EU-rettsakter som vil kunne behandles etter skriftlig prosedyre 20. februar 2025

I det nedenstående følger oversikt inndelt som følger:

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

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

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

FINANSDEPARTEMENTET

32022R2554 Europaparlaments- og rådforordning (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

Forordningen innføres ved lov, og det tar derfor forbehold om Stortingets samtykke.

Status

Et forslag om gjennomføring av DORA i norsk rett var på høring våren 2024. Finansdepartementet tar sikte på å legge frem en Prop. LS for Stortinget i løpet av første kvartal 2025.

DORA trådte i kraft i EU 17.01.2025.

Sammendrag av innhold

Innledning

Forordning (EU)2022/2554 om digital og operasjonell motstandsdyktighet i den finansielle sektoren (DORA-forordningen, heretter DORA). Forordningen gjelder for de fleste finansforetak og i tillegg for IKT-tjenesteleverandører. Noen typer foretak er unntatt. DORA ble vedtatt i november 2022 og trådte i kraft 17. januar 2025 i EU.

DORA inneholder flere bestemmelser som gir de europeiske tilsynsmyndighetene myndighet til å utarbeide regulatoriske tekniske standarder.

DORA medfører også at flere forordninger innen finansområdet må endres. Disse er inntatt som endringsbestemmelser til DORA. Videre medfører DORA at flere direktiver innen finansområdet må endres. Endringene fremgår av direktiv (EU) 2022/2556

Bakgrunnen for det vedtatte regelverket

I september 2020 fremla Europakommisjonen en digital finanspakke, «Digital Finance Package», med en digital finansiell strategi og regelverk, for å sikre forbrukere tilgang til innovative finansielle produkter, samtidig som forbrukervern og finansiell stabilitet er ivaretatt. Som en del av pakken ble DORA lansert.

EU-regelverket på det digitale området er i stor grad regulert sektorvis i finanssektoren. I tillegg har man, både i EU og på nasjonalt nivå, valgt forskjellige tilnærminger, som anses som et potensielt hinder for fri flyt av varer og tjenester for foretak med grensekryssende virksomhet i finanssektoren.

Finanssektoren er preget av rask digitalisering. Dette omfatter stadig nye og avanserte digitale løsninger. Løsningene medfører gevinster for forbrukere, finansforetak og samfunnet for øvrig, men introduserer samtidig nye sårbarheter. Finanssektoren er i stor grad avhengig av slike løsninger.

Foretakenes benytter seg i større grad av leverandører og antallet leverandører øker. I tillegg øker kompleksiteten i løsningene og det samme gjelder kontraktsforholdene med leverandørene. Dette representerer i mange tilfeller en endret/økt risiko for foretakene. Konsentrasjonsrisikoen er tidvis høy, da visse tjenester leveres til mange foretak av et fåtall leverandører. I tillegg er finanssektoren utsatt for digitale angrep, som kan få store samfunnsmessige konsekvenser og true finansiell stabilitet.

DORA er utarbeidet for å imøtekomme truslene som foreligger. Regelverket fokuserer på overordnet risikostyring, håndtering av hendelser, testing, håndtering av tredjepartsrisiko samt informasjonsdeling. Ved anvendelse av regelverket er det lagt til grunn at proporsjonalitetsprinsippet skal gjelde.

Forordningens innhold

DORA er delt inn i ni kapitler. Bestemmelsene angir krav til foretakene, herunder tiltak foretakene skal iverksette for å være motstandsdyktige ovenfor digitale angrep. Det er også gitt regler om rapportering av hendelser. I tillegg reguleres EU sin rolle som overvåkningsorgan. Nedenfor følger en kort redegjørelse for kapitlene. Små og mellomstore foretak er delvis unntatt fra regelverket.

<u>Kapittel I – Generelle bestemmelser</u>

Kapittelet inneholder overordnede bestemmelser vedrørende forordningens formål og hvem den gjelder for. De fleste finansforetak, verdipapirforetak og fond er omfattet. I tillegg er en rekke begreper definert. Det er også inntatt en bestemmelse om anvendelse av proporsjonalitetsprinsippet for deler av forordningens bestemmelser. Foretakets størrelse, risikoprofil, type virksomhet samt tjenestenes skala og kompleksitet er relevante momenter i vurderingen.

Microentrepriser er en definisjon som er verdt å merke seg, da slike foretak i flere sammenhenger er unntatt for krav i regelverket. Det samme gjelder små og mellomstore entrepriser.

DORA gjelder for følgende foretak:

a. Kredittforetak

b. Betalingsforetak, inkludert betalingsforetak unntatt i PSD2 ((EU) 2015/2366)

c. Kontoinformasjonstilbydere

d. E-pengeforetak, inkludert e-pengeforetak unntatt i E-pengedirektivet (2009/110/EC)

e. Verdipapirforetak

f. Tilbydere av kryptotjenester, med tillatelse i henhold til MiCA(52020PC0593), m.m.

g. Verdipapirsentraler

h. Sentrale motparter

i. Markedsplasser

j. Transaksjonsregistre

k. AIF-forvaltere

l. Administrasjonsselskaper

m. Leverandører av datarapporteringstjenester

n. Forsikrings- og gjenforsikringsforetak

o. Forsikringsformidlere, gjenforsikringsformidlere og aksessoriske forsikringsformidlere

p. Arbeidsmarkedsrelaterte pensjonskasser

q. Kredittvurderingsforetak

r. Administratorer av kritiske benchmarks

s. Tjenesteleverandører for folkefinansiering

t. Verdipapirregistre

u. Tredjepartstilbydere av IKT

Følgende er unntatt:

a. AIF-forvaltere, jf. AIFMD (2011/61/EU), Art 3(2)

b. Forsikrings- og gjenforsikringsforetak, jf. Solvens II (2009/138/EF), art. 4

c. Arbeidsmarkedsrelaterte pensjonskasser, som forvalter pensjonsordninger, som til sammen ikke har flere enn 15 medlemmer totalt

d. Faktiske og juridiske personer unntatt i henhold til MIFID II (2014/65/EU), art. 2 og 3.

e. Forsikringsformidlere, gjenforsikringsformidlere og aksessoriske forsikringsformidlere, som er mikroentrepriser eller små/mellomstore foretak.

f. Postgirokontorer, jf. CRD (2013/36/EU), art 2(5), nr. 3.

