som er identifisert som slike av FATF, og som anses å kunne medføre problemer

---

7 Europaparlaments- og rådsdirektiv (EU) 2015/849 av 20. mai 2015 om tiltak for å hindre at finanssystemet brukes til hvitvasking av penger eller finansiering av terrorisme, om endring av europaparlaments- og rådsforordning (EU) nr. 648/2012 og om oppheving av europaparlaments- og rådsdirektiv 2005/60/EF og kommisjonsdirektiv 2006/70/EF (EUT L 141 av 5.6.2015, s. 73).

8 Europaparlaments- og rådsdirektiv (EU) 2018/843 av 30. mai 2018 om endring av direktiv (EU) 2015/849 om tiltak for å hindre at finanssystemet brukes til hvitvasking av penger eller finansiering av terrorisme, og om endring av direktiv 2009/138/EF og 2013/36/EU (EUT L 156 av 19.6.2018, s. 43).

9 Europaparlaments- og rådsforordning (EU) 2023/1114 av 31. mai 2023 om markeder for kryptoeiendeler og om endring av forordning (EU) nr. 1093/2010 og (EU) nr. 1095/2010 samt direktiv 2013/36/EU og (EU) 2019/1937 (EUT L 150 av 9.6.2023, s. 40).

med hvitvasking av penger og finansiering av terrorisme. For å sikre sammenheng i unionsretten på dette området bør denne forordningen anvende de samme definisjonene av kryptoeiendeler, kryptoeiendelstjenester og ytere av kryptoeiendelstjenester som dem som anvendes i forordning (EU) 2023/1114.

11) Å gjennomføre og håndheve denne forordningen er en relevant og effektiv metode for å forebygge og bekjempe hvitvasking av penger og finansiering av terrorisme.

12) Denne forordningen har ikke som mål å påføre ytere av betalingstjenester eller kryptoeiendelstjenester eller personer som benytter deres tjenester, unødvendige byrder eller kostnader. I så henseende bør den forebyggende strategien være målrettet, forholdsmessig og helt i samsvar med den frie kapitalbevegelsen som garanteres i hele Unionen.

13) I Unionens reviderte strategi mot finansiering av terrorisme av 17. juli 2008 (heretter kalt «den reviderte strategien») ble det påpekt at innsatsen for å forebygge finansiering av terrorisme og kontrollere hvordan antatte terrorister bruker sine økonomiske midler, må fortsette. Det fastslås der at FATF stadig søker å forbedre sine anbefalinger og arbeider for å skape en felles forståelse av hvordan de bør gjennomføres. Det er anført i den reviderte strategien at det jevnlig vil bli foretatt en vurdering av hvordan alle FATF-medlemmer og medlemmer av FATF-tilknyttede regionale organer gjennomfører de reviderte FATF-anbefalingene, og at det derfor er viktig at medlemsstatene har en felles tilnærming til gjennomføringen.

14) I sin melding av 7. mai 2020 om en handlingsplan for en samlet unionspolitikk for forebygging av hvitvasking av penger og finansiering av terrorisme identifiserte Kommisjonen dessuten seks prioriterte områder der det skal treffes hastetiltak for å forbedre Unionens ordning for bekjempelse av hvitvasking av penger og finansiering av terrorisme, blant annet innføring av et sammenhengende regelverk for denne ordningen i Unionen slik at reglene blir mer detaljerte og harmoniserte, særlig for å ta hensyn til konsekvensene av teknologisk innovasjon og utviklingen i nasjonale standarder og å unngå divergerende gjennomføring av eksisterende regler. Arbeid på internasjonalt plan tyder på at det er behov for å utvide omfanget av sektorer eller enheter som omfattes av denne ordningen, og for å vurdere hvordan den bør få anvendelse på ytere av kryptoeiendelstjenester som foreløpig ikke er omfattet.

15) For å forebygge finansiering av terrorisme er det truffet tiltak med sikte på å fryse visse personers, gruppers og foretaks midler og økonomiske ressurser, herunder rådsforordning (EF) nr. 2580/2001[10], (EF) nr. 881/2002[11] og (EU) nr. 356/2010[12]. For samme formål er det også truffet tiltak med sikte på å beskytte finanssystemet mot kanalisering av midler og økonomiske ressurser til terrorformål. Direktiv (EU) 2015/849 inneholder en rekke slike tiltak. Disse tiltakene er imidlertid ikke tilstrekkelige til å hindre at terrorister eller andre kriminelle får tilgang til betalingssystemer med sikte på pengeoverføringer.

16) For å kunne forebygge, avdekke og etterforske hvitvasking av penger og finansiering av terrorisme vil sporbarhet av overføringer av penger og kryptoeiendeler være et spesielt viktig og verdifullt verktøy, også i forbindelse med gjennomføringen av restriktive tiltak, særlig tiltakene som er innført ved forordning (EF) nr. 2580/2001, (EF) nr. 881/2002 og (EU) nr. 356/2010. For å sikre at opplysninger overføres gjennom hele betalingskjeden eller overføringskjeden for kryptoeiendeler, bør det derfor innføres et system som forutsetter at betalingstjenesteyterne oversender opplysninger om betaleren og betalingsmottakeren sammen med pengeoverføringer, og som forutsetter at yterne av kryptoeiendelstjenester oversender opplysninger om avsenderen og mottakeren sammen med overføringer av kryptoeiendeler.

17) Visse overføringer av kryptoeiendeler innebærer særlige høyrisikofaktorer for hvitvasking av penger, finansiering av terrorisme og annen kriminell virksomhet, særlig overføringer knyttet til produkter, transaksjoner eller teknologier som er utformet for å øke anonymiteten, herunder anonyme lommebøker og miksetjenester. For å sikre sporbarheten av slike overføringer bør Den europeiske tilsynsmyndighet (Den europeiske

---

[10] Rådsforordning (EF) nr. 2580/2001 av 27. desember 2001 om særskilde restriktive tiltak retta mot visse personar og føretak med sikte på motkjemping av terrorisme (EFT L 344 av 28.12.2001, s. 70).

[11] Rådsforordning (EF) nr. 881/2002 av 27. mai 2002 om innføring av visse særlige restriktive tiltak rettet mot visse personer og foretak knyttet til organisasjonene IS (Daesh) og al-Qaida (EFT L 139 av 29.5.2002, s. 9).

[12] Rådsforordning (EU) nr. 356/2010 av 26. april 2010 om innføring av visse særlige restriktive tiltak rettet mot visse fysiske eller juridiske personer, foretak eller organer i lys av situasjonen i Somalia (EUT L 105 av 27.4.2010, s. 1).

banktilsynsmyndighet), som ble opprettet ved europaparlaments- og rådsforordning (EU) nr. 1093/2010[13] (EBA), særlig presisere hvordan ytere av kryptoeiendelstjenester skal ta hensyn til de risikofaktorene som er oppført i vedlegg III til direktiv (EU) 2015/849, blant annet når de utfører transaksjoner med enheter utenfor Unionen som ikke er regulert, registrert eller har en tillatelse i et tredjeland, eller med frittstående adresser. Dersom det identifiseres situasjoner med høyere risiko, bør EBA utstede retningslinjer som spesifiserer hvilke utvidede kundekontrolltiltak de ansvarlige enhetene bør vurdere å anvende for å redusere slike risikoer, herunder vedtakelse av hensiktsmessige prosedyrer, for eksempel bruk av analyseverktøy for desentralisert registerteknologi (DLT), for å fastslå kryptoeiendelers opprinnelse eller bestemmelsessted.

18) Denne forordningen bør få anvendelse uten at det berører de nasjonale restriktive tiltakene og Unionens restriktive tiltak som innføres ved forordninger som bygger på artikkel 215 i traktaten om Den europeiske unions virkemåte, for eksempel forordning (EF) nr. 2580/2001, (EF) nr. 881/2002 og (EU) nr. 356/2010 og rådsforordning (EU) nr. 267/2012[14], (EU) 2016/1686[15] og (EU) 2017/1509[16], som kan kreve at betaleres og betalingsmottakeres betalingstjenesteytere, avsenderes og mottakeres ytere av kryptoeiendelstjenester, ytere av mellomliggende betalingstjenester samt ytere av mellomliggende kryptoeiendelstjenester treffer hensiktsmessige tiltak for å fryse visse midler og kryptoeiendeler, eller at de overholder spesifikke restriksjoner med hensyn til visse pengeoverføringer eller overføringer av kryptoeiendeler. Betalingstjenesteytere og ytere av kryptoeiendelstjenester bør ha innført interne retningslinjer, prosedyrer og kontroller for å sikre gjennomføringen av disse restriktive tiltakene, herunder tiltak for kontroll med hensyn til Unionens og nasjonale lister over utpekte personer. EBA bør utstede retningslinjer som presiserer disse interne retningslinjene, prosedyrene og kontrollene. Denne forordningens krav om interne retningslinjer, prosedyrer og kontroller knyttet til restriktive tiltak skal oppheves i nær framtid ved en europaparlaments- og rådsforordning om tiltak for å hindre at finanssystemet brukes til hvitvasking av penger eller finansiering av terrorisme.

19) Behandlingen av personopplysninger i henhold til denne forordningen bør skje i fullt samsvar med europaparlaments- og rådsforordning (EU) 2016/679[17]. Ytterligere behandling av personopplysninger for kommersielle formål bør være strengt forbudt. Alle medlemsstater anser kampen mot hvitvasking av penger og finansiering av terrorisme som nødvendig av hensyn til allmennhetens interesse. Ved anvendelsen av denne forordningen skal overføring av personopplysninger til et tredjeland skje i samsvar med kapittel V i forordning (EU) 2016/679. Det er viktig at betalingstjenesteytere og ytere av kryptoeiendelstjenester som driver virksomhet i flere jurisdiksjoner og har filialer eller datterforetak utenfor Unionen, ikke hindres i å overføre opplysninger om mistenkelige transaksjoner innenfor den samme organisasjonen, forutsatt at de har tatt tilstrekkelige forholdsregler. Dessuten bør avsenderens og mottakerens ytere av kryptoeiendelstjenester, betalerens og betalingsmottakerens betalingstjenesteytere og yterne av mellomliggende betalingstjenester samt yterne av mellomliggende kryptoeiendelstjenester ha innført hensiktsmessige tekniske og organisatoriske tiltak for å beskytte personopplysningene mot utilsiktet tap, endring, ulovlig videreformidling eller ulovlig tilgang.

20) Personer som bare konverterer papirdokumenter til elektroniske data på grunnlag av en avtale med en betalingstjenesteyter, og personer som utelukkende forsyner betalingstjenesteytere med et meldingssystem eller

---

13 Europaparlaments- og rådsforordning (EU) nr. 1093/2010 av 24. november 2010 om opprettelse av en europeisk tilsynsmyndighet (Den europeiske banktilsynsmyndighet), om endring av beslutning nr. 716/2009/EF og om oppheving av kommisjonsbeslutning 2009/78/EF (EUT L 331 av 15.12.2010, s. 12).

14 Rådsforordning (EU) nr. 267/2012 av 23. mars 2012 om restriktive tiltak mot Iran og om oppheving av forordning (EU) nr. 961/2010 (EUT L 88 av 24.3.2012, s. 1).

15 Rådsforordning (EU) 2016/1686 av 20. september 2016 om innføring av ytterligere restriktive tiltak rettet mot IS (Daesh) og al-Qaida samt fysiske og juridiske personer, foretak eller organer som er knyttet til dem (EUT L 255 av 21.9.2016, s. 1.)

16 Rådsforordning (EU) 2017/1509 av 30. august 2017 om restriktive tiltak rettet mot Den demokratiske folkerepublikk Korea og om oppheving av forordning (EF) nr. 329/2007 (EUT L 224 av 31.8.2017, s. 1).

17 Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) (EUT L 119 av 4.5.2016, s. 1).

andre støttesystemer for pengeoverføringer eller med avregnings- og oppgjørssystemer, faller ikke inn under denne forordningens virkeområde.

21) Personer som bare leverer supplerende infrastruktur, for eksempel leverandører av nettverks- og infrastrukturtjenester for internett, leverandører av skytjenester eller programvareutviklere, som gjør det mulig for en annen enhet å yte tjenester knyttet til overføring av kryptoeiendeler, bør ikke være omfattet av denne forordningens virkeområde med mindre de foretar overføringer av kryptoeiendeler.

22) Denne forordningen bør ikke få anvendelse på overføringer av kryptoeiendeler mellom personer som foretas uten at det benyttes en yter av kryptoeiendelstjenester, eller i tilfeller der både avsenderen og mottakeren er ytere av tjenester knyttet til overføring av kryptoeiendeler, som handler på egne vegne.

23) Pengeoverføringer tilsvarende tjenestene som er omhandlet i artikkel 3 bokstav a)–m) og o) i europaparlaments- og rådsdirektiv (EU) 2015/2366[18], faller ikke inn under denne forordningens virkeområde. Pengeoverføringer og overføringer av e-pengetoken som definert i artikkel 3 nr. 1 punkt 7 i forordning (EU) 2023/1114, med en lav risiko for hvitvasking av penger eller finansiering av terrorisme, bør også unntas fra denne forordningens virkeområde. Slike unntak bør omfatte betalingskort, betalingsinstrumenter for elektroniske penger, mobiltelefoner eller andre forhånds- eller etterhåndsbetalte digitale innretninger eller IT-innretninger med lignende egenskaper dersom de brukes utelukkende til kjøp av varer eller tjenester og nummeret på kortet, instrumentet eller innretningen følger alle overføringer. Bruk av et betalingskort, et betalingsinstrument for elektroniske penger, en mobiltelefon eller en annen forhånds- eller etterhåndsbetalt digital innretning eller IT-innretning med lignende egenskaper for å foreta en pengeoverføring eller overføring av e-pengetoken mellom fysiske personer som opptrer som forbrukere for andre formål enn handel, forretningsvirksomhet eller yrkesvirksomhet, faller imidlertid inn under denne forordningens virkeområde. Dessuten bør uttak fra kontantautomater, betaling av skatter, bøter og andre avgifter, pengeoverføringer som utføres gjennom utveksling av bilder av sjekker, herunder trunkerte sjekker eller veksler, samt pengeoverføringer der både betaleren og betalingsmottakeren er betalingstjenesteytere som opptrer på egne vegne, også unntas fra denne forordningens virkeområde.

24) Kryptoeiendeler som er unike og ikke-ombyttelige, er ikke omfattet av kravene i denne forordningen med mindre de er klassifisert som kryptoeiendeler eller midler i henhold til forordning (EU) 2023/1114.

25) Minibanker for kryptoeiendeler («kryptominibanker») kan gi brukerne mulighet til å foreta overføringer av kryptoeiendeler til en kryptoeiendelsadresse ved å deponere kontanter, ofte uten noen form for identifisering og kontroll av kunder. Kryptominibanker er særlig utsatt for risiko for hvitvasking av penger og finansiering av terrorisme fordi anonymiteten og muligheten for å bruke kontanter av ukjent opprinnelse gjør dem til et ideelt verktøy for ulovlig virksomhet. Med tanke på kryptominibankers rolle når det gjelder å foreta eller aktivt lette overføringer av kryptoeiendeler, bør overføringer av kryptoeiendeler som er knyttet til kryptominibanker, være omfattet av denne forordningens virkeområde.

26) For å gjenspeile særtrekkene ved de nasjonale betalingssystemene, og forutsatt at det alltid er mulig å spore pengeoverføringen tilbake til betaleren, bør medlemsstatene også kunne unnta fra denne forordningens virkeområde visse små, innenlandske pengeoverføringer, herunder elektroniske girobetalinger, som er benyttet til kjøp av varer eller tjenester.

27) På grunn av den iboende grenseløse arten og den globale rekkevidden av overføringer av kryptoeiendeler og av yting av kryptoeiendelstjenester finnes det ingen objektive grunner til å skjelne mellom behandlingen av risikoene for hvitvasking av penger og finansiering av terrorisme ved nasjonale overføringer og overføringer over landegrensene. For å gjenspeile disse særtrekkene bør innenlandske overføringer av kryptoeiendeler av lav verdi ikke unntas fra denne forordningens virkeområde, i samsvar med FATF-kravet om at alle overføringer av kryptoeiendeler skal behandles som grensekryssende.

28) Betalingstjenesteytere og ytere av kryptoeiendelstjenester bør sikre at opplysninger om betaleren og betalingsmottakeren eller om

[18] Europaparlaments- og rådsdirektiv (EU) 2015/2366 av 25. november 2015 om betalingstjenester i det indre marked, om endring av direktiv 2002/65/EF, 2009/110/EF og 2013/36/EU og forordning (EU) nr. 1093/2010 og om oppheving av direktiv 2007/64/EF (EUT L 337 av 23.12.2015, s. 35).

avsenderen og mottakeren ikke mangler eller er ufullstendige.

29) For ikke å redusere betalingssystemenes effektivitet og for å skape en balanse mellom risikoen for at transaksjoner vil skje utenfor det offisielle systemet dersom det pålegges for strenge identifikasjonskrav, og den potensielle terrortrusselen som små pengeoverføringer utgjør, bør plikten til å kontrollere at opplysningene om betaleren eller betalingsmottakeren er riktige ved pengeoverføringer der en kontroll ennå ikke er utført, pålegges bare for enkeltoverføringer som overstiger 1 000 euro, med mindre overføringen synes å være knyttet til andre pengeoverføringer som til sammen overstiger 1 000 euro, pengene er mottatt eller utbetalt i kontanter eller i anonyme elektroniske penger, eller det er rimelig grunn til mistanke om hvitvasking av penger eller finansiering av terrorisme.

