FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

## EUs nye lovgivning om digital operasjonell motstandsdyktighet (Digital Operational Resilience Act)

# DORA

## VFFs Complianceseminar 19. oktober 2022

Olav Johannessen, Seksjonssjef tilsyn med IT og betalingstjenester

# "Digital Finance Strategy"

- Del av EUs Digital Finance Package  publisert 24. september 2020
- Digitalisering av finanstjenestene, redusert fragmentering, grensekryssende tjenester
- Lovgivningen skal
  - Stimulere til innovasjon, konkurranse og markedseffektivitet
  - Fremme datadeling og datadreven innovasjon
  - Stimulere til open finance
  - Sikre at nye utfordringer og risikoer håndteres
  - Sikre like vilkår: Samme aktivitet, Samme risiko, Samme regler

- Forslag til lov om krypto-eiendeler (MiCA)
  - Utnytte muligheter og redusere risiko som ligger i kryptoverdier
- Forslag til lov om digital operasjonell motstandsdyktighet (DORA) + endringsbestemmelser
  - Redusere (konsekvensen av) digitale angrep og andre risikoer
  - Håndtere alle typer driftsforstyrrelser

# Digital Operational Resilience Act (DORA)

- Del av EUs Digital Finance Strategy
- Nye utfordringer og risikoer som er forbundet med den digitale omstillingen skal håndteres
- Forslag til lov om digital operasjonell motstandsdyktighet (DORA)
  - Felles regelverk
  - Teknologiselskaper
  - Sikkerhetstiltak
  - Digitale angrep og andre risikoer
  - Driftsforstyrrelser
- EØS-notat i EØS-notatbasen
- Regelverkforslaget EØS-relevant

# Endringsbestemmelser - Direktiv

- Forordningen skal «monteres» inn i en rekke direktiver
- Endring i operasjonelle risiko- eller risikostyringskrav i direktivene

**Krysshenvisninger**

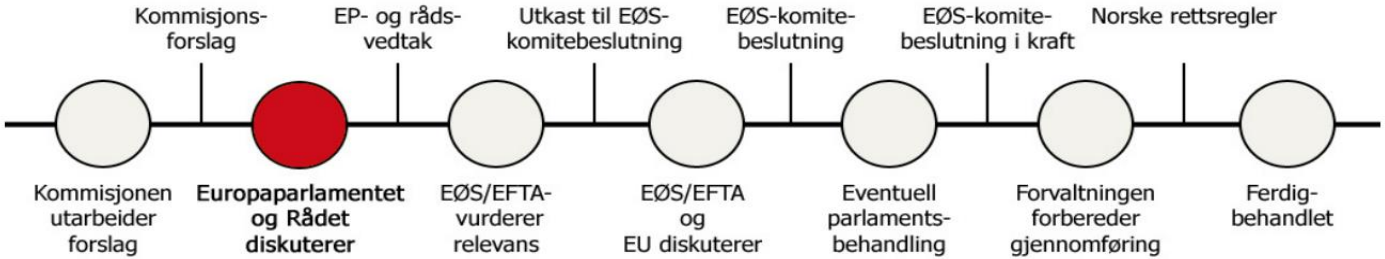
| | |
|---|---|
| 2009/65/EC | UCITS, kollektiv investering i omsettelige verdipapirer |
| 2009/138/EU | SOLVENS II, forsikring og reassuranse |
| 2011/61/EU | AIFMD, alternative investeringsfondforvaltere |
| EU/2016/2341 | IORP - tjenestepensjon |

**IKT-relaterte bestemmelser**

| | |
|---|---|
| EU/2013/36 | CRD, Kapitaldekning - banker mm - |
| 2014/65/EU | MIFID2 - finansielle instrumenter |
| (EU) 2015/2366 | PSD2 – betalingstjenester og -foretak |

- Samtidig implementering

# Prosessen med fastsettelse av regelverket i norsk rett




- *Rettslige konsekvenser*
  Dersom forslaget blir vedtatt i EU og vurdert for innlemmelse i EØS-avtalen er det nærliggende å anta at reglene forslaget legger opp til må implementeres i lov ved henvisning
- *Økonomiske og administrative konsekvenser*
  Eksisterende regelverk som i dag praktiseres ligger tett opp til kravene som stilles i regelverksforslaget. Det er derfor lite trolig at det vil medføre større økonomiske og administrative kostnader.
- *Sakkyndige instansers merknader*
  Finanstilsynet har vurdert regelverkforslaget som EØS-relevant og akseptabelt.
- ***Vurdering***
  Når regelverket er endelig vedtatt må det vurderes hvorvidt det vil være behov for materielle eller tekniske tilpasninger før rettsakten kan innlemmes i EØS-avtalen.