Kapittel II – Risikostyring på IKT-området

Kapittelet er delt inn i to hoveddeler. Den første delen inneholder en generell bestemmelse om overordnet virksomhetsstyring og organisering av foretaket. Den andre delen inneholder krav til et rammeverk for risikostyring og krav til elementer rammeverket skal inneholde.

Overordnet virksomhetsstyring og organisering

Det stilles krav til at foretakene skal ha et overordnet rammeverk for styring og kontroll av IKT-virksomheten. Rammeverket skal sikre en effektiv og forsvarlig risikostyring samt sikre en høy grad av motstandsdyktighet. Videre stilles det krav til at ledelsen skal definere, godkjenne, overvåke og være ansvarlig for å implementere et rammeverk for risikostyring.

For å oppnå styring og kontroll på IKT-virksomheten stilles det flere krav til ledelsen. Ledelsen er ansvarlig for å styre foretakets håndtering av IKT-risiko. Videre skal det utarbeides retningslinjer for å

sikre tilgjengelighet, autentisitet, integritet og konfidensialitet av data. IKT-relaterte funksjoner i foretaket skal ha tydelige roller, og ledelsen skal sørge for at funksjonene kan kommunisere rettidig, samarbeide og koordinere arbeidet sitt. Videre har ledelsen ansvaret for å fastsette og godkjenne en strategi for digital motstandsdyktighet, herunder definere et akseptabelt nivå for risikotoleranse.

Ledelsen skal også godkjenne, overvåke og jevnlig vurdere foretakets kontinuitetsplan og kriseplan. Det stilles krav til at ledelsen skal godkjenne og jevnlig revidere internrevisjonens planer på IKT-området, IKT-revisjoner og vesentlige endringer av dem. I tillegg skal ledelsen tildele og jevnlig gjennomgå et passende budsjett for å imøtekomme foretakets behov i forbindelse med digital motstandsdyktighet.

I forhold til IKT-tjenesteleverandører er ledelsen ansvarlig for å godkjenne og jevnlig revidere retningslinjer for IKT-tjenesteavtaler. Ledelsen er også ansvarlig for å etablere rapporteringskanaler, slik at de er oppdatert på bruk av IKT-tjenesteleverandører, planlagte vesentlige endringer av leverandørforhold og potensiell innvirkning på kritiske og viktige funksjoner eventuelle endringer har. Som en del av rapporteringen av potensielle endringer av kritiske og viktige funksjoner, skal rapporteringen også inneholde oppsummering av utført risikoanalyse, for at ledelsen kan vurdere konsekvensen av endringer. Rapporteringen skal også omfatte større IKT-hendelser og deres innvirkning på foretaket, herunder respons samt tiltak for gjenoppretting og korrigering.

Regelverket stiller krav til at foretakene skal ha en funksjon som skal overvåke tjenester levert av tredjeparter. Alternativt kan ansvaret for å følge opp risikoeksponeringen og relevant dokumentasjon i forbindelse med tjenesteleveransen delegeres. Kravene beskrevet i dette avsnittet gjelder ikke for microentrepriser.

Operasjonelle bestemmelser

Det stilles krav til et solid, helhetlig og veldokumentert rammeverk for risikostyring på IKT-området. Rammeverkets formål skal være å håndtere risiko raskt, effektivt og helhetlig, for å sikre en høy grad av operasjonell motstandsdyktighet.

Det stilles flere krav til rammeverket. Blant annet skal det minimum inneholde nødvendige strategier, retningslinjer, prosedyrer, IKT-protokoller og IKT-verktøy for å beskytte foretakets data og redusere risiko. Foretakene skal følge opp rammeverket i praksis. Den kompetente myndigheten kan kreve å få se helhetlig og oppdatert dokumentasjon vedrørende IKT-risiko og rammeverket for risikostyring.

Overvåkningen av IKT-risiko skal tillegges en kontrollfunksjon, som skal være uavhengig for å unngå interessekonflikter, jf. blant annet prinsippet om tre forsvarslinjer. Rammeverket skal gjennomgås minimum årlig. For microentrepriser stilles det imidlertid kun krav til periodisk gjennomgang. I tillegg skal rammeverket gjennomgås i etterkant av større IKT-hendelser, eller i henhold til instruksjoner/konklusjoner fra tilsynsmyndigheten i forbindelse med testing av operasjonell motstandsdyktighet eller revisjoner. Den kompetente myndigheten kan kreve å få fremlagt en rapport med foretakets vurdering av rammeverket for IKT-risiko. Rammeverket skal gjennomgås av internrevisjonen. Revisjonsrapporten skal følges opp med nødvendige tiltak, og det skal foreligge en operasjonell strategi for implementeringen. Regelverket stiller minimumskrav til implementeringsstrategien.

For å kunne håndtere IKT-risiko, stilles det krav til at foretakene skal benytte oppdaterte IKT-systemer, protokoller og verktøy. Regelverket stiller i denne sammenheng flere minimumskrav.

Regelverket inneholder bestemmelser om identifikasjon, som går ut på at foretaket skal identifisere, klassifisere og dokumentere IKT-relaterte funksjoner. Identifiseringen omfatter blant annet konfigurasjoner, systemavhengigheter, kartlegging av utstyr, avhengigheter i forhold til tredjeparter og kilder til IKT-risiko. Det stilles også krav til tiltak foretaket må implementere for å beskytte seg

mot, forhindre og avdekke eventuelle dataangrep, samt krav til hvordan foretaket skal respondere og ha mekanismer for å gjenopprette driften ved hendelser eller avvik.

Som en del av rammeverket for risikostyring på IKT-området, skal foretaket utarbeide en kontinuitetsplan for IKT-virksomheten og -løsningene, herunder gjenopprettelsesplaner. Videre skal det foretas en konsekvensanalyse for virksomheten (Business Impact Assessment, BIA) som skal ligge til grunn for kontinuitetsplanen. Kontinuitetsplanen skal være gjenstand for testing. På forespørsel fra den kompetente myndigheten skal foretakene rapportere antatt kostnad og mulige tap som følge av et alvorlig angrep.