30) Sammenlignet med pengeoverføringer kan overføringer av kryptoeiendeler foretas på tvers av flere jurisdiksjoner i større skala og høyere hastighet på grunn av deres globale rekkevidde og teknologiske egenskaper. I tillegg til kryptoeiendelers pseudoanonymitet gir disse særtrekkene ved overføringer av kryptoeiendeler kriminelle mulighet til svært raskt å foreta store ulovlige overføringer og samtidig omgå sporbarhetsforpliktelsene og unngå avsløring ved å strukturere en stor transaksjon i mindre beløp ved hjelp av flere DLT-adresser som tilsynelatende er uten tilknytning til hverandre, herunder engangsbruk av DLT-adresser, og ved hjelp av automatiserte prosesser. De fleste kryptoeiendeler er også svært volatile, og deres verdi kan svinge betydelig innenfor en svært kort tidsramme, noe som gjør beregningen av innbyrdes forbundne transaksjoner mer usikker. For å gjenspeile disse særtrekkene bør overføringer av kryptoeiendeler være omfattet av de samme kravene uavhengig av deres verdi og av om de er innenlandske eller grensekryssende overføringer.

31) Ved pengeoverføringer eller overføringer av kryptoeiendeler der kontrollen anses å ha blitt utført, bør betalingstjenesteytere og ytere av kryptoeiendelstjenester ikke ha plikt til å kontrollere at opplysningene om betaleren eller betalingsmottakeren som følger hver pengeoverføring, eller opplysningene om avsenderen eller mottakeren som følger hver overføring av kryptoeiendeler, er riktige, forutsatt at forpliktelsene fastsatt i direktiv (EU) 2015/849 er oppfylt.

32) På bakgrunn av Unionens regelverksakter om betalingstjenester, dvs. europaparlaments- og rådsforordning (EU) nr. 260/2012[19], europaparlaments- og rådsdirektiv (EU) 2015/2366 og europaparlaments- og rådsforordning (EU) 2021/1230[20], bør det være tilstrekkelig å fastsette at bare forenklede opplysninger trenger å oversendes sammen med pengeoverføringer innenfor Unionen, for eksempel betalingskontonummer eller en entydig transaksjonsidentifikator.

33) For å gjøre det mulig for de myndighetene som har ansvar for å bekjempe hvitvasking av penger eller finansiering av terrorisme i tredjeland, å spore kilden til penger eller kryptoeiendeler som brukes for disse formålene, bør pengeoverføringer eller overføringer av kryptoeiendeler fra Unionen til land utenfor Unionen inneholde fullstendige opplysninger om betaleren og betalingsmottakeren når det gjelder pengeoverføringer, og om avsenderen og mottakeren når det gjelder overføringer av kryptoeiendeler. Fullstendige opplysninger om betaleren og betalingsmottakeren bør inneholde identifikatoren for juridisk person (LEI-kode) eller en tilsvarende offisiell identifikator, dersom betaleren framlegger en slik identifikator for sin betalingstjenesteyter, ettersom dette vil gjøre det mulig å bedre identifisere de partene som er involvert i en pengeoverføring, og lett kan inkluderes i eksisterende formater for betalingsmeldinger, for eksempel det formatet som er utviklet av Den internasjonale standardiseringsorganisasjon for elektronisk datautveksling mellom finansinstitusjoner. De myndighetene som har ansvar for bekjempelse av hvitvasking av penger eller finansiering av terrorisme i tredjeland, bør bare ha tilgang til de fullstendige opplysningene om betaleren og betalingsmottakeren eller om avsenderen og mottakeren, alt etter hva som er relevant, med sikte på å forebygge, avdekke og etterforske hvitvasking av penger og finansiering av terrorisme.

34) Kryptoeiendeler eksisterer i en grenseløs virtuell virkelighet og kan overføres til enhver yter av kryptoeiendelstjenester, uavhengig av

---

[19] Europaparlaments- og rådsforordning (EU) nr. 260/2012 av 14. mars 2012 om tekniske og forretningsmessige krav til kreditoverføringer og direkte debiteringer i euro og om endring av forordning (EF) nr. 924/2009 (EUT L 94 av 30.3.2012, s. 22).

[20] Europaparlaments- og rådsforordning (EU) 2021/1230 av 14. juli 2021 om betalinger på tvers av landegrensene i Unionen (EUT L 274 av 30.7.2021, s. 20).

om yteren er eller ikke er registrert i en jurisdiksjon. Mange jurisdiksjoner utenfor Unionen har innført regler for vern av personopplysninger og håndheving som avviker fra dem som gjelder i Unionen. Ved overføring av kryptoeiendeler på vegne av en kunde til en yter av kryptoeiendelstjenester som ikke er registrert i Unionen, bør avsenderens yter av kryptoeiendelstjenester vurdere om mottakerens yter av kryptoeiendelstjenester er i stand til å motta og oppbevare de opplysningene som kreves i henhold til denne forordningen i samsvar med forordning (EU) 2016/679, eventuelt ved å benytte mulighetene omhandlet i kapittel V i forordning (EU) 2016/679. Det europeiske personvernråd bør etter samråd med EBA utstede retningslinjer for den praktiske gjennomføringen av personvernkravene for overføring av personopplysninger til tredjeland i forbindelse med overføringer av kryptoeiendeler. Det kan oppstå situasjoner der personopplysninger ikke kan sendes fordi kravene i forordning (EU) 2016/679 ikke kan oppfylles. EBA bør utstede retningslinjer for egnede prosedyrer for å fastslå om overføringen av kryptoeiendeler bør gjennomføres, avvises eller innstilles i slike tilfeller.

35) Medlemsstatenes myndigheter som har ansvar for å bekjempe hvitvasking av penger og finansiering av terrorisme, og de berørte rettsmyndighetene og myndigheter som har ansvar for å håndheve loven i medlemsstatene og på unionsplan, bør styrke samarbeidet seg imellom og med berørte tredjelandsmyndigheter, herunder i utviklingsland, for ytterligere å øke åpenheten og fremme utvekslingen av opplysninger og beste praksis.

36) Avsenderens yter av kryptoeiendelstjenester bør sikre at overføringer av kryptoeiendeler ledsages av avsenderens navn, avsenderens desentralisert register-adresse i tilfeller der en overføring av kryptoeiendeler registreres i et nettverk som bruker DLT eller lignende teknologi, avsenderens kryptoeiendelskontonummer i tilfeller der en slik konto finnes og benyttes for å behandle transaksjonen, avsenderens adresse, herunder landets navn, offisielle personlige dokumentnummer og kundeidentifikasjonsnummer eller alternativt avsenderens fødselsdato og -sted og, forutsatt at det nødvendige feltet i det relevante meldingsformatet finnes, og at avsenderen har opplyst sin yter av kryptoeiendelstjenester om den, den aktuelle LEI-koden eller, dersom en slik ikke finnes, enhver annen tilgjengelig tilsvarende offisiell identifikator for avsenderen. Opplysningene bør oversendes på en sikker måte og før eller samtidig eller parallelt med overføringen av kryptoeiendeler.

37) Avsenderens yter av kryptoeiendelstjenester bør også sikre at overføringer av kryptoeiendeler ledsages av mottakerens navn, mottakerens desentralisert register-adresse i tilfeller der en overføring av kryptoeiendeler registreres i et nettverk som bruker DLT eller lignende teknologi, mottakerens kontonummer i tilfeller der en slik konto finnes og benyttes for å behandle transaksjonen, og, forutsatt at det nødvendige feltet i det relevante meldingsformatet finnes, og at avsenderen har opplyst sin yter av kryptoeiendelstjenester om den, den aktuelle LEI-koden eller, dersom en slik ikke finnes, enhver annen tilgjengelig tilsvarende offisiell identifikator for mottakeren. Opplysningene bør oversendes på en sikker måte og før eller samtidig eller parallelt med overføringen av kryptoeiendeler.

38) Med hensyn til overføring av kryptoeiendeler bør kravene i denne forordningen få anvendelse på alle overføringer, også overføringer av kryptoeiendeler til eller fra en frittstående adresse, forutsatt at en yter av kryptoeiendelstjenester er involvert.

39) Ved overføring til eller fra en frittstående adresse bør yteren av kryptoeiendelstjenester innhente opplysninger om både avsenderen og mottakeren, vanligvis fra sin kunde. En yter av kryptoeiendelstjenester bør i prinsippet ikke være forpliktet til å kontrollere opplysningene om brukeren av den frittstående adressen. Ved en overføring av et beløp som overstiger 1 000 euro, som sendes eller mottas på vegne av en kunde hos en yter av kryptoeiendelstjenester til eller fra en frittstående adresse, bør denne yteren av kryptoeiendelstjenester likevel kontrollere om denne frittstående adressen faktisk eies eller kontrolleres av den berørte kunden.

40) Når det gjelder pengeoverføringer fra én enkelt betaler til flere betalingsmottakere som skal sendes i en samleoverføring som inneholder enkeltoverføringer fra Unionen til land utenfor Unionen, bør det fastsettes at slike enkeltoverføringer bare skal inneholde betalerens betalingskontonummer eller den entydige transaksjonsidentifikatoren samt fullstendige opplysninger om betalingsmottakeren, forutsatt at samlefilen inneholder fullstendige og kontrollerte opplysninger om betaleren og

fullstendige og sporbare opplysninger om betalingsmottakeren.

41) Når det gjelder samleoverføringer av kryptoeiendeler, bør det aksepteres at opplysninger om avsenderen og mottakeren oversendes i samlefiler, forutsatt at de oversendes umiddelbart og på en sikker måte. Det bør ikke være tillatt å oversende de påkrevde opplysningene etter overføringen, ettersom oversendingen må skje før eller på det tidspunktet da transaksjonen gjennomføres, og ytere av kryptoeiendelstjenester eller andre ansvarlige enheter bør oversende de påkrevde opplysningene samtidig med samleoverføringen av kryptoeiendeler.

42) For å kunne kontrollere om de nødvendige opplysningene om betaleren og betalingsmottakeren følger pengeoverføringene, og for å bidra til å identifisere mistenkelige transaksjoner, bør betalingsmottakerens betalingstjenesteyter og yteren av mellomliggende betalingstjenester ha innført effektive prosedyrer for å avdekke om opplysningene om betaleren og betalingsmottakeren mangler eller er ufullstendige. Disse prosedyrene bør omfatte overvåking etter og under overføringene dersom det er hensiktsmessig. Vedkommende myndigheter bør sikre at betalingstjenesteytere gjennom hele betalingskjeden tar med nødvendige opplysninger om transaksjonen i den elektroniske overføringen eller i en tilhørende melding.

43) Når det gjelder overføringer av kryptoeiendeler, bør mottakerens yter av kryptoeiendelstjenester gjennomføre effektive prosedyrer for å avdekke om opplysningene om avsenderen eller mottakeren mangler eller er ufullstendige. Disse prosedyrene bør, dersom det er hensiktsmessig, omfatte overvåking etter eller under overføringen. Det bør ikke kreves at opplysningene knyttes direkte til selve overføringen av kryptoeiendeler, så lenge de oversendes før eller samtidig eller parallelt med overføringen av kryptoeiendeler og gjøres tilgjengelige for berørte myndigheter på anmodning.

44) I betraktning av den potensielle risikoen for hvitvasking av penger og finansiering av terrorisme som anonyme overføringer utgjør, er det hensiktsmessig å fastsette at betalingstjenesteytere skal kreve opplysninger om betaleren og betalingsmottakeren og å kreve at ytere av kryptoeiendelstjenester skal kreve opplysninger om avsenderen og mottakeren. I tråd med den risikobaserte metoden FATF har utviklet, bør det identifiseres områder med henholdsvis lavere og høyere risiko for å kunne motvirke risikoen for hvitvasking av penger og finansiering av terrorisme på en mer målrettet måte. Derfor bør mottakerens yter av kryptoeiendelstjenester, betalingsmottakerens betalingstjenesteyter, yteren av mellomliggende betalingstjenester og yteren av mellomliggende kryptoeiendelstjenester ha effektive risikobaserte prosedyrer som kommer til anvendelse i tilfeller der en pengeoverføring mangler de påkrevde opplysningene om betaleren eller betalingsmottakeren, eller der en overføring av kryptoeiendeler mangler de påkrevde opplysningene om avsenderen eller mottakeren, for at tjenesteyteren skal kunne avgjøre om den skal utføre, avvise eller innstille overføringen, og for å kunne fastslå hvilke hensiktsmessige oppfølgingstiltak den bør treffe.

45) Ytere av kryptoeiendelstjenester bør som alle ansvarlige enheter vurdere og overvåke den risikoen som er knyttet til deres kunder, produkter og leveringskanaler. Ytere av kryptoeiendelstjenester bør også vurdere den risikoen som er knyttet til deres transaksjoner, også når de foretar overføringer til eller fra frittstående adresser. Dersom yteren av kryptoeiendelstjenester har eller får kjennskap til at opplysningene om den avsenderen eller mottakeren som bruker en frittstående adresse, er uriktige, eller dersom yteren av kryptoeiendelstjenester støter på uvanlige eller mistenkelige transaksjonsmønstre eller situasjoner med høyere risiko for hvitvasking av penger og finansiering av terrorisme i forbindelse med overføringer som involverer frittstående adresser, bør denne yteren av kryptoeiendelstjenester, dersom det er hensiktsmessig, innføre utvidede kundekontrolltiltak for å styre og redusere risikoene på egnet måte. Yteren av kryptoeiendelstjenester bør ta hensyn til disse omstendighetene når den vurderer om en overføring av kryptoeiendeler eller en tilknyttet transaksjon er uvanlig, og om den skal rapporteres til enheten for finansiell etterretning (Financial Intelligence Unit, FIU) i samsvar med direktiv (EU) 2015/849.

46) Denne forordningen bør revideres i forbindelse med vedtakelsen av en europaparlaments- og rådsforordning om tiltak for å hindre at finanssystemet brukes til hvitvasking av penger eller finansiering av terrorisme, et europaparlaments- og rådsdirektiv om ordninger som medlemsstatene skal innføre for å hindre at finanssystemet brukes til

hvitvasking av penger eller finansiering av terrorisme, og om oppheving av direktiv (EU) 2015/849, og en europaparlaments- og rådsforordning om opprettelse av Myndigheten for bekjempelse av hvitvasking av penger og finansiering av terrorisme og om endring av forordning (EU) nr. 1093/2010, (EU) nr. 1094/2010 og (EU) nr. 1095/2010, for å sikre samsvar med de relevante bestemmelsene.

47) Ved vurderingen av risikoene bør betalingsmottakerens betalingstjenesteyter, yteren av mellomliggende betalingstjenester, mottakerens yter av kryptoeiendelstjenester eller yteren av mellomliggende kryptoeiendelstjenester utvise særlig aktsomhet når de får kjennskap til at opplysninger om betaleren eller betalingsmottakeren eller om avsenderen eller mottakeren, alt etter hva som er relevant, mangler eller er ufullstendige, eller når en overføring av kryptoeiendeler skal anses som mistenkelig på grunnlag av de aktuelle kryptoeiendelenes opprinnelse eller bestemmelsessted, og de bør rapportere mistenkelige transaksjoner til vedkommende myndigheter i samsvar med rapporteringsforpliktelsene fastsatt i direktiv (EU) 2015/849.

48) I likhet med pengeoverføringer mellom betalingstjenesteytere kan overføringer av kryptoeiendeler som involverer ytere av mellomliggende kryptoeiendelstjenester, lette overføringer som et mellomledd i en kjede av overføringer av kryptoeiendeler. I tråd med internasjonale standarder bør slike ytere av mellomliggende tjenester også være omfattet av de kravene som er fastsatt i denne forordningen, på samme måte som eksisterende forpliktelser for ytere av mellomliggende betalingstjenester.

49) Bestemmelsene om pengeoverføringer og overføringer av kryptoeiendeler der opplysninger om betaleren eller betalingsmottakeren eller om avsenderen eller mottakeren mangler eller er ufullstendige, og der overføringer av kryptoeiendeler skal anses som mistenkelige på grunnlag av de aktuelle kryptoeiendelenes opprinnelse eller bestemmelsessted, får anvendelse uten at dette berører pliktene for betalingstjenesteytere, ytere av mellomliggende betalingstjenester, ytere av kryptoeiendelstjenester og ytere av mellomliggende kryptoeiendelstjenester til å avvise eller innstille pengeoverføringer og overføringer av kryptoeiendeler som er i strid med sivilrettslige, forvaltningsrettslige eller strafferettslige bestemmelser.

50) For å sikre teknologinøytralitet bør denne forordningen ikke pålegge ytere av kryptoeiendelstjenester å bruke en bestemt teknologi for overføring av transaksjonsopplysninger. For å sikre en effektiv gjennomføring av kravene som gjelder for ytere av kryptoeiendelstjenester i henhold til denne forordningen, vil det være avgjørende at kryptobransjen deltar i eller leder standardiseringsinitiativer. De resulterende løsningene bør virke sammen gjennom anvendelse av internasjonale standarder eller unionsomfattende standarder som muliggjør rask utveksling av opplysninger.

51) Med sikte på å hjelpe betalingstjenesteytere og ytere av kryptoeiendelstjenester med å innføre effektive prosedyrer for å avdekke tilfeller der de mottar pengeoverføringer eller overføringer av kryptoeiendeler med manglende eller ufullstendige opplysninger om betaleren, betalingsmottakeren, avsenderen eller mottakeren, og med å treffe effektive oppfølgingstiltak bør EBA utstede retningslinjer.

52) For å gjøre det mulig raskt å treffe tiltak i kampen mot hvitvasking av penger og finansiering av terrorisme bør betalingstjenesteytere og ytere av kryptoeiendelstjenester svare raskt på anmodninger om opplysninger om betaleren og betalingsmottakeren eller om avsenderen og mottakeren fra de myndighetene som har ansvar for å bekjempe hvitvasking av penger eller finansiering av terrorisme i den medlemsstaten der disse betalingstjenesteyterne er etablert, eller der disse yterne av kryptoeiendelstjenester har sitt forretningskontor.