DORA regulerer prosedyrer og metoder for gjenoppretting av normal drift etter en hendelse. Formålet med bestemmelsene er å sikre at foretakets IKT-systemer og data kan gjenopprettes med minimal nedetid, slik at driftsavbruddet og tap av data begrenses. Blant annet gis det nærmere bestemmelser om prosedyrer for hvordan gjenoppretting skal skje og hvilke krav som stilles til backup-løsninger. For verdipapirsentraler stilles det krav til minst et sekundært datasenter, som må oppfylle flere kriterier.

Foretakene skal ha ressurser og ansatte for å samle informasjon om sårbarheter og cybertrusler samt IKT-hendelser, spesielt dataangrep, som kan påvirke foretakets digitale motstandsdyktighet. Informasjonen skal analyseres for å kunne vurdere hvordan den affekterer den digitale motstandsdyktigheten. Videre skal foretakene evaluere større IKT-hendelser, ved å analysere årsaken og avdekke hvilke forbedringer som må gjøres i forhold til IKT-driften og kontinuitetsplanen. Ledelsen skal, minst årlig, motta rapporter om hvilke funn som er gjort samt anbefalte tiltak. Eventuelle endringer som følge av større hendelser skal rapporteres til den kompetente myndigheten på forespørsel. Erfaringer i henhold til testing og IKT-hendelser, herunder ved aktivering av kriseplan m.m., skal inntas i foretakets risikovurderingsprosess. For øvrig reguleres foretakenes plikt til å overvåke i hvilken grad strategien for digital motstandsdyktighet er effektiv og hvordan overvåkingen skal utføres. Foretakene skal også følge med på teknologiutviklingen, for å kunne vurdere hvordan den påvirker krav til IKT-sikkerhet og digital motstandsdyktighet. Foretakene skal ha intern opplæring for ansatte. Det skal også foreligge en plan for krisekommunikasjon.

Flere typer foretak er unntatt fra reglene beskrevet over, da det foreligger bestemmelser om et forenklet rammeverk for risikostyring.

Kapittel III – Håndtering av IKT-relaterte hendelser, klassifisering og rapportering

Det stilles krav til håndtering, klassifisering og rapportering av IKT-hendelser. Bestemmelsene går i hovedsak ut på at foretakene skal utarbeide prosedyrer for tilfellene hvor en hendelse inntreffer, herunder hvordan foretaket skal overvåke, håndtere og følge opp en pågående hendelse. Klassifiseringen av hendelser skal skje i henhold til visse minimumskriterier. Rapporteringen skal skje til relevant myndighet. De europeiske tilsynsmyndighetene (ESAene) skal gjennom en felles komité (Joint Committee (JC)) utarbeide en standard for rapporteringen. ESAene skal også gjennom en felles komité, og i samarbeid med den Europeiske Sentralbanken, vurdere muligheten for å sentralisere rapporteringen av større IKT-hendelser til et sentralt punkt i EU. En slik løsning må for Norges del vurderes særskilt med tanke på suverenitetsprinsippet. Den kompetente myndigheten skal følge opp en rapportert hendelse med kvittering for mottatt varsel samt gi relevante tilbakemeldinger og eventuelt veiledning. Det er spesielt lagt vekt på at den kompetente myndigheten skal veilede på eventuelle tiltak foretaket kan gjøre og hvordan man kan minimere påvirkningen på resten av sektoren. Alle IKT-hendelser og kvalifiserte cybertrusler skal loggføres etter visse kriterier. Foretakene har også anledning til å melde fra om kvalifiserte cybertrusler på frivillig basis.

Kapittel IV – Testing av digital operasjonell motstandsdyktighet

Kapittelet inneholder generelle krav til testing av digital motstandsdyktighet. Foretakene skal etablere, vedlikeholde og evaluere et solid og helhetlig program for å teste operasjonell

motstandsdyktighet. Programmet skal inngå i rammeverket for risikostyring. Formålet med testingen er å vurdere hvor forberedt foretakene er på IKT-hendelser samt avdekke svakheter, mangler og avvik i den digitale motstandsdyktigheten. Videre skal testingen gi grunnlag for å implementere forbedringstiltak raskt.

Det skal blant annet foreligge forskjellige vurderinger/analyser, tester, metoder, praksiser og verktøy i forbindelse med testingen. Testingen skal skje med en risikobasert tilnærming og foretaket skal sikre at testingen gjennomføres av en uavhengig aktør, enten intern eller ekstern. Foretakene skal utarbeide prosedyrer og rutiner for å prioritere, klassifisere og rette feil avdekket gjennom testingen. I tillegg skal det etableres en metode for intern validering for å sikre at alle avdekkede svakheter, mangler og avvik følges opp. Kritiske IKT-systemer skal minimum testes årlig. Microentrepriser er unntatt flere av kravene gitt i forbindelse med testing.

Testprogrammet for operasjonell motstandsdyktighet skal, i tråd med proporsjonalitetsprinsippet, legge til rette for gjennomføring av adekvat testing. I denne sammenheng lister regelverket opp eksempler på en rekke type tester. På dette området foreligger det egne regler for verdipapirsentraler, sentrale motparter og microentrepriser.

Det stilles krav til trusselbasert penetrasjonstesting (TLPT). En rekke typer foretak er unntatt fra slik testing, blant annet microentrepriser. En TLPT skal gjennomføres minst hvert tredje år. Den kompetente myndigheten skal vurdere hvilke foretak som skal utføre TLPT ut ifra et proporsjonalitetsprinsipp samt vurderingskriterier i regelverket. En TLPT skal dekke flere eller alle kritiske funksjoner i et foretak. Finansforetak skal identifisere relevante underliggende IKT-systemer, prosesser og teknologier, som støtter kritiske og viktige funksjoner. Dette omfatter funksjoner som er satt bort til leverandør. Foretakene skal vurdere hvilke kritiske og viktige funksjoner som bør være en del av TLPT, med tanke på å definere et presist tema/omfang for testingen. Vurderingen skal godkjennes av den kompetente myndigheten.