53) Antallet virkedager som har gått i medlemsstaten til betalerens betalingstjenesteyter, avgjør antallet dager tilgjengelig for besvarelse av anmodninger om opplysninger om betaleren.

54) Ettersom det i etterforskningen av straffesaker ikke alltid er mulig å identifisere de nødvendige opplysningene eller de involverte personene før mange måneder eller til og med år etter den opprinnelige pengeoverføringen eller overføringen av kryptoeiendeler, og for å kunne få tilgang til viktige bevis i etterforskningen bør det fastsettes at betalingstjenesteytere eller ytere av kryptoeiendelstjenester skal oppbevare opplysninger om betaleren og betalingsmottakeren eller avsenderen og mottakeren i et visst tidsrom med sikte på å forebygge, avdekke og etterforske hvitvasking av penger og finansiering av terrorisme. Dette tidsrommet bør være begrenset til fem år, og deretter bør alle personopplysninger slettes, med mindre noe annet er

fastsatt i nasjonal rett. Dersom det er nødvendig for å forebygge, avdekke eller etterforske hvitvasking av penger eller finansiering av terrorisme, bør medlemsstatene, etter å ha gjennomført en vurdering av om tiltaket er nødvendig og forholdsmessig, ha anledning til å tillate eller kreve at opplysningene skal oppbevares i et ytterligere tidsrom på inntil fem år, uten at det berører nasjonal strafferett om bevis som får anvendelse i pågående etterforskning i straffesaker og rettergang, og i fullt samsvar med europaparlaments- og rådsdirektiv (EU) 2016/680[21]. Disse tiltakene kan revideres i lys av vedtakelsen av en europaparlaments- og rådsforordning om tiltak for å hindre at finanssystemet brukes til hvitvasking av penger eller finansiering av terrorisme.

55) For å forbedre overholdelsen av denne forordningen, og i samsvar med kommisjonsmeldingen av 9. desember 2010 med tittelen «Reinforcing sanctioning regimes in the financial services sector», bør vedkommende myndigheter gis videre fullmakter til å vedta tilsynstiltak samt utvidet sanksjonsmyndighet. Administrative sanksjoner og tiltak bør fastsettes, og i betraktning av hvor viktig kampen mot hvitvasking av penger og finansiering av terrorisme er, bør medlemsstatene fastsette sanksjoner og tiltak som er effektive og forholdsmessige og virker avskrekkende. Medlemsstatene bør underrette Kommisjonen og den faste interne komiteen for bekjempelse av hvitvasking av penger og finansiering av terrorisme som er omhandlet i artikkel 9a nr. 7 i forordning (EU) nr. 1093/2010, om disse sanksjonene og tiltakene.

56) For å sikre ensartede vilkår for gjennomføringen av denne forordningen bør Kommisjonen gis gjennomføringsmyndighet. Denne myndigheten bør utøves i samsvar med europaparlaments- og rådsforordning (EU) nr. 182/2011[22].

57) En rekke land og territorier som ikke utgjør en del av Unionens territorium, inngår i en monetær union med en medlemsstat, tilhører en medlemsstats valutaområde eller har undertegnet en monetær avtale med Unionen representert ved en medlemsstat, og har betalingstjenesteytere som deltar direkte eller indirekte i betalings- og oppgjørssystemer i denne medlemsstaten. For å unngå at anvendelsen av denne forordningen på pengeoverføringer mellom de berørte medlemsstatene og disse landene eller territoriene får en betydelig negativ innvirkning på økonomien i disse landene eller territoriene, bør det åpnes for at slike pengeoverføringer kan behandles som pengeoverføringer innenfor de berørte medlemsstatene.

58) I lys av de potensielt høye risikoene som er knyttet til frittstående adresser, og den teknologiske og regelverksmessige kompleksiteten som de innebærer, herunder i forbindelse med kontroll av eierskapsopplysninger, bør Kommisjonen innen 1. juli 2026 vurdere behovet for ytterligere spesifikke tiltak for å redusere de risikoene som er knyttet til overføringer til eller fra frittstående adresser eller til eller fra enheter som ikke er etablert i Unionen, herunder innføring av eventuelle begrensninger, og den bør vurdere om de ordningene som benyttes for å kontrollere nøyaktigheten av opplysningene om eierskapet til frittstående adresser, er effektive og forholdsmessige.

59) For tiden får direktiv (EU) 2015/849 bare anvendelse på to kategorier av ytere av kryptoeiendelstjenester, det vil si tilbydere av oppbevaringstjenester for virtuelle valutaer og tilbydere av vekslingstjenester mellom virtuelle valutaer og offisielle valutaer. For å lukke eksisterende smutthull i rammen for bekjempelse av hvitvasking av penger og finansiering av terrorisme og for å tilpasse unionsretten til internasjonale anbefalinger bør direktiv (EU) 2015/849 endres slik at det omfatter alle kategorier av ytere av kryptoeiendelstjenester som definert i forordning (EU) 2023/1114, som dekker et bredere spekter av ytere av kryptoeiendelstjenester. For å sikre at ytere av kryptoeiendelstjenester er omfattet av de samme kravene og det samme tilsynsnivået som kreditt- og finansinstitusjoner, er det særlig hensiktsmessig å ajourføre listen over ansvarlige enheter ved å inkludere ytere av kryptoeiendelstjenester i kategorien finansinstitusjoner med sikte på direktiv (EU) 2015/849. I lys av at tradisjonelle finansinstitusjoner også omfattes av definisjonen av ytere av kryptoeiendelstjenester når de tilbyr slike tjenester, innebærer identifi-

---

[21] Europaparlaments- og rådsdirektiv (EU) 2016/680 av 27. april 2016 om vern av fysiske personer i forbindelse med vedkommende myndigheters behandling av personopplysninger med henblikk på å forebygge, etterforske, avsløre eller straffeforfølge straffbare forhold eller iverksette strafferettslige sanksjoner, om fri utveksling av slike opplysninger og om oppheving av Rådets rammebeslutning 2008/977/JIS (EUT L 119 av 4.5.2016, s. 89).

[22] Europaparlaments- og rådsforordning (EU) nr. 182/2011 av 16. februar 2011 om fastsettelse av allmenne regler og prinsipper for medlemsstatenes kontroll med Kommisjonens utøvelse av sin gjennomføringsmyndighet (EUT L 55 av 28.2.2011, s. 13).

seringen av ytere av kryptoeiendelstjenester som finansinstitusjoner dessuten at et ensartet sett av regler kan anvendes på enheter som yter både tradisjonelle finansielle tjenester og kryptoeiendelstjenester. Direktiv (EU) 2015/849 bør også endres for å sikre at ytere av kryptoeiendelstjenester på en hensiktsmessig måte kan redusere de risikoene for hvitvasking av penger og finansiering av terrorisme som de er utsatt for.

60) Forbindelser som opprettes mellom ytere av kryptoeiendelstjenester og enheter som er etablert i tredjeland, med sikte på å gjennomføre overføringer av kryptoeiendeler eller yting av lignende kryptoeiendelstjenester, har likhetstrekk med korrespondentbankforbindelser som opprettes med et tredjelands respondentinstitusjon. Ettersom disse forbindelsene kjennetegnes av at de er løpende og gjentakende, bør de anses som en form for korrespondentforbindelse og være omfattet av spesifikke utvidede kundekontrolltiltak som i prinsippet svarer til dem som anvendes i forbindelse med banktjenester og finansielle tjenester. Ytere av kryptoeiendelstjenester bør særlig, når de oppretter en ny korrespondentforbindelse med en respondentenhet, anvende spesifikke utvidede kundekontrolltiltak med sikte på å identifisere og vurdere den berørte respondentens risikoeksponering på grunnlag av dens omdømme, tilsynets kvalitet og dens kontroller for bekjempelse av hvitvasking av penger og finansiering av terrorisme (AML/CFT-kontroller). På grunnlag av de innhentede opplysningene bør korrespondentyterne av kryptoeiendelstjenester gjennomføre hensiktsmessige risikoreduserende tiltak, som særlig bør ta hensyn til at enheter som ikke er registrert eller ikke har en tillatelse, kan innebære høyere risiko for hvitvasking av penger og finansiering av terrorisme. Dette er særlig relevant så lenge det fortsatt er varierende gjennomføring av FATFs standarder for kryptoeiendeler på globalt plan, noe som medfører ytterligere risikoer og utfordringer. EBA bør gi veiledning om hvordan ytere av kryptoeiendelstjenester bør gjennomføre de utvidede kundekontrolltiltakene, og bør spesifisere de hensiktsmessige risikoreduserende tiltakene, herunder minstekrav til de tiltakene som skal treffes, ved samhandling med enheter som yter kryptoeiendelstjenester uten å være registrert eller ha en tillatelse.

61) Ved forordning (EU) 2023/1114 er det fastsatt omfattende rammeregler for ytere av kryptoeiendelstjenester, som harmoniserer reglene for tillatelsen til og driften av ytere av kryptoeiendelstjenester i hele Unionen. For å unngå overlappende krav bør direktiv (EU) 2015/849 endres for å fjerne registreringskrav i forbindelse med de kategoriene av ytere av kryptoeiendelstjenester som vil bli omfattet av en felles godkjenningsordning i henhold til forordning (EU) 2023/1114.

62) Ettersom målene for denne forordningen, som er å bekjempe hvitvasking av penger og finansiering av terrorisme, herunder ved å gjennomføre internasjonale standarder, og idet det sikres tilgang til grunnleggende opplysninger om betalere og betalingsmottakere ved pengeoverføringer og om avsendere og mottakere ved overføringer av kryptoeiendeler, ikke kan nås i tilstrekkelig grad av medlemsstatene og derfor på grunn av tiltakets omfang og virkninger bedre kan nås på unionsplan, kan Unionen treffe tiltak i samsvar med nærhetsprinsippet som fastsatt i artikkel 5 i traktaten om Den europeiske union. I samsvar med forholdsmessighetsprinsippet fastsatt i nevnte artikkel går denne forordningen ikke lenger enn det som er nødvendig for å nå disse målene.

63) Denne forordningen er underlagt europaparlaments- og rådsforordning (EU) 2016/679 og (EU) 2018/1725[23]. Den er forenlig med de grunnleggende rettighetene og de prinsippene som er anerkjent i Den europeiske unions pakt om grunnleggende rettigheter, særlig retten til respekt for privatliv og familieliv (artikkel 7), retten til vern av personopplysninger (artikkel 8), retten til effektiv klageadgang og rettferdig rettergang (artikkel 47) og forbudet mot gjentatt straffeforfølgning.

64) For å sikre samsvar med forordning (EU) 2023/1114 bør denne forordningen få anvendelse fra anvendelsesdatoen for nevnte forordning. Senest samme dato bør medlemsstatene også gjennomføre endringene av direktiv (EU) 2015/849.

65) EUs datatilsyn er blitt rådspurt i samsvar med artikkel 42 nr. 1 i forordning (EU) 2018/1725 og avga uttalelse 22. september 2021[24].

---

[23] Europaparlaments- og rådsforordning (EU) 2018/1725 av 23. oktober 2018 om vern av fysiske personer i forbindelse med behandling av personopplysninger i Unionens institusjoner, organer, kontorer og byråer og om fri utveksling av slike opplysninger samt om oppheving av forordning (EF) nr. 45/2001 og beslutning nr. 1247/2002/EF (EUT L 295 av 21.11.2018, s. 39).

[24] EUT C 524 av 29.12 2021, s. 10.

VEDTATT DENNE FORORDNINGEN:

Kapittel I

Formål, virkeområde og definisjoner

Artikkel 1

Formål

Denne forordningen fastsetter regler for opplysninger om betalere og betalingsmottakere som skal følge pengeoverføringer i enhver valuta, og for opplysninger om avsendere og mottakere som skal følge overføringer av kryptoeiendeler, med sikte på å forebygge, avdekke og etterforske hvitvasking av penger og finansiering av terrorisme, når minst en av de betalingstjenesteyterne eller yterne av kryptoeiendelstjenester som er involvert i pengeoverføringen eller overføringen av kryptoeiendeler, er etablert eller har sitt forretningskontor, alt etter hva som er relevant, i Unionen. Denne forordningen fastsetter også regler om interne retningslinjer, prosedyrer og kontroller for å sikre gjennomføringen av restriktive tiltak når minst en av de betalingstjenesteyterne eller yterne av kryptoeiendelstjenester som er involvert i pengeoverføringen eller overføringen av kryptoeiendeler, er etablert eller har sitt forretningskontor, alt etter hva som er relevant, i Unionen.

Artikkel 2

Virkeområde

1. Denne forordningen får anvendelse på pengeoverføringer i enhver valuta som sendes eller mottas av en betalingstjenesteyter eller en yter av mellomliggende betalingstjenester som er etablert i Unionen. Den får også anvendelse på overføringer av kryptoeiendeler, herunder overføringer av kryptoeiendeler som utføres ved hjelp av kryptominibanker, når enten avsenderens eller mottakerens yter av kryptoeiendelstjenester eller yter av mellomliggende kryptoeiendelstjenester har sitt forretningskontor i Unionen.
2. Denne forordningen får ikke anvendelse på de tjenestene som er oppført i artikkel 3 bokstav a)–m) og o) i direktiv (EU) 2015/2366.
3. Denne forordningen får ikke anvendelse på pengeoverføringer eller overføringer av e-pengetoken som definert i artikkel 3 nr. 1 punkt 7 i forordning (EU) 2023/1114, som utføres ved hjelp av et betalingskort, et betalingsinstrument for elektroniske penger, en mobiltelefon eller en annen forhånds- eller etterhåndsbetalt digital innretning eller IT-innretning med lignende egenskaper, dersom følgende vilkår er oppfylt:
   a) Kortet, instrumentet eller innretningen brukes utelukkende til å betale for varer eller tjenester.
   b) Nummeret på kortet, instrumentet eller innretningen følger alle overføringer som er forbundet med transaksjonen.

   Denne forordningen får imidlertid anvendelse når et betalingskort, et betalingsinstrument for elektroniske penger, en mobiltelefon eller en annen forhånds- eller etterhåndsbetalt digital innretning eller IT-innretning med lignende egenskaper brukes til å utføre en overføring av penger eller e-pengetoken mellom fysiske personer som opptrer som forbrukere for andre formål enn handel, forretningsvirksomhet eller yrkesvirksomhet.
4. Denne forordningen får ikke anvendelse på personer som ikke driver annen virksomhet enn å konvertere papirdokumenter til elektroniske data, og som gjør dette i henhold til en avtale med en betalingstjenesteyter, eller på personer som ikke driver annen virksomhet enn å forsyne betalingstjenesteytere med meldingssystemer eller andre støttesystemer for pengeoverføringer eller med avregnings- og oppgjørssystemer.

   Denne forordningen får ikke anvendelse på en pengeoverføring dersom noen av følgende vilkår er oppfylt:
   a) Den innebærer at betaleren tar ut kontanter fra sin egen betalingskonto.
   b) Den utgjør en overføring av penger til en offentlig myndighet til betaling av skatter, bøter eller andre avgifter innenfor en medlemsstat.
   c) Både betaleren og betalingsmottakeren er betalingstjenesteytere som opptrer på egne vegne.
   d) Den utføres gjennom utveksling av bilder av sjekker, herunder trunkerte sjekker.

   Denne forordningen får ikke anvendelse på en overføring av kryptoeiendeler dersom noen av følgende vilkår er oppfylt:
   a) Både avsenderen og mottakeren er ytere av kryptoeiendelstjenester som opptrer på egne vegne.
   b) Overføringen er en overføring av kryptoeiendeler mellom personer, som utføres uten at det benyttes en yter av kryptoeiendelstjenester.

   E-pengetoken som definert i artikkel 3 nr. 1 punkt 7 i forordning (EU) 2023/1114 skal

behandles som kryptoeiendeler i henhold til denne forordningen.

5. En medlemsstat kan beslutte ikke å anvende denne forordningen på pengeoverføringer innenfor sitt territorium til en betalingsmottakers betalingskonto som utelukkende tillater betaling for yting av varer eller tjenester, forutsatt at samtlige av følgende vilkår er oppfylt:
   a) Betalingsmottakerens betalingstjenesteyter er omfattet av direktiv (EU) 2015/849.
   b) Betalingsmottakerens betalingstjenesteyter har mulighet til, ved hjelp av en entydig transaksjonsidentifikator, å spore pengeoverføringen via betalingsmottakeren tilbake til den personen som har en avtale med betalingsmottakeren om yting av varer eller tjenester.
   c) Pengeoverføringens beløp overstiger ikke 1 000 euro.