I noen tilfeller legges det opp til at TLPT ovenfor leverandører, etter avtale, kan gjennomføres som en samlet test, på vegne av flere foretak, av en ekstern tester.

Finansforetak skal, under testingen, minimere potensiell innvirkning på data, skade på ressurser, forstyrrelser på kritiske og viktige funksjoner, tjenester eller drift i eget foretak, konkurrenter, eller finanssektoren generelt. For å oppnå dette skal foretaket anvende effektive risikokontroller.

Etter at en TLPT er gjennomført, skal den kompetente myndigheten tilsendes et sammendrag av funn, planer for å rette opp funn og dokumentasjon som viser at testen er gjennomført i henholdt til gjeldende krav. Det skal foreligge en attest på at testen er gjennomført korrekt, for å kunne tillate gjensidig anerkjennelse av testen mellom kompetente myndigheter. Attesten skal formidles til den kompetente myndigheten.

Finansforetak skal ansette testere, med formålet å kunne gjennomføre TLPT. Signifikante kredittinstitusjoner skal kun bruke eksterne testere. Når det gjelder testere, stilles det krav til aktørene som skal gjennomføre testene.

Regelverket åpner for at det kan utpekes en egen TLPT-myndighet, som er ansvarlig for å følge opp TLPT-relaterte spørsmål. Dersom det ikke pekes ut en egen myndighet, er det tilsynsmyndigheten etter DORA som er TLPT-myndigheten. I slike tilfeller oppgaver i relasjon til TLPT delegeres til en annen nasjonal myndighet i finanssektoren.

<u>Kapittel V – Håndtering av tredjepartsrisiko på IKT-området</u>

Kapittelet er delt inn i to hoveddeler. Den første delen omhandler grunnleggende prinsipper for håndtering av tredjepartsrisikoer, mens den andre delen omhandler et tilsynsrammeverk for vesentlige IKT-tjenesteleverandører.

Grunnleggende prinsipper for håndtering av tredjepartsrisikoer

Når det gjelder tredjepartsrisiko, skal styringen av tredjepartsrisikoen inngå som en del av den overordnede risikostyringen. Foretaket er ansvarlig for etterlevelse av alle forpliktelser som følger av DORA og annet relevant regelverk, også ved inngåelse av IKT-tjenesteavtaler. I tillegg angis retningslinjer for hva foretakene skal legge vekt på ved risikostyringen. Foretakene plikter å ha en oversikt over IKT-tjenesteavtaler og skal definere og dokumentere hvilke avtaler som er kritiske eller viktige. Oversikten skal forelegges på forespørsel fra relevant tilsynsmyndighet. Foretakene skal minimum årlig rapportere nye avtaler som er inngått, hva slags type kontrakt som er inngått, form for avtaleinngåelse og type IKT- tjeneste eller funksjon som er satt bort, til kompetent myndighet. I tillegg skal foretakene informere den kompetente myndigheten i rimelig tid om planlagte IKT-tjenesteavtaler, forutsatt at avtalen er kritisk eller viktig.

Før et foretak inngår en leverandøravtale, stilles det krav til hva foretaket må ha foretatt seg på forhånd, blant annet due diligence av leverandøren. Videre legges det en begrensing på foretakene, ved at de kun kan inngå kontrakter med leverandører som etterlever adekvate informasjonssikkerhetsstandarder. Dersom det er tale om en kritisk eller viktig IKT-tjeneste, må leverandøren etterleve de beste og nyeste standardene. Når det gjelder foretakenes rett til tilgang, inspeksjoner og revisjon, er det lagt opp til at foretakene skal ha en risikobasert tilnærming, hvor hyppigheten av revisjoner og inspeksjoner, samt hvilke områder som skal revideres skal være forhåndsdefinert. Foretaket skal verifisere at revisor har tilstrekkelig kunnskap og evner til å gjennomføre IKT-revisjoner og vurderinger.

Ved inngåelse av leverandøravtale skal foretaket i visse definerte tilfeller sikre adgang til oppsigelse av avtalen. Hvis det er tale om en kritisk eller viktig avtale, skal foretaket sikre en uttredelsesstrategi (exit-strategi) og det stilles krav til hva denne må inneholde. Det stilles også krav til at finansforetaket skal sikre muligheten til å tre ut av en leverandøravtale, uten at dette går ut over finansforetakets kontinuitet, både i forhold til drift og ytelse av tjenester ovenfor kunder og etterlevelse av regelverk. Planene for uttredelse skal være dekkende, veldokumenterte og skal testes og revurderes jevnlig. Foretakene skal kartlegge alternative løsninger og overgangsordninger, slik at den virksomheten som er satt bort til leverandør, med tilhørende data, kan overføres til en alternativ leverandør eller tilbake til egen virksomhet. Foretakene skal også ha adekvate beredskapsordninger for å sikre kontinuitet ved en uttredelse av kontrakt.

Forut for inngåelse av kritiske eller viktige IKT-tjenesteavtaler skal foretaket vurdere om avtalen vil føre til at man inngår en avtale med en aktør som er vanskelig å erstatte eller om flere tjenester er konsentrert hos samme leverandør, eller leverandører som har et tett samarbeid. Foretakene skal også gjøre en kost-nytte-vurdering i forhold til alternative leverandører og muligheten for at leverandør for kritiske/viktige tjenester benytter underleverandører. Som en del av risikovurderingen skal foretaket ta stilling til om IKT-tjenesteavtaler medfører komplekse verdikjeder.

Forordningen stiller krav til utforming av avtalen. Avtalen skal være skriftlig. Videre skal partenes rettigheter og plikter være tydelig fordelt. Avtalen skal også inneholde krav til tjenestekvalitet. For øvrig stilles det flere minimumskrav til innholdet i kontrakten. I kontraktsforhandlingene skal foretaket vurdere bruk av standard kontraktsbestemmelser utarbeidet av offentlige myndigheter.