Artikkel 3

Definisjoner

I denne forordningen menes med

1) «finansiering av terrorisme» finansiering av terrorisme som definert i artikkel 1 nr. 5 i direktiv (EU) 2015/849,
2) «hvitvasking av penger» de hvitvaskingshandlingene som er nevnt i artikkel 1 nr. 3 og 4 i direktiv (EU) 2015/849,
3) «betaler» en person som innehar en betalingskonto og tillater en pengeoverføring fra denne betalingskontoen, eller, dersom det ikke finnes noen betalingskonto, som gir ordre om en pengeoverføring,
4) «betalingsmottaker» den personen som er den tiltenkte mottakeren av pengeoverføringen,
5) «betalingstjenesteyter» de kategoriene betalingstjenesteytere som det vises til i artikkel 1 nr. 1 i direktiv (EU) 2015/2366, fysiske eller juridiske personer som omfattes av et av unntakene i artikkel 32 i samme direktiv, samt juridiske personer som omfattes av et av unntakene i henhold til artikkel 9 i direktiv 2009/110/EF, og som yter pengeoverføringstjenester,
6) «yter av mellomliggende betalingstjenester» en betalingstjenesteyter som ikke er betalerens eller betalingsmottakerens betalingstjenesteyter, og som tar imot og effektuerer en pengeoverføring på vegne av betalerens eller betalingsmottakerens betalingstjenesteyter eller på vegne av en annen yter av mellomliggende betalingstjenester,
7) «betalingskonto» en betalingskonto som definert i artikkel 4 nr. 12 i direktiv (EU) 2015/2366,
8) «midler» midler som definert i artikkel 4 nr. 25 i direktiv (EU) 2015/2366,
9) «pengeoverføring» enhver transaksjon som i det minste delvis utføres elektronisk på vegne av en betaler gjennom en betalingstjenesteyter, med sikte på å stille midler til rådighet for en betalingsmottaker hos en betalingstjenesteyter, uavhengig av om betaleren og betalingsmottakeren er samme person, og uavhengig av om betalerens og betalingsmottakerens betalingstjenesteyter er samme person, herunder
   a) en kreditoverføring som definert i artikkel 4 nr. 24 i direktiv (EU) 2015/2366,
   b) en direkte debitering som definert i artikkel 4 nr. 23 i direktiv (EU) 2015/2366,
   c) en pengeoverføring som definert i artikkel 4 nr. 22 i direktiv (EU) 2015/2366, enten innenlandsk eller over landegrensene,
   d) en overføring utført ved hjelp av et betalingskort, et betalingsinstrument for elektroniske penger, en mobiltelefon eller en annen forhånds- eller etterhåndsbetalt digital innretning eller IT-innretning med lignende egenskaper,
10) «overføring av kryptoeiendeler» en transaksjon som har som formål å flytte kryptoeiendeler fra én desentralisert register-adresse, én kryptoeiendelskonto eller en annen enhet som muliggjør oppbevaring av kryptoeiendeler, til en annen, som utføres av minst én yter av kryptoeiendelstjenester som opptrer på vegne av enten en avsender eller en mottaker, uavhengig av om avsenderen og mottakeren er samme person, og uavhengig av om avsenderens og mottakerens yter av kryptoeiendelstjenester er en og samme yter,
11) «samleoverføring» en pakke av flere individuelle pengeoverføringer eller overføringer av kryptoeiendeler som sendes samlet,
12) «entydig transaksjonsidentifikator» en kombinasjon av bokstaver, tall eller symboler som fastsettes av betalingstjenesteyteren i samsvar med protokoller for betalings- og oppgjørssystemer eller meldingssystemer som brukes til å utføre pengeoverføringen, eller som fastsettes av en yter av kryptoeiendelstjenester, og som gjør det mulig å spore transaksjonen tilbake til betaleren og betalingsmottakeren, eller å spore overføringen av kryptoeiendeler tilbake til avsenderen og mottakeren,
13) «overføring av kryptoeiendeler mellom personer» en overføring av kryptoeiendeler uten at

det benyttes en yter av kryptoeiendelstjenester,

14) «kryptoeiendel» en kryptoeiendel som definert i artikkel 3 nr. 1 punkt 5 i forordning (EU) 2023/1114, unntatt når den inngår i de kategoriene som er oppført i artikkel 2 nr. 2, 3 og 4 i nevnte forordning, eller på annen måte kan anses som midler,
15) «yter av kryptoeiendelstjenester» en yter av kryptoeiendelstjenester som definert i artikkel 3 nr. 1 punkt 15 i forordning (EU) 2023/1114, når denne yter en eller flere av de kryptoeiendelstjenestene som er definert i artikkel 3 nr. 1 punkt 16 i nevnte forordning,
16) «yter av mellomliggende kryptoeiendelstjenester» en yter av kryptoeiendelstjenester som ikke er avsenderens eller mottakerens yter av kryptoeiendelstjenester, og som tar imot og effektuerer en overføring av kryptoeiendeler på vegne av avsenderens eller mottakerens yter av kryptoeiendelstjenester eller på vegne av en annen yter av mellomliggende kryptoeiendelstjenester,
17) «minibanker for kryptoeiendeler» eller «kryptominibanker»« fysiske eller nettbaserte elektroniske terminaler som gjør det mulig for en yter av kryptoeiendelstjenester å særlig utføre overføringstjenester for kryptoeiendeler, som omhandlet i artikkel 3 nr. 1 punkt 16 bokstav j) i forordning (EU) 2023/1114,
18) «desentralisert register-adresse» en alfanumerisk kode som identifiserer en adresse i et nettverk som bruker desentralisert registerteknologi (distributed ledger technology – DLT) eller lignende teknologi, som kryptoeiendeler kan sendes til eller mottas fra,
19) «kryptoeiendelskonto» en konto som innehas av en yter av kryptoeiendelstjenester i en eller flere fysiske eller juridiske personers navn, og som kan brukes for å gjennomføre overføringer av kryptoeiendeler,
20) «frittstående adresse» en desentralisert register-adresse som ikke er knyttet til noen av følgende:
    a) En yter av kryptoeiendelstjenester.
    b) En enhet som ikke er etablert i Unionen, og som yter tjenester som ligner de tjenestene som ytes av en yter av kryptoeiendelstjenester,
21) «avsender» en person som har en kryptoeiendelskonto hos en yter av kryptoeiendelstjenester, en desentralisert register-adresse eller en enhet som muliggjør oppbevaring av kryptoeiendeler, og som gjør det mulig å overføre kryptoeiendeler fra denne kontoen, desentraliserte register-adressen eller enheten, eller, dersom en slik konto, desentralisert register-adresse eller enhet ikke finnes, en person som gir en ordre om eller initierer en overføring av kryptoeiendeler,
22) «mottaker» den personen som er den tiltenkte mottakeren av de overførte kryptoeiendelene,
23) «identifikator for juridisk person» eller «LEI» en alfanumerisk referansekode som er basert på ISO 17442-standarden, og som er tildelt en juridisk person,
24) «desentralisert registerteknologi» eller «DLT» desentralisert registerteknologi som definert i artikkel 3 nr. 1 punkt 1 i forordning (EU) 2023/1114.

Kapittel II

Plikter for betalingstjenesteytere

Avsnitt 1

Plikter for betalerens betalingstjenesteyter

Artikkel 4

Opplysninger som skal følge pengeoverføringer

1. Betalerens betalingstjenesteyter skal sikre at pengeoverføringer følges av følgende opplysninger om betaleren:
    a) Betalerens navn.
    b) Betalerens betalingskontonummer.
    c) Betalerens adresse, herunder landets navn, offisielt personlig dokumentnummer og kundeidentifikasjonsnummer eller alternativt betalerens fødselsdato og -sted.
    d) Betalerens aktuelle LEI-kode eller, dersom en slik kode ikke finnes, enhver tilgjengelig tilsvarende offisiell identifikator, forutsatt at det nødvendige feltet i det relevante betalingsmeldingsformatet finnes, og at betaleren har opplyst sin betalingstjenesteyter om den.
2. Betalerens betalingstjenesteyter skal sikre at pengeoverføringer følges av følgende opplysninger om betalingsmottakeren:
    a) Betalingsmottakerens navn.
    b) Betalingsmottakerens betalingskontonummer.
    c) Betalingsmottakerens aktuelle LEI-kode eller, dersom en slik kode ikke finnes, enhver tilgjengelig tilsvarende offisiell identifikator, forutsatt at det nødvendige feltet i det relevante betalingsmeldingsformatet finnes, og at betaleren har opplyst sin betalingstjenesteyter om den.
3. Som unntak fra nr. 1 bokstav b) og nr. 2 bokstav b) skal betalerens betalingstjenesteyter,

når det gjelder en overføring som ikke foretas til eller fra en betalingskonto, sikre at pengeoverføringen følges av en entydig transaksjonsidentifikator og ikke av betalingskontonummeret.

4. Før midlene overføres, skal betalerens betalingstjenesteyter kontrollere, på grunnlag av dokumenter, data eller opplysninger innhentet fra en pålitelig og uavhengig kilde, at opplysningene nevnt i nr. 1, og eventuelt i nr. 3, er korrekte.
5. Kontrollen omhandlet i nr. 4 i denne artikkelen skal anses å ha blitt utført dersom et av følgende forhold gjør seg gjeldende:
   a) Betalerens identitet er kontrollert i samsvar med artikkel 13 i direktiv (EU) 2015/849 og opplysningene innhentet ved kontrollen er oppbevart i samsvar med artikkel 40 i nevnte direktiv.
   b) Betaleren er omfattet av artikkel 14 nr. 5 i direktiv (EU) 2015/849.
6. Uten at det berører unntakene fastsatt i artikkel 5 og 6, skal betalerens betalingstjenesteyter ikke utføre noen pengeoverføringer før den har forsikret seg om at alle krav i denne artikkelen er oppfylt.

Artikkel 5

Pengeoverføringer innenfor Unionen

1. Som unntak fra artikkel 4 nr. 1 og 2 skal pengeoverføringer der alle betalingstjenesteytere i betalingskjeden er etablert i Unionen, følges av minst både betalerens og betalingsmottakerens betalingskontonummer eller, dersom artikkel 4 nr. 3 kommer til anvendelse, den entydige transaksjonsidentifikatoren, uten at dette berører opplysningskravene fastsatt i forordning (EU) nr. 260/2012, der det er relevant.
2. Uten hensyn til nr. 1 skal betalerens betalingstjenesteyter innen tre virkedager etter å ha mottatt en anmodning om opplysninger fra betalingsmottakerens betalingstjenesteyter eller fra yteren av mellomliggende betalingstjenester, gjøre tilgjengelig følgende:
   a) For pengeoverføringer som overstiger 1 000 euro, uten hensyn til om overføringene utføres i én enkelt transaksjon eller flere transaksjoner som synes å henge sammen, de opplysningene om betaleren eller betalingsmottakeren som er nevnt i artikkel 4.
   b) For pengeoverføringer som ikke overstiger 1 000 euro, og som ikke synes å henge sammen med andre pengeoverføringer som sammen med den aktuelle overføringen overstiger 1 000 euro, minst
      i) navnet på betaleren og betalingsmottakeren, og
      ii) betalerens og betalingsmottakerens betalingskontonummer eller, dersom artikkel 4 nr. 3 kommer til anvendelse, den entydige transaksjonsidentifikatoren.
3. Som unntak fra artikkel 4 nr. 4 trenger ikke betalerens betalingstjenesteyter, når det gjelder pengeoverføringene nevnt i nr. 2 bokstav b) i denne artikkelen, å kontrollere opplysningene om betaleren med mindre betalerens betalingstjenesteyter
   a) har mottatt pengene som skal overføres, i kontanter eller i anonyme elektroniske penger eller
   b) har rimelig grunn til mistanke om hvitvasking av penger eller finansiering av terrorisme.

Artikkel 6

Pengeoverføringer til land utenfor Unionen

1. Ved en samleoverføring fra én enkelt betaler der betalingsmottakernes betalingstjenesteytere er etablert utenfor Unionen, får artikkel 4 nr. 1 ikke anvendelse på de enkeltoverføringene som er samlet, forutsatt at samlefilen inneholder opplysningene nevnt i artikkel 4 nr. 1, 2 og 3, at opplysningene har blitt kontrollert i samsvar med artikkel 4 nr. 4 og 5, og at enkeltoverføringene inneholder betalerens betalingskontonummer eller, dersom artikkel 4 nr. 3 kommer til anvendelse, den entydige transaksjonsidentifikatoren.
2. Som unntak fra artikkel 4 nr. 1 og uten at det berører opplysningene som kreves i henhold til forordning (EU) nr. 260/2012, der det er relevant, skal pengeoverføringer som ikke overstiger 1 000 euro, og som ikke synes å henge sammen med andre pengeoverføringer som sammen med den aktuelle overføringen overstiger 1 000 euro, og der betalingsmottakerens betalingstjenesteyter er etablert utenfor Unionen, følges av minst følgende opplysninger:
   a) Navnet på betaleren og betalingsmottakeren.
   b) Betalerens og betalingsmottakerens betalingskontonummer eller, dersom artikkel 4 nr. 3 kommer til anvendelse, den entydige transaksjonsidentifikatoren.

   Som unntak fra artikkel 4 nr. 4 trenger ikke betalerens betalingstjenesteyter å kontrollere opplysningene om betaleren som nevnt i dette

nummeret, med mindre betalerens betalingstjenesteyter
a) har mottatt pengene som skal overføres, i kontanter eller i anonyme elektroniske penger eller
b) har rimelig grunn til mistanke om hvitvasking av penger eller finansiering av terrorisme.

Avsnitt 2

Plikter for betalingsmottakerens betalingstjenesteyter

Artikkel 7

Avdekking av manglende opplysninger om betaleren eller betalingsmottakeren

1. Betalingsmottakerens betalingstjenesteyter skal gjennomføre effektive prosedyrer for å avdekke om feltene med opplysninger om betaleren og betalingsmottakeren i meldingssystemet eller betalings- og oppgjørssystemet som brukes til å utføre pengeoverføringen, er utfylt med tillatte tegn eller inndata i henhold til reglene for systemet.
2. Betalingsmottakerens betalingstjenesteyter skal gjennomføre effektive prosedyrer, herunder overvåking etter eller under overføringene, der det er relevant, for å avdekke om følgende opplysninger om betaleren eller betalingsmottakeren mangler:
   a) For pengeoverføringer der betalerens betalingstjenesteyter er etablert i Unionen, opplysningene nevnt i artikkel 5.
   b) For pengeoverføringer der betalerens betalingstjenesteyter er etablert utenfor Unionen, opplysningene nevnt i artikkel 4 nr. 1 bokstav a), b) og c) og artikkel 4 nr. 2 bokstav a) og b).
   c) For samleoverføringer der betalerens betalingstjenesteyter er etablert utenfor Unionen, opplysningene nevnt i artikkel 4 nr. 1 bokstav a), b) og c) og artikkel 4 nr. 2 bokstav a) og b) for den aktuelle samleoverføringen.
3. Ved pengeoverføringer som overstiger 1 000 euro, uten hensyn til om overføringene utføres i én enkelt transaksjon eller flere transaksjoner som synes å henge sammen, skal betalingsmottakerens betalingstjenesteyter, før betalingsmottakerens betalingskonto krediteres eller midlene gjøres tilgjengelige for betalingsmottakeren, kontrollere, på grunnlag av dokumenter, data eller opplysninger innhentet fra en pålitelig og uavhengig kilde, at opplysningene om betalingsmottakeren nevnt i nr. 2 i denne artikkelen er korrekte, uten at dette berører kravene fastsatt i artikkel 83 og 84 i direktiv (EU) 2015/2366.
4. Ved pengeoverføringer som ikke overstiger 1 000 euro, og som ikke synes å henge sammen med andre pengeoverføringer som sammen med den aktuelle overføringen overstiger 1 000 euro, trenger ikke betalingsmottakerens betalingstjenesteyter å kontrollere at opplysningene om betalingsmottakeren er korrekte, med mindre betalingsmottakerens betalingstjenesteyter
   a) utbetaler midlene i kontanter eller i anonyme elektroniske penger eller
   b) har rimelig grunn til mistanke om hvitvasking av penger eller finansiering av terrorisme.
5. Kontrollen nevnt i nr. 3 og 4 i denne artikkelen skal anses å ha blitt utført dersom et av følgende forhold gjør seg gjeldende:
   a) Betalingsmottakerens identitet er kontrollert i samsvar med artikkel 13 i direktiv (EU) 2015/849 og opplysningene innhentet ved kontrollen er oppbevart i samsvar med artikkel 40 i nevnte direktiv.
   b) Betalingsmottakeren er omfattet av artikkel 14 nr. 5 i direktiv (EU) 2015/849.

Artikkel 8

Pengeoverføringer med manglende eller ufullstendige opplysninger om betaleren eller betalingsmottakeren

1. Betalingsmottakerens betalingstjenesteyter skal gjennomføre effektive risikobaserte prosedyrer, herunder prosedyrer som bygger på risikovurderingen nevnt i artikkel 13 i direktiv (EU) 2015/849, for å avgjøre om en pengeoverføring som mangler fullstendige opplysninger om betaleren eller betalingsmottakeren, skal utføres, avvises eller innstilles, og for å treffe hensiktsmessige oppfølgingstiltak.

   Dersom betalingsmottakerens betalingstjenesteyter ved mottak av en pengeoverføring får kjennskap til at opplysningene nevnt i artikkel 4 nr. 1 bokstav a), b) og c), artikkel 4 nr. 2 bokstav a) og b), artikkel 5 nr. 1 eller artikkel 6 mangler eller er ufullstendige eller ikke er fylt ut med tillatte tegn eller inndata i henhold til reglene for meldingssystemet eller betalings- og oppgjørssystemet som nevnt i artikkel 7 nr. 1, skal betalingsmottakerens betalingstjenesteyter på grunnlag av en risikovurdering
   a) avvise overføringen eller

b) be om de nødvendige opplysningene om betaleren og betalingsmottakeren før eller etter at betalingsmottakerens betalingskonto krediteres eller midlene gjøres tilgjengelige for betalingsmottakeren.

2. Dersom en betalingstjenesteyter gjentatte ganger unnlater å gi de påkrevde opplysningene om betaleren eller betalingsmottakeren, skal betalingsmottakerens betalingstjenesteyter
   a) treffe tiltak, som i første omgang kan omfatte utsending av advarsler og fastsettelse av frister, før den går videre med en avvisning, begrensning eller avslutning i samsvar med bokstav b) dersom de påkrevde opplysningene fortsatt ikke er gitt, eller
   b) direkte avvise enhver framtidig pengeoverføring fra denne betalingstjenesteyteren eller begrense eller avslutte forretningsforbindelsen med denne betalingstjenesteyteren.