Overvåkingsrammeverk for kritiske tredjepartstilbydere av IKT-tjenester

ESAene skal, gjennom deres felles komite og på anbefaling fra overvåkingsforumet (som skal etableres), vurdere og utpeke hvilke IKT-tjenesteleverandører som er kritiske for foretakene, ut ifra gitte kriterier. Felleskomiteen skal også utpeke hvilken ESA som skal være ansvarlig for overvåking (hovedovervåker) av den enkelte kritiske tjenesteleverandør, ut ifra gitte kriterier. Hvert år skal en oppdatert liste over kritiske tjenesteleverandører publiseres.

Det er gitt regler for strukturen av overvåkingsrammeverket, hvilke oppgaver den ansvarlige overvåkeren skal ha, samhandling mellom ansvarlige overvåkere, hvilken kompetanse hovedovervåkeren skal ha og hvordan denne skal utøves. I tillegg er det gitt regler for hovedovervåkerens anledning til å innhente informasjon og hvilke undersøkelser som kan gjennomføres. Hovedovervåkeren kan foreta inspeksjon hos en utpekt tjenesteleverandør og det er regulert nærmere hva overvåkeren kan foreta seg.

Ved tilsynet skal den ansvarlige overvåkeren assisteres av en gruppe bestående av ESAene og relevante kompetente myndigheter hvor finansforetak hører hjemme. I tillegg kan den nasjonale kompetente myndigheten i henhold til NIS2-direktivet (EU 2022/2555) og en kompetent myndighet fra landet den kritiske leverandøren hører hjemme delta på frivillig basis.

Tjenesteleverandøren skal innen 60 dager etter en undersøkelse eller inspeksjon, opplyse hovedovervåkeren om hensikten til å følge opp anbefalinger, eventuelt grunngi valg om å ikke følge anbefalingene. Tilbakemeldingen fra tjenesteleverandør skal umiddelbart videreformidles til de kompetente myndighetene.

Regelverket legger opp til at kritiske tjenesteleverandører skal betale avgift for å dekke den ansvarlige overvåkerens utgifter i forbindelse med tillagte oppgaver. Det legges også opp til muligheten for å inngå samarbeid med tilsynsmyndigheter i tredjeland.

Kapittel VI – Ordninger for informasjonsdeling

Regelverket legger opp til at foretakene kan dele informasjon om cybertrusler seg imellom, forutsatt at delingen vil styrke digital motstandsdyktighet for foretakene og at kommunikasjonen skjer i et anerkjent miljø. Foretakene skal underrette kompetent myndighet om deltakelse i slike ordninger for informasjonsdeling. Det antas at NFCERT er et slikt type miljø.

Kapittel VII – Kompetente myndigheter

Reglene i kapitlet angir hvem som er kompetent tilsynsmyndighet.

I henhold til NIS 2-direktivet ((EU) 2022/255)) skal det dannes en samarbeidsgruppe (heretter Samarbeidsgruppen) for å legge til rette for samarbeid og utveksling av informasjon mellom medlemslandene. I DORA legges det opp til at ESAene og kompetente myndigheter kan delta i Samarbeidsgruppen, når det gjelder tilsynsaktiviteter i forbindelse med finansforetak. Målet er å fremme samarbeid og erfaringsutveksling mellom kompetente myndigheter, i henhold til DORA, og Samarbeidsgruppen. Videre legges det opp til at myndigheter skal samarbeide seg imellom. Relevant informasjon vedrørende kritiske IKT-leverandører skal utveksles mellom den kompetente og den overordnede tilsynsmyndigheten.

Det gis adgang til at til ESAene, gjennom JC og i samarbeid med kompetente myndigheter m.fl., kan etablere ordninger for å muliggjøre erfaringsutveksling vedrørende praksis i den finansielle sektoren. Målet er å fremme økt bevissthet samt identifisere felles sårbarheter og risikoer på tvers av sektorer. Videre legges det opp til at det kan gjennomføres felles øvelser i krisehåndtering og beredskap ved cyberangrep. Øvelsene skal ta sikte på å utvikle kommunikasjonskanaler og legge til rette for en effektiv og koordinert håndtering på EU-nivå, skulle en grensekryssende IKT-hendelse eller tilhørende trusler med påvirkning på det europeiske finansielle systemet oppstå.

Regelverket gir den kompetente myndigheten myndighet til å føre tilsyn med, undersøke og sanksjonere foretakene, i den grad det er nødvendig for å gjennomføre forordningen. Medlemslandene skal innføre regler for adekvate administrative reaksjoner og gjenopprettende tiltak ved brudd på bestemmelser i forordningen. Reaksjonene skal være effektive, proporsjonale og preventive. Medlemslandene står fritt til å innføre strafferettslige sanksjoner i nasjonal rett.

Medlemslandene skal meddele hvordan bestemmelsene i dette kapittelet implementeres, i lov, forskrift og rundskriv, til Kommisjonen, ESMA, EBA og EIOPA. Videre gis det bestemmelser om hvordan kompetente myndigheter skal publisere administrative reaksjoner.

Konfidensiell informasjon tilegnet i forbindelse med forordningen skal underlegges profesjonell taushetsplikt. Det gis også bestemmelser om når ESAene og den kompetente myndigheter kan behandle persondata.

Kapittel VIII – Delegeringer

Kommisjonen er gitt myndighet til å vedta delegerte forordninger under visse forutsetninger. Delegeringen av myndighet kan når som helst trekkes tilbake av Europaparlamentet eller Kommisjonen.

Kapittel IX – Overgangsbestemmelser (samt endringer til eksisterende forordninger)

Innen fem år etter at forordningen trer i kraft skal Kommisjonen evaluere den. Det er lagt føringer på hva evalueringen skal inneholde. Innen tre år etter at forordningen trer i kraft skal Kommisjonen vurdere og rapportere behovet for forsterkede krav til standarder for revisorer og revisjonsfirmaer i forhold til digital motstandsdyktighet, ved et lovforslag.

Kapittelet inneholder også endringer i følgende forordninger:

Kortnavn	**Referanse**
CRA	(EF) 1060/2009
EMIR	(EU) 648/2012
CSDR	(EU) 909/2014
MiFIR	(EU) 600/2014
BMR	(EU) 2016/2011

Om tekniske standarder og retningslinjer

I forordningen framgår det at det skal utarbeides en rekke retningslinjer, regulatoriske tekniske standarder og implementeringstekniske standarder, m.m. Standardene er omtalt samlet grunnet det store antallet. I vedlagte bilder følger en oversikt over arbeidsgrupper i JC og hvilke retningslinjer og standarder, samt andre leveranser, som skal utarbeides og hvilket organ som er ansvarlig for den enkelte standard.