   Betalingsmottakerens betalingstjenesteyter skal rapportere forholdet og redegjøre for de tiltakene som er truffet, til vedkommende myndighet som har ansvar for å føre tilsyn med at bestemmelsene som gjelder bekjempelse av hvitvasking av penger og finansiering av terrorisme, blir overholdt.

Artikkel 9

Vurdering og rapportering

Betalingsmottakerens betalingstjenesteyter skal anse manglende eller ufullstendige opplysninger om betaleren eller betalingsmottakeren som en faktor i vurderingen av om en pengeoverføring eller en tilknyttet transaksjon er mistenkelig, og om den skal rapporteres til enheten for finansiell etterretning i samsvar med direktiv (EU) 2015/849.

Avsnitt 3

Plikter for ytere av mellomliggende betalingstjenester

Artikkel 10

Oppbevaring av opplysninger om betaleren og betalingsmottakeren som følger overføringen

Ytere av mellomliggende betalingstjenester skal sikre at alle opplysninger som mottas om betaleren og betalingsmottakeren sammen med en pengeoverføring, oppbevares sammen med overføringen.

Artikkel 11

Avdekking av manglende opplysninger om betaleren eller betalingsmottakeren

1. Yteren av mellomliggende betalingstjenester skal gjennomføre effektive prosedyrer for å avdekke om feltene med opplysninger om betaleren og betalingsmottakeren i meldingssystemet eller betalings- og oppgjørssystemet som brukes til å utføre pengeoverføringen, er utfylt med tillatte tegn eller inndata i henhold til reglene for systemet.
2. Yteren av mellomliggende betalingstjenester skal gjennomføre effektive prosedyrer, herunder overvåking etter eller under overføringene, der det er relevant, for å avdekke om følgende opplysninger om betaleren eller betalingsmottakeren mangler:
   a) For pengeoverføringer der betalerens og betalingsmottakerens betalingstjenesteyter er etablert i Unionen, opplysningene nevnt i artikkel 5.
   b) For pengeoverføringer der betalerens eller betalingsmottakerens betalingstjenesteyter er etablert utenfor Unionen, opplysningene nevnt i artikkel 4 nr. 1 bokstav a), b) og c) og artikkel 4 nr. 2 bokstav a) og b).
   c) For samleoverføringer der betalerens eller betalingsmottakerens betalingstjenesteyter er etablert utenfor Unionen, opplysningene nevnt i artikkel 4 nr. 1 bokstav a), b) og c) og artikkel 4 nr. 2 bokstav a) og b) for den aktuelle samleoverføringen.

Artikkel 12

Pengeoverføringer med manglende opplysninger om betaleren eller betalingsmottakeren

1. Yteren av mellomliggende betalingstjenester skal utarbeide effektive risikobaserte prosedyrer for å avgjøre om en pengeoverføring som mangler de påkrevde opplysningene om betaleren eller betalingsmottakeren, skal utføres, avvises eller innstilles, og for å treffe hensiktsmessige oppfølgingstiltak.

   Dersom yteren av mellomliggende betalingstjenester ved mottak av pengeoverføringer får kjennskap til at opplysningene nevnt i artikkel 4 nr. 1 bokstav a), b) og c), artikkel 4 nr. 2 bokstav a) og b), artikkel 5 nr. 1 eller artikkel 6 mangler eller ikke er fylt ut med tillatte tegn eller inndata i henhold til reglene for meldingssystemet eller betalings- og opp-

gjørssystemet som nevnt i artikkel 7 nr. 1, skal yteren av mellomliggende betalingstjenester på grunnlag av en risikovurdering

a) avvise overføringen eller
b) be om de påkrevde opplysningene om betaleren og betalingsmottakeren før eller etter pengeoverføringen.

2. Dersom en betalingstjenesteyter gjentatte ganger unnlater å gi de påkrevde opplysningene om betaleren eller betalingsmottakeren, skal yteren av mellomliggende betalingstjenester

a) treffe tiltak, som i første omgang kan omfatte utsending av advarsler og fastsettelse av frister, før den går videre med en avvisning, begrensning eller avslutning i samsvar med bokstav b) dersom de påkrevde opplysningene fortsatt ikke er gitt, eller
b) direkte avvise enhver framtidig pengeoverføring fra denne betalingstjenesteyteren eller begrense eller avslutte forretningsforbindelsen med denne betalingstjenesteyteren.

Yteren av mellomliggende betalingstjenester skal rapportere forholdet og redegjøre for de tiltakene som er truffet, til vedkommende myndighet som har ansvar for å føre tilsyn med at bestemmelsene som gjelder bekjempelse av hvitvasking av penger og finansiering av terrorisme, blir overholdt.

Artikkel 13

Vurdering og rapportering

Yteren av mellomliggende betalingstjenester skal anse manglende opplysninger om betaleren eller betalingsmottakeren som en faktor i vurderingen av om en pengeoverføring eller en tilknyttet transaksjon er mistenkelig, og om den skal rapporteres til enheten for finansiell etterretning i samsvar med direktiv (EU) 2015/849.

Kapittel III

Plikter for ytere av kryptoeiendelstjenester

Avsnitt 1

Plikter for avsenderens yter av kryptoeiendelstjenester

Artikkel 14

Opplysninger som skal følge overføringer av kryptoeiendeler

1. Avsenderens yter av kryptoeiendelstjenester skal sikre at overføringer av kryptoeiendeler følges av følgende opplysninger om avsenderen:

a) Avsenderens navn.
b) Avsenderens desentralisert registeradresse i tilfeller der en overføring av kryptoeiendeler registreres i et nettverk som bruker DLT eller lignende teknologi, og avsenderens kryptoeiendelskontonummer dersom en slik konto finnes og benyttes for å behandle transaksjonen.
c) Avsenderens kryptoeiendelskontonummer i tilfeller der en overføring av kryptoeiendeler ikke registreres i et nettverk som bruker DLT eller lignende teknologi.
d) Avsenderens adresse, herunder landets navn, offisielt personlig dokumentnummer og kundeidentifikasjonsnummer eller alternativt avsenderens fødselsdato og -sted.
e) Avsenderens aktuelle LEI-kode eller, dersom en slik kode ikke finnes, enhver tilgjengelig tilsvarende offisiell identifikator, forutsatt at det nødvendige feltet i det relevante meldingsformatet finnes, og at avsenderen har opplyst sin yter av kryptoeiendelstjenester om den.

2. Avsenderens yter av kryptoeiendelstjenester skal sikre at overføringer av kryptoeiendeler følges av følgende opplysninger om mottakeren:

a) Mottakerens navn.
b) Mottakerens desentralisert registeradresse i tilfeller der en overføring av kryptoeiendeler registreres i et nettverk som bruker DLT eller lignende teknologi, og mottakerens kryptoeiendelskontonummer dersom en slik konto finnes og benyttes for å behandle transaksjonen.
c) Mottakerens kryptoeiendelskontonummer i tilfeller der en overføring av kryptoeiendeler ikke registreres i et nettverk som bruker DLT eller lignende teknologi.
d) Mottakerens aktuelle LEI-kode eller, dersom en slik kode ikke finnes, enhver annen tilgjengelig tilsvarende offisiell identifikator for mottakeren, forutsatt at det nødvendige feltet i det relevante meldingsformatet finnes, og at avsenderen har opplyst sin yter av kryptoeiendelstjenester om den.

3. Som unntak fra nr. 1 bokstav c) og nr. 2 bokstav c) skal avsenderens yter av kryptoeiendelstjenester sikre at overføringer av kryptoeiendeler som ikke registreres i et nettverk som bruker DLT eller lignende teknologi, og som ikke er foretatt til eller fra en kryptoeien-

delskonto, følges av en entydig transaksjonsidentifikator.

4. Opplysningene nevnt i nr. 1 og 2 skal oversendes før eller samtidig eller parallelt med overføringen av kryptoeiendeler, på en sikker måte og i samsvar med forordning (EU) 2016/679.

   Det skal ikke kreves at opplysningene nevnt i nr. 1 og 2 må knyttes direkte til eller inngå i overføringen av kryptoeiendeler.
5. Ved en overføring av kryptoeiendeler til en frittstående adresse skal avsenderens yter av kryptoeiendelstjenester innhente og oppbevare opplysningene nevnt i nr. 1 og 2 og sikre at overføringen av kryptoeiendeler kan identifiseres individuelt.

   Uten at det berører spesifikke risikoreduserende tiltak truffet i samsvar med artikkel 19b i direktiv (EU) 2015/849, skal avsenderens yter av kryptoeiendelstjenester ved en overføring av et beløp som overstiger 1 000 euro, til en frittstående adresse, treffe hensiktsmessige tiltak for å vurdere om denne adressen eies eller kontrolleres av avsenderen.
6. Før kryptoeiendelene overføres, skal avsenderens yter av kryptoeiendelstjenester kontrollere, på grunnlag av dokumenter, data eller opplysninger innhentet fra en pålitelig og uavhengig kilde, at opplysningene nevnt i nr. 1 er korrekte.
7. Kontrollen omhandlet i nr. 6 i denne artikkelen skal anses å ha blitt utført dersom et av følgende forhold gjør seg gjeldende:
   a) Avsenderens identitet er kontrollert i samsvar med artikkel 13 i direktiv (EU) 2015/849 og opplysningene innhentet ved kontrollen er oppbevart i samsvar med artikkel 40 i nevnte direktiv.
   b) Avsenderen er omfattet av artikkel 14 nr. 5 i direktiv (EU) 2015/849.
8. Avsenderens yter av kryptoeiendelstjenester skal ikke tillate at en overføring av kryptoeiendeler innledes eller gjennomføres før den har forsikret seg om at alle krav i denne artikkelen er oppfylt.

Artikkel 15

Samleoverføringer av kryptoeiendeler

Ved samleoverføringer av kryptoeiendeler fra en enkelt avsender får artikkel 14 nr. 1 ikke anvendelse på de enkelte overføringene som er samlet, forutsatt at samlefilen inneholder de opplysningene som er nevnt i artikkel 14 nr. 1, 2 og 3, at opplysningene er kontrollert i samsvar med artikkel 14 nr. 6 og 7, og at de enkelte overføringene inneholder avsenderens desentralisert registeradresse dersom artikkel 14 nr. 2 bokstav b) får anvendelse, avsenderens kryptoeiendelskontonummer dersom artikkel 14 nr. 2 bokstav c) får anvendelse, eller den entydige transaksjonsidentifikatoren dersom artikkel 14 nr. 3 får anvendelse.

Avsnitt 2

Plikter for mottakerens yter av kryptoeiendelstjenester

Artikkel 16

Avdekking av manglende opplysninger om avsenderen eller mottakeren

1. Mottakerens yter av kryptoeiendelstjenester skal innføre effektive prosedyrer, herunder overvåking etter eller under overføringene, der det er relevant, for å avdekke om opplysningene om avsenderen og mottakeren som er nevnt i artikkel 14 nr. 1 og 2, inngår i eller følger etter overføringen eller samleoverføringen av kryptoeiendeler.
2. Ved en overføring av kryptoeiendeler fra en frittstående adresse skal mottakerens yter av kryptoeiendelstjenester innhente og oppbevare opplysningene som er nevnt i artikkel 14 nr. 1 og 2, og sikre at overføringen av kryptoeiendeler kan identifiseres individuelt.

   Uten at det berører spesifikke risikoreduserende tiltak truffet i samsvar med artikkel 19b i direktiv (EU) 2015/849, skal mottakerens yter av kryptoeiendelstjenester ved en overføring av et beløp som overstiger 1 000 euro, fra en frittstående adresse, treffe hensiktsmessige tiltak for å vurdere om denne adressen eies eller kontrolleres av mottakeren.
3. Før kryptoeiendelene gjøres tilgjengelige for mottakeren, skal mottakerens yter av kryptoeiendelstjenester kontrollere, på grunnlag av dokumenter, data eller opplysninger innhentet fra en pålitelig og uavhengig kilde, at de opplysningene om mottakeren som er nevnt i artikkel 14 nr. 2, er korrekte.
4. Kontrollen nevnt i nr. 2 og 3 i denne artikkelen skal anses å ha blitt utført dersom et av følgende forhold gjør seg gjeldende:
   a) Mottakerens identitet er kontrollert i samsvar med artikkel 13 i direktiv (EU) 2015/849 og opplysningene innhentet ved kontrollen er oppbevart i samsvar med artikkel 40 i nevnte direktiv.
   b) Mottakeren er omfattet av artikkel 14 nr. 5 i direktiv (EU) 2015/849.

Artikkel 17

Overføringer av kryptoeiendeler med manglende eller ufullstendige opplysninger om avsenderen eller mottakeren

1. Mottakerens yter av kryptoeiendelstjenester skal gjennomføre effektive risikobaserte prosedyrer, herunder prosedyrer som bygger på risikovurderingen nevnt i artikkel 13 i direktiv (EU) 2015/849, for å avgjøre om en overføring av kryptoeiendeler som mangler fullstendige opplysninger om avsenderen eller mottakeren, skal utføres, avvises, returneres eller innstilles, og for å treffe hensiktsmessige oppfølgingstiltak.

   Dersom mottakerens yter av kryptoeiendelstjenester får kjennskap til at opplysningene nevnt i artikkel 14 nr. 1 eller 2 eller i artikkel 15 mangler eller er ufullstendige, skal denne yteren av kryptoeiendelstjenester på grunnlag av en risikovurdering og uten unødig opphold
   a) avvise overføringen eller sende de overførte kryptoeiendelene tilbake til avsenderens kryptoeiendelskonto, eller
   b) be om de påkrevde opplysningene om avsenderen og mottakeren før kryptoeiendelene gjøres tilgjengelig for mottakeren.
2. Dersom en yter av kryptoeiendelstjenester gjentatte ganger unnlater å gi de påkrevde opplysningene om avsenderen eller mottakeren, skal mottakerens yter av kryptoeiendelstjenester
   a) treffe tiltak, som i første omgang kan omfatte utsending av advarsler og fastsettelse av frister, før den går videre med en avvisning, begrensning eller avslutning i samsvar med bokstav b) dersom de påkrevde opplysningene fortsatt ikke er gitt, eller
   b) direkte avvise enhver framtidig overføring av kryptoeiendeler til eller fra, eller begrense eller avslutte forretningsforbindelsen med, denne yteren av kryptoeiendelstjenester.

   Mottakerens yter av kryptoeiendelstjenester skal rapportere forholdet og redegjøre for de tiltakene som er truffet, til vedkommende myndighet som har ansvar for å føre tilsyn med at bestemmelsene som gjelder bekjempelse av hvitvasking av penger og finansiering av terrorisme, blir overholdt.

Artikkel 18

Vurdering og rapportering

Mottakerens yter av kryptoeiendelstjenester skal anse manglende eller ufullstendige opplysninger om avsenderen eller mottakeren som en faktor i vurderingen av om en overføring av kryptoeiendeler eller en tilknyttet transaksjon er mistenkelig, og om den skal rapporteres til enheten for finansiell etterretning i samsvar med direktiv (EU) 2015/849.

Avsnitt 3

Plikter for ytere av mellomliggende kryptoeiendelstjenester

Artikkel 19

Oppbevaring av opplysninger om avsenderen og mottakeren som følger overføringen

Ytere av mellomliggende kryptoeiendelstjenester skal sikre at alle mottatte opplysninger om avsenderen og mottakeren som følger en overføring av kryptoeiendeler, overføres sammen med overføringen, og at registreringer av slike opplysninger oppbevares og på anmodning gjøres tilgjengelig for vedkommende myndigheter.

Artikkel 20

Avdekking av manglende opplysninger om avsenderen eller mottakeren

Yteren av mellomliggende kryptoeiendelstjenester skal innføre effektive prosedyrer, herunder overvåking etter eller under overføringene, der det er relevant, for å avdekke om de opplysningene om avsenderen eller mottakeren som er nevnt i artikkel 14 nr. 1 bokstav a), b) og c) og artikkel 14 nr. 2 bokstav a), b) og c), er oversendt før eller samtidig med eller parallelt med overføringen eller samleoverføringen av kryptoeiendeler, også når overføringen foretas til eller fra en frittstående adresse.

Artikkel 21

Overføringer av kryptoeiendeler med manglende opplysninger om avsenderen eller mottakeren

1. Yteren av mellomliggende kryptoeiendelstjenester skal innføre effektive risikobaserte prosedyrer, herunder prosedyrer som bygger på risikovurderingen nevnt i artikkel 13 i direktiv (EU) 2015/849, for å avgjøre om en overføring av kryptoeiendeler som mangler de

påkrevde opplysningene om avsenderen eller mottakeren, skal utføres, avvises, returneres eller innstilles, og for å treffe hensiktsmessige oppfølgingstiltak.

Dersom en yter av mellomliggende kryptoeiendelstjenester når den mottar en overføring av kryptoeiendeler, får kjennskap til at opplysningene nevnt i artikkel 14 nr. 1 bokstav a), b) og c) og artikkel 14 nr. 2 bokstav a), b) og c) eller artikkel 15 nr. 1 mangler eller er ufullstendige, skal denne yteren av mellomliggende kryptoeiendelstjenester på grunnlag av en risikovurdering og uten unødig opphold

a) avvise overføringen eller returnere de overførte kryptoeiendelene, eller
b) be om de påkrevde opplysningene om avsenderen og mottakeren før kryptoeiendelene overføres.

2. Dersom en yter av kryptoeiendelstjenester gjentatte ganger unnlater å gi de påkrevde opplysningene om avsenderen eller mottakeren, skal yteren av mellomliggende kryptoeiendelstjenester
   a) treffe tiltak, som i første omgang kan omfatte utsending av advarsler og fastsettelse av frister, før den går videre med en avvisning, begrensning eller avslutning i samsvar med bokstav b) dersom de påkrevde opplysningene fortsatt ikke er gitt, eller
   b) direkte avvise enhver framtidig overføring av kryptoeiendeler til eller fra, eller begrense eller avslutte forretningsforbindelsen med, denne yteren av kryptoeiendelstjenester.