De regulatoriske tekniske standardene og implementeringstekniske standardene er nivå 2-regelverk og vil reguleres i form av delegerte kommisjonsforordninger.

Forordning (EU) 2022/2554 (DORA) om digital operasjonell motstandsdyktighet i finanssektoren krever tilpasninger i flere direktiver. Tilpasningene fremgår av direktiv (EU) 2022/2556 (DORA-direktivet). Følgende direktiver endres:

Kortnavn	**Referanse**
Solvens II	2009/138/EF
UCITS	2009/65/EF
AIFMD	2011/61/EU

CRD	2013/36/EU
BRRD	2014/59/EU
MIFID II	2014/65/EU
PSD II	(EU) 2015/2366
IORP II	(EU) 2016/2341

Vurdering

DORA vil gi gevinster, da regelverket bidrar til å harmonisere IKT-regelverket i finanssektoren, slik at det vil bli enklere å forholde seg til hva som er gjeldende rett på det digitale området. Når reglene foreligger i kraft av én forordning fremfor dagens regulering i form av diverse lover, forskrifter og retningslinjer, antas det at krav til foretakenes arbeid med IKT-sikkerhet får større oppmerksomhet i foretakene.

Regelverket er utformet med tanke på å beskytte foretakene, kundene og samfunnet for øvrig, noe som skaper trygghet ovenfor og tillit til den finansielle sektoren. Trygghet og tillit kombinert med forhåpentligvis færre vellykkede alvorlige angrep og hendelser vil også bidra til stabilitet i den finansielle sektoren og samfunnet ellers.

Rettslige konsekvenser

I finanssektoren gjelder IKT-forskriften for foretaks IKT-virksomhet, med unntak av verdipapirsentraler. I tillegg finnes IKT-relaterte bestemmelser i enkelte sektorregelverk. Bestemmelsene i IKT-forskriften og annet sektorregelverk tilsvarer i stor grad DORAs bestemmelser.

DORA er en forordning, hvilket innebærer at den som utgangspunkt skal inntas direkte i norsk lovgivning. Det må også tas stilling til behov for endringer i lovbestemmelser og forskriftsbestemmelser, da DORA-forordningen krever endringer i flere direktiver og andre forordninger.

DORA regulerer foretakenes meldeplikt for inngåtte IKT-tjenesteavtaler. Meldepliktforskriften (forskrift av 15. september nr. 2777) dekker hovedsakelig denne. Det kan imidlertid oppstå behov for tilpasninger, som sannsynligvis vil kunne implementeres ved endring av forskriften.

I forbindelse med innlemmelse av forordningen i EØS-avtalen må det vurderes om det skal gjøres tekniske eller materielle tilpasninger, blant annet for å sikre samarbeid mellom EBA, ESMA, EIOPA og ESA (EFTAs overvåkningsorgan). Det må også blant annet gjøres tilpasninger slik at myndigheten EBA, ESMA og EIOPA har til å fatte bindende vedtak(i henhold til artikkel 31, 33, 35-39, 42 og 43) ovenfor fysiske og juridiske personer etablert i Eus medlemsstater, legges til ESA for fysiske og juridiske personer etablert i EFTA-statene.

De regulatoriske tekniske standardene som utarbeides i tilknytning til DORA er nivå 2-regelverk, er også EØS-relevante og må implementeres i norsk lovgivning. Dette vil kunne gjøres i form av forskrift.

Økonomiske og administrative konsekvenser

DORA introduserer en rekke krav til rapportering, som vil få konsekvenser for den kompetente myndigheten og foretak under tilsyn. Noe rapportering foreligger allerede i dag, blant annet på hendelser og IKT-tjenesteavtaler, men DORA legger i mange tilfeller opp til en mer omfattende

rapportering. Rapporteringen vil medføre økt oppfølging fra den kompetente myndighetens side ovenfor foretakene. I tillegg økes rapportering til EU.

DORA er et komplekst regelverk med mange detaljer. Både for foretakene og tilsynsmyndigheten vil regelverket være krevende å forvalte. For tilsynsmyndigheten vil det bety et mer omfattende tilsynsansvar og mulig større behov for veiledning ovenfor foretakene.

Per i dag samarbeider Finanstilsynet med NSM og Datatilsynet. DORA kan medføre at slikt samarbeid må utvides. Dette vil muligens medføre økt ressursbruk i NSM og Datatilsynet også.

Det er noe vanskelig å si hvor krevende det blir å følge opp regelverket praksis, men sannsynligvis vil det bli behov for noe økte ressurser, både i foretakene og hos myndigheter. De regulatoriske tekniske standardene utgjør sammen med DORA et større sett med regler, med et høyere detaljnivå enn dagens regelverk og retningslinjer. Derfor vil de samlet kreve ytterligere ressurser å forvalte. I tillegg forventes det nye regelverket å medføre økt behov for samhandling med andre lands tilsynsmyndigheter. I Norge vil Finanstilsynet hovedsakelig være kompetent myndighet.

Sakkyndige instansers merknader

Finanstilsynet vurderer at DORA bør innføres ved lov. Finanstilsynet har vurdert saken vurderer rettsakten til å være EØS-relevant og akseptabel. Gjennomføringen i norsk rett innebærer endring i direktivene 2009/138/EF, 2011/61/EU, 2014/65/EU, (EU) 2015/2366 og (EU) 2016/2341, som er gjennomført i lov. Det tas derfor forbehold om Stortingets samtykke etter EØS-avtalens artikkel 103.

32022L2556 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

Direktivet medfører endringer i direktiver som er gjennomført i lov, derfor tas det forbehold om Stortingets samtykke.

Status

Rettsakten trådte i kraft i EU 17.01.2025.

Forordningen er til vurdering i EØS/EFTA-landene for innlemmelse i EØS-avtalen.

Et høringsforslag utarbeidet av finanstilsynet var på høring våren 2024.