   Yteren av mellomliggende kryptoeiendelstjenester skal rapportere forholdet og redegjøre for de tiltakene som er truffet, til vedkommende myndighet som har ansvar for å føre tilsyn med at bestemmelsene som gjelder bekjempelse av hvitvasking av penger og finansiering av terrorisme, blir overholdt.

Artikkel 22

Vurdering og rapportering

Yteren av mellomliggende kryptoeiendelstjenester skal anse manglende opplysninger om avsenderen eller mottakeren som en faktor i vurderingen av om en overføring av kryptoeiendeler eller en tilknyttet transaksjon er mistenkelig, og om den skal rapporteres til enheten for finansiell etterretning i samsvar med direktiv (EU) 2015/849.

Kapittel IV

Felles tiltak som skal anvendes av betalingstjenesteytere og ytere av kryptoeiendelstjenester

Artikkel 23

Interne retningslinjer, prosedyrer og kontroller for å sikre gjennomføringen av restriktive tiltak

Betalingstjenesteytere og ytere av kryptoeiendelstjenester skal ha innført interne retningslinjer, prosedyrer og kontroller for å sikre gjennomføringen av restriktive tiltak på unionsplan og nasjonalt plan i forbindelse med pengeoverføringer og overføring av kryptoeiendeler i henhold til denne forordningen.

Den europeiske banktilsynsmyndighet (EBA) skal innen 30. desember 2024 utstede retningslinjer som spesifiserer tiltakene omhandlet i denne artikkelen.

Kapittel V

Opplysninger, vern av personopplysninger og oppbevaring av opplysninger

Artikkel 24

Framlegging av opplysninger

Betalingstjenesteytere og ytere av kryptoeiendelstjenester skal i samsvar med prosedyrene i nasjonal rett i medlemsstaten der de er etablert eller har sitt forretningskontor, alt etter hva som er relevant, straks gi utfyllende svar på anmodninger fra utelukkende de myndighetene som har ansvar for å bekjempe hvitvasking av penger eller finansiering av terrorisme i den berørte medlemsstaten, med hensyn til opplysningene som kreves i henhold til denne forordningen, herunder gjennom et sentralt kontaktpunkt i samsvar med artikkel 45 nr. 9 i direktiv (EU) 2015/849, dersom et slikt kontaktpunkt er utpekt.

Artikkel 25

Vern av personopplysninger

1. Behandling av personopplysninger i henhold til denne forordningen omfattes også av forordning (EU) 2016/679. Personopplysninger som behandles i henhold til denne forordningen av Kommisjonen eller EBA, omfattes også av forordning (EU) 2018/1725.
2. Personopplysninger skal behandles av betalingstjenesteytere og ytere av kryptoeiendelstjenester på grunnlag av denne forordningen utelukkende med sikte på å forebygge hvit-

vasking av penger og finansiering av terrorisme og skal ikke viderebehandles på en måte som er uforenlig med disse formålene. Behandling av personopplysninger på grunnlag av denne forordningen for kommersielle formål skal være forbudt.

3. Betalingstjenesteytere og ytere av kryptoeiendelstjenester skal gi nye kunder de opplysningene som kreves i henhold til artikkel 13 i forordning (EU) 2016/679, før de oppretter en forretningsforbindelse eller utfører en enkeltstående transaksjon. Disse opplysningene skal framlegges på en kortfattet, åpen, forståelig og lett tilgjengelig måte i samsvar med artikkel 12 i forordning (EU) 2016/679 og skal særlig omfatte en generell melding om de juridiske forpliktelsene som betalingstjenesteytere og ytere av kryptoeiendelstjenester har i henhold til denne forordningen, når de behandler personopplysninger med sikte på å forebygge hvitvasking av penger og finansiering av terrorisme.
4. Betalingstjenesteytere og ytere av kryptoeiendelstjenester skal til enhver tid sikre at personopplysninger om de partene som er involvert i en pengeoverføring eller en overføring av kryptoeiendeler, formidles i samsvar med forordning (EU) 2016/679.

Det europeiske personvernråd skal etter samråd med EBA utstede retningslinjer for den praktiske gjennomføringen av personvernkravene for overføring av personopplysninger til tredjeland i forbindelse med overføringer av kryptoeiendeler. EBA skal utstede retningslinjer for egnede prosedyrer for å avgjøre om en overføring av kryptoeiendeler skal gjennomføres, avvises, returneres eller innstilles i situasjoner der det ikke kan sikres at personvernkravene for overføringen av personopplysninger til tredjeland overholdes.

Artikkel 26

Oppbevaring av opplysninger

1. Opplysningene om betaleren og betalingsmottakeren eller om avsenderen og mottakeren skal ikke oppbevares lenger enn det som er strengt nødvendig. Betalerens og betalingsmottakerens betalingstjenesteytere skal oppbevare opplysningene nevnt i artikkel 4–7, og avsenderens og mottakerens yter av kryptoeiendelstjenester skal oppbevare opplysningene nevnt i artikkel 14–16, i en periode på fem år.
2. Ved utløpet av oppbevaringstiden nevnt i nr. 1 skal betalingstjenesteyterne og yterne av kryptoeiendelstjenester sikre at personopplysningene slettes, med mindre noe annet er fastsatt i nasjonal rett, som avgjør under hvilke omstendigheter betalingstjenesteyterne og yterne av kryptoeiendelstjenester deretter kan eller skal oppbevare slike opplysninger. Medlemsstatene kan tillate eller kreve oppbevaring i lengre tid først etter at de har foretatt en grundig vurdering av om slik videre oppbevaring er nødvendig og forholdsmessig, og forutsatt at de anser at dette er nødvendig for å kunne forebygge, avdekke eller etterforske hvitvasking av penger eller finansiering av terrorisme. Oppbevaringstiden skal ikke forlenges med mer enn fem år.
3. Dersom det per 25. juni 2015 pågår rettergang i en medlemsstat som gjelder forebygging eller avdekking av antatte tilfeller av hvitvasking av penger eller finansiering av terrorisme eller etterforsknings- eller påtalemessige skritt i den anledning, og en betalingstjenesteyter har opplysninger eller dokumenter som gjelder den aktuelle saken, kan betalingstjenesteyteren oppbevare disse opplysningene eller dokumentene i samsvar med nasjonal rett i fem år fra og med 25. juni 2015. Medlemsstatene kan, uten at det berører nasjonal strafferett om bevis som får anvendelse i pågående etterforskning i straffesaker og rettergang, tillate eller kreve at slike opplysninger eller dokumenter oppbevares i ytterligere fem år dersom det er godtgjort at fortsatt oppbevaring er et nødvendig og forholdsmessig tiltak for å kunne forebygge eller avdekke antatte tilfeller av hvitvasking av penger eller finansiering av terrorisme eller foreta etterforsknings- eller påtalemessige skritt i den anledning.

Artikkel 27

Samarbeid mellom vedkommende myndigheter

Utveksling av opplysninger mellom vedkommende myndigheter og med relevante tredjelandsmyndigheter i henhold til denne forordningen skal omfattes av direktiv (EU) 2015/849.

Kapittel VI

Sanksjoner og overvåking

Artikkel 28

Administrative sanksjoner og tiltak

1. Uten at det berører retten til å fastsette og ilegge strafferettslige sanksjoner, skal med-

lemsstatene fastsette regler for administrative sanksjoner og tiltak som kan anvendes ved overtredelse av bestemmelsene i denne forordningen, og treffe alle nødvendige tiltak for å sikre at de gjennomføres. Sanksjonene og tiltakene skal være effektive og forholdsmessige, virke avskrekkende og være i samsvar med dem som er fastsatt i samsvar med kapittel VI avsnitt 4 i direktiv (EU) 2015/849.

Medlemsstatene kan vedta at de ikke skal fastsette regler for administrative sanksjoner eller tiltak ved overtredelse av bestemmelsene i denne forordningen som omfattes av strafferettslige sanksjoner i henhold til deres nasjonale rett. I så fall skal medlemsstatene underrette Kommisjonen om de relevante strafferettslige bestemmelsene.

2. Medlemsstatene skal sikre at de ved overtredelse av bestemmelsene i denne forordningen, i tilfeller der betalingstjenesteyterne og yterne av kryptoeiendelstjenester er pålagt plikter, har sanksjoner eller tiltak som kan anvendes, med forbehold for nasjonal rett, på medlemmene av ledelsesorganet til den berørte tjenesteyteren og på enhver annen fysisk person som i henhold til nasjonal rett har ansvar for overtredelsen.
3. Medlemsstatene skal underrette Kommisjonen og den faste interne komiteen for bekjempelse av hvitvasking av penger og finansiering av terrorisme som er omhandlet i artikkel 9a nr. 7 i forordning (EU) nr. 1093/2010, om reglene omhandlet i nr. 1. Medlemsstatene skal uten unødig opphold underrette Kommisjonen og den faste interne komiteen om eventuelle senere endringer av dem.
4. I samsvar med artikkel 58 nr. 4 i direktiv (EU) 2015/849 skal vedkommende myndigheter gis den tilsyns- og granskingsmyndigheten de trenger for å kunne utføre sine oppgaver. Vedkommende myndigheter skal under utøvelsen av sin myndighet til å ilegge administrative sanksjoner og iverksette administrative tiltak ha et nært samarbeid for å sikre at administrative sanksjoner eller tiltak gir de ønskede virkningene, og de skal samordne sine handlinger i forbindelse med tverrnasjonale saker.
5. Medlemsstatene skal sikre at juridiske personer kan holdes ansvarlige for overtredelsene nevnt i artikkel 29 som er begått til deres fordel av en person som handler alene eller som del av et organ under den juridiske personen, og som har en ledende stilling hos den juridiske personen, basert på
   a) fullmakt til å representere den juridiske personen,
   b) myndighet til å treffe beslutninger på vegne av den juridiske personen eller
   c) myndighet til å utøve kontroll innenfor den juridiske personen.
6. Medlemsstatene skal også sørge for at juridiske personer kan holdes ansvarlige dersom manglende tilsyn eller kontroll fra en person som nevnt i nr. 5 i denne artikkelen har gjort det mulig for en person under den juridiske personens myndighet å begå en av overtredelsene nevnt i artikkel 29 til fordel for den juridiske personen.
7. Vedkommende myndigheter skal utøve sin myndighet til å ilegge administrative sanksjoner og iverksette administrative tiltak i samsvar med denne forordningen på en av følgende måter:
   a) Direkte.
   b) I samarbeid med andre myndigheter.
   c) På eget ansvar ved delegering til slike andre myndigheter.
   d) Etter søknad til vedkommende rettsmyndigheter.

   Vedkommende myndigheter skal under utøvelsen av sin myndighet til å ilegge administrative sanksjoner og iverksette administrative tiltak ha et nært samarbeid for å sikre at administrative sanksjoner eller tiltak gir de ønskede virkningene, og de skal samordne sine handlinger i forbindelse med tverrnasjonale saker.

Artikkel 29

Særlige bestemmelser

Medlemsstatene skal sikre at deres administrative sanksjoner og tiltak minst omfatter de som er fastsatt i artikkel 59 nr. 2 og 3 i direktiv (EU) 2015/849, ved følgende overtredelser av denne forordningen:

a) Gjentatt eller systematisk unnlatelse fra en betalingstjenesteyter med hensyn til å ta med de påkrevde opplysningene om betaleren eller betalingsmottakeren, i strid med artikkel 4, 5 eller 6, eller gjentatt eller systematisk unnlatelse fra en yter av kryptoeiendelstjenester med hensyn til å ta med de påkrevde opplysningene om avsenderen og mottakeren ved overføring av kryptoeiendeler, i strid med artikkel 14 eller 15
b) Gjentatt, systematisk eller alvorlig unnlatelse fra en betalingstjenesteyter eller fra en yter av kryptoeiendelstjenester med hensyn til å oppbevare opplysninger, i strid med artikkel 26.

c) En betalingstjenesteyters manglende innføring av effektive risikobaserte prosedyrer, i strid med artikkel 8 eller 12, eller manglende innføring av effektive risikobaserte prosedyrer når det gjelder en yter av kryptoeiendelstjenester, i strid med artikkel 17.
d) Alvorlig unnlatelse fra en yter av mellomliggende betalingstjenester med hensyn til å overholde artikkel 11 eller 12 eller fra en yter av mellomliggende kryptoeiendelstjenester med hensyn til å overholde artikkel 19, 20 eller 21.

Artikkel 30

Offentliggjøring av sanksjoner og tiltak

I samsvar med artikkel 60 nr. 1, 2 og 3 i direktiv (EU) 2015/849 skal vedkommende myndigheter uten unødig opphold offentliggjøre ilagte administrative sanksjoner og tiltak som er iverksatt i tilfellene nevnt i artikkel 28 og 29 i denne forordningen, herunder opplysninger om overtredelsens type og art og identiteten til de personene som har ansvaret for den, dersom dette etter en vurdering i hvert enkelt tilfelle er nødvendig og forholdsmessig.

Artikkel 31

Vedkommende myndigheters anvendelse av sanksjoner og tiltak

1. Når vedkommende myndigheter fastsetter hvilken type administrative sanksjoner eller tiltak som skal anvendes, og størrelsen på administrative økonomiske sanksjoner, skal de ta hensyn til alle relevante omstendigheter, herunder omstendighetene angitt i artikkel 60 nr. 4 i direktiv (EU) 2015/849.
2. Når det gjelder ilagte administrative sanksjoner og tiltak som er iverksatt i samsvar med denne forordningen, får artikkel 62 i direktiv (EU) 2015/849 anvendelse.

Artikkel 32

Rapportering av overtredelser

1. Medlemsstatene skal innføre effektive ordninger som oppmuntrer til rapportering til vedkommende myndigheter av overtredelser av denne forordningen.

   Ordningene skal omfatte minst det som er nevnt i artikkel 61 nr. 2 i direktiv (EU) 2015/849.
2. Betalingstjenesteytere og ytere av kryptoeiendelstjenester skal i samarbeid med vedkommende myndigheter fastsette hensiktsmessige interne prosedyrer slik at deres ansatte eller personer i tilsvarende stilling skal kunne rapportere internt om overtredelser gjennom en sikker, uavhengig og anonym kanal, der prosedyrene står i forhold til den berørte betalingstjenesteyterens eller yteren av kryptoeiendelstjenesters art og størrelse.

Artikkel 33

Overvåking

1. Medlemsstatene skal kreve at vedkommende myndigheter effektivt overvåker og treffer de nødvendige tiltakene for å sikre at denne forordningen overholdes, og gjennom effektive ordninger oppmuntrer til rapportering til vedkommende myndigheter av overtredelser av bestemmelsene i denne forordningen.
2. Kommisjonen skal innen 31. desember 2026 og deretter hvert tredje år legge fram en rapport for Europaparlamentet og Rådet om anvendelsen av kapittel VI, særlig med hensyn til tverrnasjonale saker.

Kapittel VII

Gjennomføringsmyndighet

Artikkel 34

Komitéprosedyre

1. Kommisjonen skal bistås av Komiteen for forebygging av hvitvasking av penger og finansiering av terrorisme. Nevnte komité skal være en komité i henhold til forordning (EU) nr. 182/2011.
2. Når det vises til dette nummeret, får artikkel 5 i forordning (EU) nr. 182/2011 anvendelse.

Kapittel VIII

Unntak

Artikkel 35

Avtaler med land og territorier som ikke utgjør en del av Unionens territorium

1. Kommisjonen kan bemyndige enhver medlemsstat til å inngå en avtale med et tredjeland eller et territorium som ligger utenfor det geografiske virkeområdet for traktaten om Den europeiske union og traktaten om Den europeiske unions virkemåte (TEUV) som nevnt i artikkel 355 i TEUV (heretter kalt «vedkommende land eller territorium»), som inne-

holder unntak fra denne forordningen, for å gjøre det mulig å behandle pengeoverføringer mellom nevnte land eller territorium og den berørte medlemsstaten som pengeoverføringer innenfor medlemsstaten.

Slike avtaler kan tillates bare dersom samtlige av følgende vilkår er oppfylt:

a) Vedkommende land eller territorium er i monetær union med den berørte medlemsstaten, utgjør en del av medlemsstatens valutaområde eller har undertegnet en monetær avtale med Unionen representert ved en medlemsstat.
b) Ytere av betalingstjenester i det berørte landet eller territoriet deltar direkte eller indirekte i betalings- og oppgjørssystemer i medlemsstaten.
c) Vedkommende land eller territorium krever at betalingstjenesteytere under dets jurisdiksjon anvender de samme reglene som dem fastsatt i denne forordningen.

2. En medlemsstat som ønsker å inngå en avtale som nevnt i nr. 1, skal sende en anmodning til Kommisjonen og oppgi alle opplysninger som er nødvendige for at anmodningen skal kunne vurderes.
3. Når Kommisjonen mottar en slik anmodning, skal pengeoverføringer mellom medlemsstaten og vedkommende land eller territorium midlertidig behandles som overføringer innenfor medlemsstaten, inntil det treffes en beslutning i samsvar med denne artikkelen.
4. Dersom Kommisjonen innen to måneder etter at anmodningen er mottatt, anser at den ikke har alle opplysninger som er nødvendige for å vurdere anmodningen, skal den ta kontakt med den berørte medlemsstaten og oppgi hvilke tilleggsopplysninger som kreves.
5. Innen én måned etter at Kommisjonen har mottatt alle de opplysningene den anser som nødvendige for å vurdere anmodningen, skal den underrette den anmodende medlemsstaten om dette og oversende kopi av anmodningen til de andre medlemsstatene.
6. Kommisjonen skal innen tre måneder etter underretningen nevnt i nr. 5 i denne artikkelen treffe beslutning i samsvar med artikkel 34 nr. 2 om hvorvidt den berørte medlemsstaten skal få tillatelse til å inngå avtalen som anmodningen gjaldt.

Kommisjonen skal under alle omstendigheter vedta en beslutning som nevnt i første ledd i dette nummeret innen 18 måneder etter at anmodningen er mottatt.

Kapittel IX

Andre bestemmelser

Artikkel 36

Retningslinjer

EBA skal utstede retningslinjer til vedkommende myndigheter og betalingstjenesteyterne i samsvar med artikkel 16 i forordning (EU) nr. 1093/2010, om tiltak som skal treffes i samsvar med denne forordningen, særlig når det gjelder gjennomføringen av artikkel 7, 8, 11 og 12 i denne forordningen. EBA skal innen 30. juni 2024 utstede retningslinjer til vedkommende myndigheter og til yterne av kryptoeiendelstjenester om tiltak som skal treffes med hensyn til gjennomføringen av artikkel 14–17 og 19–22 i denne forordningen.

EBA skal utstede retningslinjer som spesifiserer de tekniske aspektene ved anvendelsen av denne forordningen på direkte debiteringer samt de tiltakene som skal treffes av ytere av betalingsinitieringstjenester som definert i artikkel 4 nr. 18 i direktiv (EU) 2015/2366 i henhold til denne forordningen, idet det tas hensyn til deres begrensede rolle i betalingstransaksjoner.

EBA skal utstede retningslinjer til vedkommende myndigheter om særtrekkene ved en risikobasert tilsynsmetode i forbindelse med ytere av kryptoeiendelstjenester og de tiltakene som skal treffes ved gjennomføring av slikt tilsyn.

EBA skal sikre en regelmessig dialog med berørte parter om utviklingen av tekniske interoperabile løsninger med sikte på å lette gjennomføringen av kravene i denne forordningen.

Artikkel 37

Gjennomgåelse

1. Innen tolv måneder etter ikrafttredelsen av en forordning om tiltak for å hindre at finanssystemet brukes til hvitvasking av penger og finansiering av terrorisme skal Kommisjonen revidere denne forordningen og, dersom det er hensiktsmessig, foreslå endringer for å sikre en konsekvent tilnærming og tilpasning til forordningen om tiltak for å hindre at finanssystemet brukes til hvitvasking av penger og finansiering av terrorisme.
2. Innen 1. juli 2026 skal Kommisjonen etter samråd med EBA legge fram en rapport med en vurdering av de risikoene som er knyttet til overføringer til eller fra frittstående adresser eller enheter som ikke er etablert i Unionen, og behovet for spesifikke tiltak for å redusere disse risikoene og, dersom det er hensikts-

messig, foreslå endringer av denne forordningen.

3. Innen 30. juni 2027 skal Kommisjonen legge fram for Europaparlamentet og Rådet en rapport om anvendelsen og håndhevingen av denne forordningen, eventuelt sammen med et forslag til regelverk.

Rapporten nevnt i første ledd skal omfatte følgende:

a) En vurdering av hvor effektive tiltakene fastsatt i denne forordningen er, og av hvordan betalingstjenesteytere og ytere av kryptoeiendelstjenester overholder denne forordningen.

b) En vurdering av de teknologiske løsningene for å oppfylle de forpliktelsene som pålegges ytere av kryptoeiendelstjenester i henhold til denne forordningen, herunder vurdering av den seneste utviklingen innenfor teknologisk forsvarlige og interoperabile løsninger for å overholde denne forordningen, og av anvendelsen av analyseverktøy for DLT for å fastslå opprinnelsen til og bestemmelsesstedet for overføringer av kryptoeiendeler og for å foreta en vurdering av transaksjonskjennskap («kjenn din transaksjon» – KYT).

c) En vurdering av hvor effektive og egnede minimumsterskler for pengeoverføringer er, særlig med hensyn til anvendelsesområdet og det settet av opplysninger som skal følge med overføringer, og en vurdering av behovet for å senke eller fjerne slike terskler.

d) En vurdering av kostnader og fordeler ved å innføre minimumsterskler knyttet til det settet av opplysninger som følger med overføringer av kryptoeiendeler, herunder en vurdering av de tilknyttede risikoene for hvitvasking av penger og finansiering av terrorisme.

e) En analyse av tendensene i bruken av frittstående adresser for å utføre overføringer uten å involvere en tredjepart, sammen med en vurdering av de tilknyttede risikoene for hvitvasking av penger og finansiering av terrorisme og en evaluering av behovet for og effektiviteten og håndhevingen av ytterligere risikoreduserende tiltak, for eksempel spesifikke forpliktelser for leverandører av maskinvare- og programvarelommebøker og begrensning og kontroll av eller forbud mot overføringer som involverer frittstående adresser.

Rapporten skal ta hensyn til ny utvikling på området for bekjempelse av hvitvasking av penger og finansiering av terrorisme, og til relevante evalueringer, vurderinger og rapporter på dette området som er utarbeidet av internasjonale organisasjoner og standardiseringsorganer, rettshåndhevende myndigheter og etterretningstjenester, ytere av kryptoeiendelstjenester eller andre pålitelige kilder.

Kapittel X

Sluttbestemmelser

Artikkel 38

Endring av direktiv (EU) 2015/849

I direktiv (EU) 2015/849 gjøres følgende endringer:

1) Artikkel 2 nr. 1 punkt 3 bokstav g) og h) utgår.

2) I artikkel 3 gjøres følgende endringer:

a) I nr. 2 skal ny bokstav lyde:

«g) ytere av kryptoeiendelstjenester,».

b) Nr. 8 skal lyde:

«8) «korrespondentforbindelse»

a) yting av banktjenester fra en bank som korrespondentbank til en annen bank som respondentbank, herunder opprettelse av en foliokonto eller annen passivakonto med tilknyttede tjenester, som likviditetsstyring, internasjonale overføringer av midler, sjekkavregning, gjennomstrømningskontoer og valutatjenester,

b) forbindelsene mellom kredittinstitusjoner og finansinstitusjoner og kredittinstitusjoner og finansinstitusjoner seg imellom, herunder der lignende tjenester ytes av en korrespondentinstitusjon til en respondentinstitusjon, samt forbindelsene som er opprettet med sikte på verdipapirtransaksjoner eller overføringer av midler, eller forbindelsene som er opprettet med sikte på transaksjoner med kryptoeiendeler eller overføringer av kryptoeiendeler,».

c) Nr. 18 og 19 skal lyde:

«18) «kryptoeiendel» en kryptoeiendel som definert i artikkel 3 nr. 1 punkt 5 i europaparlaments- og rådsforordning (EU) 2023/1114(*), unntatt når den inngår i de kategoriene som er oppført i artikkel 2 nr. 2, 3 og 4 i nevnte forordning, eller på annen måte kan anses som midler,

19) «yter av kryptoeiendelstjenester» en yter av kryptoeiendelstjenester som definert i artikkel 3 nr. 1 punkt 15 i for-

ordning (EU) 2023/1114, når denne yter en eller flere av de kryptoeiendelstjenestene som er definert i artikkel 3 nr. 1 punkt 16 i nevnte forordning, med unntak av rådgivning om kryptoeiendeler som omhandlet i artikkel 3 nr. 1 punkt 16 bokstav h) i nevnte forordning,

(*) Europaparlaments- og rådsforordning (EU) 2023/1114 av 31. mai 2023 om markeder for kryptoeiendeler og om endring av forordning (EU) nr. 1093/2010 og (EU) nr. 1095/2010 samt direktiv 2013/36/EU og (EU) 2019/1937 (EUT L 150 av 9.6.2023, s. 40).»

d) Nytt nummer skal lyde:

«20) «frittstående adresse» en frittstående adresse som definert i artikkel 3 nr. 20 i europaparlaments- og rådsforordning (EU) 2023/1113(*).

(*) Europaparlaments- og rådsforordning (EU) 2023/1113 av 31. mai 2023 om opplysninger som skal følge overføringer av penger og visse kryptoeiendeler, og om endring av direktiv (EU) 2015/849 (EUT L 150 av 9.6.2023, s. 1).»

3) I artikkel 18 tilføyes følgende numre:

«5. EBA skal innen 30. desember 2024 utstede retningslinjer for risikovariabler og risikofaktorer som ytere av kryptoeiendelstjenester skal ta hensyn til når de inngår forretningsforbindelser eller gjennomfører transaksjoner med kryptoeiendeler.

6. EBA bør særlig presisere hvordan ytere av kryptoeiendelstjenester skal ta hensyn til de risikofaktorene som er oppført i vedlegg III, også når de utfører transaksjoner med personer og enheter som ikke omfattes av dette direktivet. For dette formålet skal EBA være særlig oppmerksom på produkter, transaksjoner og teknologier som har potensial til å fremme anonymitet, for eksempel anonyme lommebøker og miksetjenester.

Dersom det identifiseres situasjoner med høyere risiko, bør retningslinjene omhandlet i nr. 5 omfatte utvidede kundekontrolltiltak som ansvarlige enheter skal vurdere å anvende for å redusere slike risikoer, herunder vedtakelse av hensiktsmessige prosedyrer for å fastslå kryptoeiendelers opprinnelse eller bestemmelsessted.»

4) Nye artikler skal lyde:

«*Artikkel 19a*

1. Medlemsstatene skal kreve at ytere av kryptoeiendelstjenester identifiserer og vurderer risikoen for hvitvasking av penger og finansiering av terrorisme i forbindelse med overføringer av kryptoeiendeler til eller fra en frittstående adresse. For dette formålet skal ytere av kryptoeiendelstjenester innføre interne retningslinjer, prosedyrer og kontroller. Medlemsstatene skal kreve at ytere av kryptoeiendelstjenester treffer risikoreduserende tiltak som står i et rimelig forhold til de identifiserte risikoene. Disse risikoreduserende tiltakene skal omfatte ett eller flere av følgende elementer:

a) Innføring av risikobaserte tiltak som skal identifisere og kontrollere identiteten til avsenderen eller mottakeren ved en overføring til eller fra en frittstående adresse eller avsenderens eller mottakerens reelle eier, herunder ved å benytte tredjeparter.

b) Krav om ytterligere opplysninger om de overførte kryptoeiendelenes opprinnelse og bestemmelsessted.

c) Gjennomføring av løpende utvidet overvåking av disse transaksjonene.

d) Ethvert annet tiltak for å redusere og håndtere risikoen for hvitvasking av penger og finansiering av terrorisme samt risikoen for at målrettede økonomiske sanksjoner og målrettede økonomiske sanksjoner mot finansiering av våpenspredning ikke blir gjennomført eller omgås.

2. EBA skal innen 30. desember 2024 utstede retningslinjer for få spesifisere tiltakene omhandlet i denne artikkelen, herunder kriteriene og formene for identifisering og kontroll av identiteten til avsenderen eller mottakeren ved en overføring til eller fra en frittstående adresse, særlig ved å benytte tredjeparter, idet det tas hensyn til den seneste teknologiske utviklingen.

Artikkel 19b

1. Som unntak fra artikkel 19 skal medlemsstatene, når det gjelder korrespondentforbindelser over landegrensene som involverer utførelse av kryptoeiendelstjenester som definert i artikkel 3 nr. 1 punkt 16 i forordning (EU) 2023/1114, med unntak av bokstav h) i nevnte punkt, med en respondentenhet som ikke er etablert i Unionen og som yter lignende tjenester, herunder overføringer av kryptoeiendeler, i tillegg til de kundekontrolltiltakene som er fastsatt i artikkel 13 i dette direktivet, kreve at ytere

av kryptoeiendelstjenester når de inngår en forretningsforbindelse med en slik enhet,

a) fastslår om respondentenheten har en tillatelse eller er registrert,
b) innhenter tilstrekkelig informasjon om respondentenheten til fullt ut å forstå arten av dens virksomhet og ut fra offentlig tilgjengelig informasjon fastslå enhetens omdømme og tilsynets kvalitet,
c) vurderer respondentenhetens kontroller for bekjempelse av hvitvasking av penger og finansiering av terrorisme,
d) innhenter godkjenning fra den øverste ledelsen før nye korrespondentforbindelser inngås,
e) dokumenterer de respektive ansvarsområdene til hver part i korrespondentforbindelsen,
f) når det gjelder gjennomstrømningskontoer for kryptoeiendeler, forvisser seg om at respondentenheten har kontrollert identiteten til og løpende har utført kundekontroll av kunder som har direkte tilgang til korrespondentenhetens kontoer, og at den på anmodning kan framlegge relevante kundekontrollopplysninger for korrespondentenheten.

Når ytere av kryptoeiendelstjenester beslutter å avslutte korrespondentforbindelser av årsaker som er knyttet til retningslinjer for bekjempelse av hvitvasking av penger og finansiering av terrorisme, skal de dokumentere og registrere sin beslutning.

Ytere av kryptoeiendelstjenester skal ajourføre kundekontrollopplysningene for korrespondentforbindelsen regelmessig, eller når det oppstår nye risikoer i forbindelse med respondentenheten.

2. Medlemsstatene skal sikre at ytere av kryptoeiendelstjenester tar hensyn til opplysningene som er omhandlet i nr. 1, for på grunnlag av en risikovurdering å fastsette de hensiktsmessige tiltakene som skal treffes for å redusere de risikoene som er forbundet med respondentenheten.
3. EBA skal innen 30. juni 2024 utstede retningslinjer for å spesifisere de kriteriene og elementene som ytere av kryptoeiendelstjenester skal ta hensyn til når de foretar vurderingen omhandlet i nr. 1, og de risikoreduserende tiltakene som er omhandlet i nr. 2, herunder minstekrav til de tiltakene som ytere av kryptoeiendelstjenester skal treffe dersom respondentenheten ikke er registrert eller ikke har en tillatelse.»

5) Følgende artikkel innsettes:
«*Artikkel 24a*
EBA skal innen 1. januar 2024 utstede retningslinjer som spesifiserer hvordan de utvidede kundekontrolltiltakene i dette avsnittet får anvendelse når ansvarlige enheter utfører kryptoeiendelstjenester som definert i artikkel 3 nr. 1 punkt 16 i forordning (EU) 2023/1114, med unntak av bokstav h) i nevnte punkt, samt overføringer av kryptoeiendeler som definert i artikkel 3 nr. 10 i forordning (EU) 2023/1113. EBA skal særlig spesifisere hvordan og når disse ansvarlige enhetene skal innhente ytterligere opplysninger om avsenderen og mottakeren.»
6) I artikkel 45 skal nr. 9 lyde:
«9. Medlemsstatene kan kreve at utstedere av elektroniske penger som definert i artikkel 2 nr. 3 i direktiv 2009/110/EF, betalingstjenesteytere som definert i artikkel 4 nr. 11 i direktiv (EU) 2015/2366 og ytere av kryptoeiendelstjenester som er etablert på deres territorium i annen form enn en filial, og som har sitt hovedkontor i en annen medlemsstat, utpeker et sentralt kontaktpunkt på deres territorium. Dette sentrale kontaktpunktet skal sikre, på vegne av den enheten som driver virksomhet over landegrensene, overholdelse av reglene for bekjempelse av hvitvasking av penger og finansiering av terrorisme, og skal lette tilsynsmyndighetenes tilsyn, herunder ved å gi tilsynsmyndighetene dokumenter og opplysninger på anmodning.»
7) I artikkel 47 skal nr. 1 lyde:
«1. Medlemsstatene skal sikre at vekslekontorer, sjekkinnløsningskontorer og ytere av tjenester til truster eller selskaper har en tillatelse eller er registrert, og at ytere av pengespilltjenester er regulert.»
8) I artikkel 67 skal nytt nummer lyde:
«3. Medlemsstatene skal innen 30. desember 2024 vedta og kunngjøre de lovene og forskriftene som er nødvendige for å etterkomme artikkel 2 nr. 1 punkt 3, artikkel 3 nr. 2 bokstav g), artikkel 3 nr. 8, 18, 19 og 20, artikkel 19a nr. 1, artikkel 19b nr. 1 og 2, artikkel 45 nr. 9 og artikkel 47 nr. 1. De skal umiddelbart oversende Kommisjonen teksten til disse bestemmelsene.

De skal anvende disse bestemmelsene fra 30. desember 2024.»

Artikkel 39

Oppheving

Forordning (EU) 2015/847 oppheves med virkning fra anvendelsesdatoen for denne forordningen.

Henvisninger til den opphevede forordningen skal forstås som henvisninger til denne forordningen og leses som angitt i sammenligningstabellen i vedlegg II.

Artikkel 40

Ikrafttredelse

Denne forordningen trer i kraft den 20. dagen etter at den er kunngjort i *Den europeiske unions tidende*.

Den får anvendelse fra 30. desember 2024.

Denne forordningen er bindende i alle deler og kommer direkte til anvendelse i alle medlemsstater.

Utferdiget i Brussel 31. mai 2023.