Sammendrag av innhold

Forordning (EU) 2022/2554 (DORA) om digital operasjonell motstandsdyktighet i finanssektoren krever tilpasninger i flere direktiver. Tilpasningene fremgår av Direktiv (EU) 2022/2556 (DORA-direktivet). Følgende direktiver endres:

Kortnavn	**Referanse**
Solvens II	2009/138/EF
UCITS	2009/65/EF
AIFMD	2011/61/EU
CRD	2013/36/EU
BRRD	2014/59/EU
MIFID II	2014/65/EU
PSD II	(EU) 2015/2366
IORP II	(EU) 2016/2341

Merknader

Rettslige konsekvenser

Endringsbestemmelsene i DORA-direktivet innebærer at IKT-risikostyring og kravene som vil gjelde etter (DORA) tas inn i bestemmelser om forsvarlig organisering og drift av virksomheten. Endringene gjelder virksomhetskravene for finansforetak, betalingsforetak, verdipapirforetak, regulerte markeder og forvaltere av verdipapirfond og alternative investeringsfond, samt justeringer i kravene til innhold i gjenopprettings- og krisehåndteringsplaner for kredittinstitusjoner mv. Endringene innebærer i seg selv ingen nye materielle forpliktelser utover de som vil følge av forordningen. Gjennomføringen i norsk rett innebærer endring i de overnevnte direktivene, herunder

2009/138/EF, 2011/61/EU, 2014/65/EU, (EU) 2015/2366 og (EU) 2016/2341, som er gjennomført i lov. Det tas derfor forbehold om Stortingets samtykke etter EØS-avtalens artikkel 103.

Økonomiske og administrative konsekvenser

DORA introduserer en rekke krav til rapportering, som vil få konsekvenser for den kompetente myndigheten og foretak under tilsyn. Noe rapportering foreligger allerede i dag, blant annet på hendelser og IKT-tjenesteavtaler, men DORA legger i mange tilfeller opp til en mer omfattende rapportering. Rapporteringen vil medføre økt oppfølging fra den kompetente myndighetens side ovenfor foretakene. I tillegg økes rapportering til EU.

DORA er et komplekst regelverk med mange detaljer. Både for foretakene og tilsynsmyndigheten vil regelverket være krevende å forvalte. For tilsynsmyndigheten vil det bety et mer omfattende tilsynsansvar og mulig større behov for veiledning ovenfor foretakene.

Per i dag samarbeider Finanstilsynet med NSM og Datatilsynet. DORA kan medføre at slikt samarbeid må utvides. Dette vil muligens medføre økt ressursbruk i NSM og Datatilsynet også.

Det er noe vanskelig å si hvor krevende det blir å følge opp regelverket praksis, men sannsynligvis vil det bli behov for noe økte ressurser, både i foretakene og hos myndigheter. De regulatoriske tekniske standardene utgjør sammen med DORA et større sett med regler, med et høyere detaljnivå enn dagens regelverk og retningslinjer. Derfor vil de samlet kreve ytterligere ressurser å forvalte. I tillegg forventes det nye regelverket å medføre økt behov for samhandling med andre lands tilsynsmyndigheter. I Norge vil Finanstilsynet hovedsakelig være kompetent myndighet.

Sakkyndige instansers merknader

Finanstilsynet har vurdert saken vurderer rettsakten til å være EØS-relevant og akseptabel.

Vurdering

Endringene innebærer ingen nye materielle forpliktelser utover de som vil følge av DORA.

32023R1114 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

Status

Rettsakten trådte i kraft i EU 30. desember 2024. Forordningen er nå aktuell for innlemmelse i EØS-avtalen. **Ettersom gjennomføring av rettsakten krever lovendringer, tas det forbehold om Stortingets samtykke.**

Et høringsnotat utarbeidet av Finanstilsynet med forslag til gjennomføring av forordningen i en ny lov om kryptoeiendeler var på høring våren 2024.

Sammendrag av innhold
Forordningen inneholder felleseuropeiske regler om utstedelse, offentlig tilbud og opptak til handel av kryptoeiendeler, ytelse av tjenester knyttet til kryptoeiendeler og om markedsmisbruk i kryptoeiendelsmarkedet. Reglene skal blant annet bidra til å fremme innovasjon, investorbeskyttelse og markedsintegritet, samt sikre finansiell stabilitet. Forordningen utvider definisjonen av hva som utgjør en tjenestetilbyder for virtuell valuta, både utover det som følger av hvitvaskingsregelverket i dag (i Norge og EU), og utover standardene til Financial Action Task Force (FATF). Gjennomføringen i norsk rett innebærer lovendring. Det tas derfor forbehold om Stortingets samtykke etter EØS-avtalens artikkel 103.

Kryptoeiendeler er i forordningen definert som en digital representasjon av en verdi eller en rettighet som kan overføres og oppbevares elektronisk ved bruk av distribuert registerteknologi eller lignende teknologi.

Forordningen regulerer tre hovedkategorier kryptoeiendeler:

- kryptoeiendeler som er en form for e-penger, ved at det anføres at de har en stabil verdi relatert til én offisiell valuta (e-pengetoken)

- eiendelsbaserte kryptoeiendeler som anføres å ha en stabil verdi relatert til andre verdier eller rettigheter, eller kombinasjoner av slike, for eksempel offisielle valutaer og ulike investeringsobjekter (eiendelsbaserte token)

- andre kryptoeiendeler.

For kryptoeiendeler som ikke er e-pengetoken eller eiendelsbaserte token, stiller forordningen krav til de som tilbyr kryptoeiendelene til offentligheten, de som søker om at kryptoeiendelen tas opp til handel på en handelsplattform, og handelsplattformer som tar opp kryptoeiendelene til handel på eget initiativ. Et sentralt krav i denne forbindelse er at det skal utarbeides et informasjonsdokument som skal gi potensielle investorer informasjon om egenskaper, funksjoner og risikoer ved kryptoeiendelene.

Utstedelse av eiendelsbaserte token vil etter forordningen være underlagt krav om tillatelse fra nasjonale tilsynsmyndigheter, unntatt der utsteder er en kredittinstitusjon. Forordningen stiller krav til utstederes organisering og opptreden, herunder utarbeidelse av informasjonsdokument.

Utstedelse av e-pengetoken vil i utgangspunktet bare kunne gjøres av kredittinstitusjoner og e-pengeforetak. Også for e-pengetoken er det krav til utarbeidelse av informasjonsdokument.

Utstedere av e-pengetoken og eiendelsbaserte token som vurderes som signifikante etter nærmere kriterier, vil være underlagt tilsyn av Den europeiske banktilsynsmyndigheten (EBA).

Forordningen regulerer også ytelse av kryptoeiendelstjenester. Kryptoeiendelstjenesteytere må i utgangspunktet ha tillatelse av nasjonale myndigheter etter forordningen, eller de må ha tillatelse til å yte nærmere angitte finansielle tjenester og ha sendt melding til tilsynsmyndigheten. Forordningen stiller nærmere krav til organiseringen og virksomheten til kryptoeiendelstjenesteytere.

Videre inneholder forordningen regler om forebygging av, og forbud mot, markedsmisbruk i tilknytning til kryptoeiendeler, herunder innsidehandel og markedsmanipulasjon. Reglene har likhetstrekk med de tilsvarende reglene som gjelder for finansielle instrumenter.

Tjenestene som reguleres av kryptoeiendelsforordningen vil kunne tilbys grensekryssende i EØS. Det gis også nærmere regler om tilsyn og administrative sanksjoner, som har mange likhetstrekk med reguleringen på verdipapirområdet.

Merknader

Rettslige konsekvenser

MiCA er en forordning, hvilket innebærer at den som utgangspunkt skal inntas direkte i norsk lovgivning. Når regelverket er innlemmet i EØS-avtalen, vil det bli gjennomført i norsk rett ved inkorporasjon. Det vil si at det i norsk lov eller forskrift fastsettes at forordningen gjelder som norsk rett.

Økonomiske og administrative konsekvenser

Kryptoeiendelsforordningen innebærer en strengere regulering av kryptoeiendelsmarkedet enn gjeldende rett, noe som ventes å bedre investorbeskyttelsen i dette markedet. Dette vil samtidig medføre økte kostnader for aktører som ønsker å yte kryptoeiendelstjenester eller utstede eiendelsbaserte token eller e-pengetoken. Den nasjonalt utpekte tilsynsmyndigheten vil også få omfattende nye tilsynsoppgaver knyttet til kryptoeiendelsmarkedet. Kostnadene knyttet til dette må utlignes på markedsaktørene.

Sakkyndige instansers merknader

Finanstilsynet har vurdert forslaget som EØS-relevant og akseptabelt.

Vurdering

Forordningen antas ikke å stride mot norske interesser eller andre internasjonale forpliktelser. Finanstilsynet finner rettsakten EØS-relevant og akseptabel.

I forbindelse med innlemmelse av forordningen i EØS-avtalen må gjøres tekniske eller materielle tilpasningstekster, blant annet for å legge tilsynet med norske utstedere av signifikante e-pengetoken og eiendelsbaserte token til EFTAs overvåkingsorgan.

Gjennomføring av forordningen i norsk rett krever lovendring. Forordningen vil derfor bli innlemmet i EØS-avtalen med forbehold om Stortingets samtykke.

32023R1113 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

Status
Forordningen trådte i kraft i EU 29. juni 2023 og vil få anvendelse i EU fra 30. desember 2024.

Forordningen er nå klar for innlemmelse i EØS-avtalen. **Ettersom gjennomføring av forordningen krever lovendring, tas det forbehold om Stortingets samtykke.**

Et høringsnotat utarbeidet av Finanstilsynet om gjennomføring i norsk rett har vært på høring våren 2024.

Sammendrag av innhold
20. juli 2021 presenterte EU-kommisjonen en pakke bestående av fire regelverksforslag med det formål å styrke EUs regler og innsats mot hvitvasking og terrorfinansiering (AML/CFT), herunder et forslag til revidert forordning (EU) 2015/849. Sistnevnte forslag er nå vedtatt og i kraft i EU i form av forordning (EU) 2023/1113.

Forordningen regulerer hvilke opplysninger som skal følge pengeoverføringer og visse kryptoeiendeler, og utvider rekkevidden av forordning (EU) 2015/847. Sistnevnte forordning gjelder pengeoverføringer, og med forordning (EU) 2023/1113 omfattes også overføringer av kryptoeiendeler foretatt av tilbydere av tjenester knyttet til kryptoeiendeler ("Crypto-Asset Service Providers"). Forordningen endrer videre direktiv (EU) 2015/849.

Tilbydere av tjenester knyttet til kryptoeiendeler som er avsender av en transaksjon må 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 kryptoeiendeler.

Tilbydere av tjenester knyttet til kryptoeiendeler som er mottaker av en transaksjon må bl.a. ha på plass effektive rutiner for å identifisere om tilstrekkelig informasjon følger transaksjonen.

Endringene i forordningen reflekterer FATF anbefaling 15 og anbefaling 16.

Merknader

Rettslige konsekvenser

Forordning (EU) 2015/847 er i dag gjennomført i forskrift til hvitvaskingsloven. Hvis forslaget tas inn i EØS-avtalen må henvisningen oppdateres.
Forordningen endrer også hvitvaskingsdirektivet, hvilket kan innebære at hvitvaskingsloven må endres.

Økonomiske og administrative konsekvenser

Forordningen oppstiller nye regler for tilbydere av tjenester knyttet til kryptoeiendeler. Bestemmelsene vil medføre økte økonomiske og administrative konsekvenser for slike aktører. Videre antas forordningen å medføre økonomiske og administrative konsekvenser for offentlige myndigheter.

Sakkyndige instansers merknader

Finanstilsynet finner rettsakten EØS-relevant og akseptabel.

Vurdering

Finanstilsynet finner rettsakten EØS-relevant og akseptabel.

Forordning (EU) 2015/847 er i dag gjennomført i forskrift til hvitvaskingsloven. Hvis forslaget tas inn i EØS-avtalen må henvisningen oppdateres.

Forordningen endrer også hvitvaskingsdirektivet, hvilket kan innebære at hvitvaskingsloven må endres.

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

Ingen.