For Europaparlamentet	*For Rådet*
R. Metsola	P. Kullgren
President	*Formann*

Vedlegg I

Opphevet forordning med endringer

Europaparlaments- og rådsforordning (EU) 2015/847 (EUT L 141 av 5.6.2015, s. 1)	
Europaparlaments- og rådsforordning (EU) 2019/2175 (EUT L 334 av 27.12.2019, s. 1)	[Bare artikkel 6]

Vedlegg II

Sammenligningstabell

Forordning (EU) 2015/847	Denne forordningen
Artikkel 1	Artikkel 1
Artikkel 2 nr. 1, 2 og 3	Artikkel 2 nr. 1, 2 og 3
Artikkel 2 nr. 4 første og andre ledd	Artikkel 2 nr. 4 første og andre ledd
–	Artikkel 2 nr. 4 tredje og fjerde ledd
Artikkel 2 nr. 5	Artikkel 2 nr. 5
Artikkel 3 innledende tekst	Artikkel 3 innledende tekst
Artikkel 3 nr. 1–9	Artikkel 3 nr. 1–9
–	Artikkel 3 nr. 10
Artikkel 3 nr. 10	Artikkel 3 nr. 11
Artikkel 3 nr. 11	Artikkel 3 nr. 12
Artikkel 3 nr. 12	–
–	Artikkel 3 nr. 13–24
Artikkel 4 nr. 1 innledende tekst	Artikkel 4 nr. 1 innledende tekst

Forordning (EU) 2015/847	Denne forordningen
Artikkel 4 nr. 1 bokstav a), b) og c)	Artikkel 4 nr. 1 bokstav a), b) og c)
–	Artikkel 4 nr. 1 bokstav d)
Artikkel 4 nr. 2 innledende tekst	Artikkel 4 nr. 2 innledende tekst
Artikkel 4 nr. 2 bokstav a) og b)	Artikkel 4 nr. 2 bokstav a) og b)
–	Artikkel 4 nr. 2 bokstav c)
Artikkel 4 nr. 3–6	Artikkel 4 nr. 3–6
Artikkel 5–13	Artikkel 5–13
–	Artikkel 14–23
Artikkel 14	Artikkel 24
Artikkel 15 nr. 1, 2 og 3	Artikkel 25 nr. 1, 2 og 3
Artikkel 15 nr. 4 eneste ledd	Artikkel 25 nr. 4 første ledd
–	Artikkel 25 nr. 4 andre ledd
Artikkel 16	Artikkel 26
–	Artikkel 27
Artikkel 17	Artikkel 28
Artikkel 18	Artikkel 29
Artikkel 19	Artikkel 30
Artikkel 20	Artikkel 31
Artikkel 21	Artikkel 32
Artikkel 22	Artikkel 33
Artikkel 23	Artikkel 34
Artikkel 24 nr. 1–6	Artikkel 35 nr. 1–6
Artikkel 24 nr. 7	–
Artikkel 25 eneste ledd	Artikkel 36 første ledd
–	Artikkel 36 andre, tredje og fjerde ledd
–	Artikkel 37
–	Artikkel 38
Artikkel 26	Artikkel 39
Artikkel 27	Artikkel 40
Vedlegg	–
–	Vedlegg I
–	Vedlegg II

Vedlegg 4

EØS-komiteens beslutning nr. 40/2025 av 20. februar 2025 om endring av EØS-avtalens vedlegg IX (Finansielle tjenester)

EØS-KOMITEEN HAR –

under henvisning til avtalen om Det europeiske økonomiske samarbeidsområde, heretter kalt EØS-avtalen, særlig artikkel 98,

og ut fra følgende betraktninger:

(1) Europaparlaments- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011[1] skal innlemmes i EØS-avtalen.

(2) Europaparlaments- og rådsdirektiv (EU) 2022/2556 av 14. desember 2022 om endring av direktiv 2009/65/EF, 2009/138/EF, 2011/61/EU, 2013/36/EU, 2014/59/EU, 2014/65/EU, (EU) 2015/2366 og (EU) 2016/2341 med hensyn til digital operasjonell motstandsdyktighet i finanssektoren[2] skal innlemmes i EØS-avtalen.

(3) EØS-avtalens vedlegg IX bør derfor endres –

TRUFFET DENNE BESLUTNING:

Artikkel 1

I EØS-avtalens vedlegg IX gjøres følgende endringer:

1. I nr. 1 (europaparlaments- og rådsdirektiv 2009/138/EF), 14 (europaparlaments- og rådsdirektiv 2013/36/EU), 19b (europaparlaments- og rådsdirektiv 2014/59/EU), 30 (europaparlaments- og rådsdirektiv 2009/65/EF), 31ba (europaparlaments- og rådsdirektiv 2014/65/EU) og 31bb (europaparlaments- og rådsdirektiv 2011/61/EU) skal nytt strekpunkt lyde:
   «– **32022 L 2556**: Europaparlaments- og rådsdirektiv (EU) 2022/2556 av 14. desember 2022 (EUT L 333 av 27.12.2022, s. 153).»
2. I nr. 16e (europaparlaments- og rådsdirektiv (EU) 2015/2366) og 31d (europaparlaments- og rådsdirektiv (EU) 2016/2341) tilføyes følgende:
   «, endret ved:
   – **32022 L 2556**: Europaparlaments- og rådsdirektiv (EU) 2022/2556 av 14. desember 2022 (EUT L 333 av 27.12.2022, s. 153).»
3. Etter nr. 31pc (delegert kommisjonsforordning (EU) 2023/2486) tilføyes følgende:
   «31q.**32022 R 2554**: Europaparlaments- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren og om endring av forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (EUT L 333 av 27.12.2022, s. 1).

   Forordningens bestemmelser skal for denne avtales formål gjelde med følgende tilpasninger:

   a) Uten at det berører bestemmelsene i EØS-avtalens protokoll 1, og dersom ikke annet er fastsatt i avtalen, skal betydningen av ordene 'medlemsstat(er)' og 'vedkommende myndigheter' også omfatte, i tillegg til den betydning de har i forordningen, henholdsvis EFTA-statene og deres vedkommende myndigheter.

   b) Dersom ikke annet er fastsatt i denne avtale, skal de europeiske tilsynsmyndighetene og EFTAs overvåkingsorgan samarbeide, utveksle opplysninger og rådføre seg med hverandre ved anvendelse av forordningen, særlig før tiltak settes i verk.

   c) Beslutninger, anmodninger, anbefalinger, uttalelser, planer og andre tiltak fra EFTAs overvåkingsorgan i samsvar med artikkel 31, 33, 35–39, 42 og 43 skal uten unødig opphold vedtas basert på utkast utarbeidet av vedkommende

[1] EUT L 333 av 27.12.2022, s. 1.
[2] EUT L 333 av 27.12.2022, s. 153.

europeiske tilsynsmyndighet i henhold til artikkel 31 nr. 1 på eget initiativ eller etter anmodning fra EFTAs overvåkingsorgan.

d) Der forordningen viser til de nasjonale sentralbankene, skal den, når det gjelder Liechtenstein, vise til finansdepartementet i Liechtenstein.

e) I artikkel 3 nr. 61 skal ordene 'eller, der det er relevant, EFTAs overvåkingsorgan' tilføyes etter ordene 'den europeiske tilsynsmyndigheten'.

f) I artikkel 3 nr. 30 skal ordene 'relevant unionsrett eller nasjonal rett' erstattes med ordene 'relevante bestemmelser i EØS-avtalen eller nasjonal rett', og i artikkel 55 nr. 3 skal ordene 'unionsretten eller nasjonal rett' erstattes med ordene 'EØS-avtalen eller nasjonal rett'.

g) I artikkel 6 nr. 10 og artikkel 19 nr. 5 skal ordene 'unionsretten og nasjonal sektorspesifikk lovgivning' erstattes med ordene 'EØS-avtalen og nasjonal sektorspesifikk lovgivning'.

h) I artikkel 19 nr. 7 skal ordene 'og EFTA-statenes nasjonale sentralbanker' tilføyes etter ordene 'medlemmene av Det europeiske system av sentralbanker'.

i) I artikkel 31 nr. 1:

i) ordene ', eller EFTAs overvåkingsorgan med hensyn til tredjepartsleverandører av IKT-tjenester som er etablert i en EFTA-stat, eller tredjepartsleverandører av IKT-tjenester som er etablert i et tredjeland, men har et datterforetak i en EFTA-stat,' skal tilføyes etter ordet 'Felleskomiteen',

ii) ordene ', eller, dersom det er relevant, EFTAs overvåkingsorgan,' skal tilføyes etter ordene 'den europeiske tilsynsmyndigheten som er ansvarlig',

iii) i bokstav b) tilføyes følgende:

'EFTAs overvåkingsorgan skal være hovedovervåker for hver kritisk tredjepartsleverandør av IKT-tjenester som er etablert i en EFTA-stat, og for tredjepartsleverandører av IKT-tjenester som er etablert i et tredjeland, men har et datterforetak i en EFTA-stat. De europeiske tilsynsmyndighetene skal gjennom Felleskomiteen utpeke den relevante europeiske tilsynsmyndigheten som skal bistå EFTAs overvåkingsorgan i å ivareta sin rolle i henhold til forordningen, herunder ved å utarbeide utkastene nevnt i tilpasning c).'.

j) I artikkel 31 nr. 5 skal ordene ', eller, der det er relevant, EFTAs overvåkingsorgan,' tilføyes etter ordet 'Felleskomiteen'.

k) I artikkel 31 nr. 8 ii) skal ordene 'eller, når det gjelder EFTA-statene, oppgaver som har til formål å støtte de samme oppgavene som de som er nevnt i artikkel 127 nr. 2 i traktaten om Den europeiske unions virkemåte' tilføyes etter ordene 'traktaten om Den europeiske unions virkemåte'.

l) I artikkel 31 nr. 11 skal ordene ', eller, der det er relevant, EFTAs overvåkingsorgan,' tilføyes etter ordet 'Felleskomiteen'.

m) I artikkel 32 nr. 4 skal nye ledd lyde:

'Vedkommende myndigheter i EFTA-statene skal ha de samme rettighetene og pliktene som vedkommende myndigheter i EU-medlemsstatene i overvåkingsforumets arbeid.

EFTAs overvåkingsorgan skal ha rett til å utpeke to representanter til overvåkingsforumet, hvorav én skal være en representant på høyt nivå, med de samme rettighetene og pliktene som de europeiske tilsynsmyndighetenes representanter.'.

n) I artikkel 32 nr. 8 skal ordet 'unionsregler' erstattes med ordene 'bestemmelser i EØS-avtalen'.

o) I artikkel 34 nr. 1 skal nytt punktum lyde:

'EFTAs overvåkingsorgan, i sin rolle som hovedovervåker, skal delta i det felles overvåkingsnettverket.'.

p) I artikkel 35 nr. 3 skal nytt ledd lyde:

'Før den ansvarlige europeiske tilsynsmyndigheten utarbeider et utkast til anbefaling i samsvar med nr. 1 bokstav d) for EFTAs overvåkingsorgan, skal den gi tredjepartsleverandøren av IKT-tjenester mulighet til å legge fram, innen 30 kalenderdager, relevante opplysninger som dokumenterer den forventede innvirkningen på kunder som er enheter som faller utenfor virkeområdet for denne forordningen, og, dersom

det er relevant, utarbeide løsninger for å redusere risikoene.'.

q) I artikkel 35 nr. 9 skal nytt punktum lyde:

'EFTA-statenes faste komité skal avgjøre fordelingen av beløpene for overtredelsesgebyrer innkrevd av EFTAs overvåkingsorgan i sin rolle som hovedovervåker.'.

r) I artikkel 35 nr. 11, etter første ledd, skal nytt ledd lyde:

'Før den ansvarlige europeiske tilsynsmyndigheten utarbeider et utkast til beslutning om overtredelsesgebyr i henhold til nr. 6 for EFTAs overvåkingsorgan, skal den gi representantene for den kritiske tredjepartsleverandøren av IKT-tjenester som saken gjelder, mulighet til å bli hørt om de omstendighetene som tilsynsmyndigheten har påtalt, og den skal basere sine beslutninger bare på omstendigheter som den kritiske tredjepartsleverandøren av IKT-tjenester som saken gjelder, har hatt mulighet til å uttale seg om.'.

s) I artikkel 36 nr. 2 skal ordene 'eller EFTAs overvåkingsorgan' tilføyes etter ordene 'EBA, ESMA eller EIOPA'.

t) I artikkel 37 nr. 3, når det gjelder EFTA-statene, skal bokstav f) lyde:

'opplyse om retten til å bringe beslutningen inn for EFTA-domstolen i samsvar med artikkel 36 i avtalen mellom EFTA-statene om opprettelse av et overvåkingsorgan og en domstol.'.

u) I artikkel 40 nr. 2:

i) ordene 'og EFTAs overvåkingsorgan' skal tilføyes etter ordene 'de europeiske tilsynsmyndighetene',

ii) nytt ledd skal lyde:

'EFTAs overvåkingsorgans deltakelse i den felles granskningsgruppen skal, i saker der overvåkingsvirksomheten ikke involverer en tredjepartsleverandør av IKT-tjenester eller et datterforetak etablert i en EFTA-stat, være på frivillig grunnlag.'.

v) I artikkel 49 nr. 1 skal ordene 'og EFTAs overvåkingsorgan' tilføyes etter ordene 'europeiske tilsynsmyndighetene'.

w) I artikkel 49 nr. 2 og artikkel 56 nr. 1 skal ordene ', EFTAs overvåkingsorgan' tilføyes etter ordene 'europeiske tilsynsmyndighetene'.

x) I artikkel 64, når det gjelder EFTA-statene, skal ordene '17. januar 2025' forstås som 'en dato utpekt i henhold til nasjonal lovgivning som ikke skal være senere enn tolv måneder etter ikrafttredelsesdatoen for EØS-komiteens beslutning nr. [nn/åååå] av [måned/år] (denne beslutningen)'.

4. I nr. 31baa (europaparlaments- og rådsforordning (EU) nr. 600/2014), 31bc (europaparlaments- og rådsforordning (EU) nr. 648/2012), 31bf (europaparlaments- og rådsforordning (EU) nr. 909/2014), 31eb (europaparlaments- og rådsforordning (EF) nr. 1060/2009) og 31l (europaparlaments- og rådsforordning (EU) 2016/1011) skal nytt strekpunkt lyde:

«– **32022 R 2554**: Europaparlaments- og rådsforordning (EU) 2022/2554 av 14. desember 2022 (EUT L 333 av 27.12.2022, s. 1).»

Artikkel 2

Teksten til forordning (EU) 2022/2554 og direktiv (EU) 2022/2556 på islandsk og norsk, som vil bli kunngjort i EØS-tillegget til *Den europeiske unions tidende*, skal gis gyldighet.

Artikkel 3

Denne beslutning trer i kraft 21. februar 2025, forutsatt at alle meddelelser etter EØS-avtalens artikkel 103 nr. 1 er inngitt[3].

Artikkel 4

Denne beslutning skal kunngjøres i EØS-avdelingen av og EØS-tillegget til *Den europeiske unions tidende*.

Utferdiget i Brussel 20. februar 2025

For EØS-komiteen
Formann
Nicolas von Lingen

EØS-komiteens
sekretærer
Knut Hermansen
Matúš Minárik

[3] [Forfatningsrettslige krav angitt.]

Vedlegg 5

EØS-komiteens beslutning nr. 42/2025 av 20. februar 2025 om endring av EØS-avtalens vedlegg IX (Finansielle tjenester)

EØS-KOMITEEN HAR –

under henvisning til avtalen om Det europeiske økonomiske samarbeidsområde, heretter kalt EØS-avtalen, særlig artikkel 98,

og ut fra følgende betraktninger:

1) Europaparlaments- og rådsforordning (EU) 2023/1113 av 31. mai 2023 om opplysninger som skal følge overføringer av penger og visse kryptoeiendeler, og om endring av direktiv (EU) 2015/849[1] skal innlemmes i EØS-avtalen.
2) Forordning (EU) 2023/1113 opphever europaparlaments- og rådsforordning (EU) 2015/847[2], som er innlemmet i EØS-avtalen, og som følgelig skal oppheves i EØS-avtalen.
3) EØS-avtalens vedlegg IX bør derfor endres –

TRUFFET DENNE BESLUTNING:

Artikkel 1

I EØS-avtalens vedlegg IX gjøres følgende endringer:

1. I nr. 23b (europaparlaments- og rådsdirektiv (EU) 2015/849) tilføyes følgende:
   «**– 32023 R 1113**: Europaparlaments- og rådsforordning (EU) 2023/1113 av 31. mai 2023 (EUT L 150 av 9.6.2023, s. 1).»
2. Teksten i nr. 23ba (europaparlaments- og rådsforordning (EU) 2015/847) skal lyde:
   «**32023 R 1113**: Europaparlaments- og rådsforordning (EU) 2023/1113 av 31. mai 2023 om opplysninger som skal følge overføringer av penger og visse kryptoeiendeler, og om endring av direktiv (EU) 2015/849 (EUT L 150 av 9.6.2023, s. 1).

   Forordningens bestemmelser skal for denne avtales formål gjelde med følgende tilpasning:

   I artikkel 23, når det gjelder EFTA-statene, skal ordene 'restriktive tiltak på unionsplan og nasjonalt plan' forstås som 'nasjonalt gjeldende restriktive tiltak'.»

Artikkel 2

Denne beslutning trer i kraft […], forutsatt at alle meddelelser etter EØS-avtalens artikkel 103 nr. 1 er inngitt[3], eller på den dag EØS-komiteens beslutning nr. …/… av […][4] [som innlemmer {forordning (EU) 2023/1114} i EØS-avtalen] trer i kraft, alt etter hva som inntreffer sist.

Artikkel 3

Denne beslutning skal kunngjøres i EØS-avdelingen av og EØS-tillegget til *Den europeiske unions tidende*.

Utferdiget i Brussel 20. februar 2025

For EØS-komiteen
Formann
Nicolas von Lingen

EØS-komiteens
sekretærer
Knut Hermansen
Matúš Minárik

[1] EUT L 150 av 9.6.2023, s. 1.
[2] EUT L 141 av 5.6.2015, s. 1.
[3] [Forfatningsrettslige krav angitt.]
[4] Ennå ikke kunngjort.

Bestilling av publikasjoner

Departementenes sikkerhets- og serviceorganisasjon
publikasjoner.dep.no
Telefon: 22 24 00 00

Publikasjonene er også tilgjengelige på
www.regjeringen.no

Trykk: Departementenes sikkerhets- og
serviceorganisasjon – 03/2025