# Aktuelle lenker

**DORA**

- https://www.europalov.no/rettsakt/eu-rammeverk-for-digitale-finansielle-tjenesters-operasjonelle-motstandsdyktighet/id-28358
- https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2020/des/forslag-til-forordning-om-digital-operasjonell-motstandsdyktighet-i-finanssektoren/id2791266/

**Endringsbestemmelser knyttet til kryptoaktiva og operasjonell sikkerhet**

- https://www.europalov.no/rettsakt/digital-finans-endringsbestemmelser-knyttet-til-kryptoverdier-operasjonell-sikkerhet/id-28360
- https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2020/des/digital-finans-forslag-til-endringsbestemmelser-knyttet-til-kryptoaktiva-og-operasjonell-sikkerhet/id2791267/

# Momenter

- EØS-relevant og akseptabelt
- DORA-regelverket
- Tilpasningsregelverk
- Virkeområde
- IKT-forskriften
- Verdipapirsentraler
- Antatt ikraftredelsestidspunkt - begynnelsen av 2025
- Samtidig (førtidig) implementering i norsk rett
- Pågående arbeider i ESAene
- Oversight leverandører

# DORA versus IKT-forskriften

| DORA | IKT-forskriften |
|---|---|
| Governance | § 2 Organisering |
| Styring av IKT-risiko | § 3 Risikoanalyse, § 5 Sikkerhet,<br>§ 8 Drift, § 11 Driftsavbrudd og kriseberedskap |
| Rapportering av større IKT-relaterte hendelser | § 9 Avviks- og endringshåndtering |
| Testing av digital operasjonell motstandsdyktighet | § 11 Driftsavbrudd og kriseberedskap |
| Utkontraktering, tredjeparts IKT-risiko og overvåkningsrammeverk | § 12 Utkontraktering |
| Deling av informasjon og etterretning ift. cybertrusler og sårbarheter | Samhandling med/gjennom NFCERT |
| *Bestemmelser for myndighetene, bl.a. sektorovergripende beredskapstesting og sanksjoner* | |

# Nærmere om regelverket

**Hensikt**

- Teknologiselskaper stadig viktigere, både som IT-leverandører for finansforetak og som leverandører av finansielle tjenester
- DORA skal sikre at alle deltakere i det finansielle systemet har de nødvendige tiltak på plass for å redusere cyberangrep og andre risikoer

**Bredt omfang av foretakstyper omfattes**

- (j) managers of alternative investment funds (AIF)
- (k) management companies, (Fondsforvaltere (UCITS))

**Proporsjonalitet**

- Størrelse
- Forretningsprofil
- Risikoprofil
- ……

# Virkeområdet

a) credit institutions,
(b) payment institutions, including payment institutions exempted in accordance with Article 32 (1) of Directive (EU) 2015/2366, (ba) account information service providers,
(c) electronic money institutions, including electronic money institutions exempted in accordance with Article 9 (1) of Directive 2009/110/EC,
(d) investment firms,
(e) crypto-asset service providers as authorized under MiCA and issuers of assetreferenced tokens,
(f) central securities depositories,
(g) central counterparties,
(h) trading venues,
(i) trade repositories,
(j) managers of alternative investment funds,
(k) management companies,
(l) data reporting service providers,
(m) insurance and reinsurance undertakings,
(n) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries,
(o) institutions for occupational retirement provision,
(p) credit rating agencies,
(q)
(r) administrators of critical benchmarks,
(s) crowdfunding service providers,
(t) securitisation repositories,
(u) ICT third-party service providers.

# Nærmere om regelverket

## Krav til styring og kontroll (Governance)

- Krav til sammenheng forretningsstrategi og IKT-strategi
- Krav til etablering av rammeverk for styring av IKT-risiko
- Krav til tydelige roller og ansvar

## Krav til styring av IKT-risiko

- Rammeverk for styring av IKT-risiko
- Krav til risikoanalyser
- Krav til rammeverk for IKT-sikkerhet, sikkerhetstiltak og sikkerhetsovervåkning
- Krav til beredskapsplaner og katastrofe- og gjenopprettingsplane

## Rapportering av IKT-hendelser

- Krav til prosesser for overvåking, registrering, klassifisering og rapportering av hendelser
- Krav til initiale, foreløpige og endelige rapporter
- Krav til informasjon til kunder og brukere
- Krav til dialog med myndighetene ved større hendelser

# Nærmere om regelverket

## Testing av digital operasjonell motstandsdyktighet

- Felles regelverk viktig for grensekryssende virksomheter
- Alle skal teste regelmessig, *(jf. krav i IKT-forskriftens § 11 Driftsavbrudd og kriseberedskap)*
- Testkravene høyere for "signifikante" foretak
- Kun "signifikante" foretak vil bli krevd å gjennomføre såkalt avansert testing (TLPT) etter foreslått regelverk
  - Noen  områder viktigere enn andre: Eks. Betaling, banker, avregning og oppgjør
  - Minimum hvert tredje år
  - Minimum kritiske funksjoner og tjenester
  - Scope skal valideres av tilsynsmyndigheten(e)
  - Resultat skal forelegges tilsynsmyndigheten(e), valideres og utstede attest

# Nærmere om regelverket

## Tredjeparts IKT-risiko

- Risiko som oppstår gjennom IKT-leverandører
- Krav til styring og kontroll med IKT-leverandører og leverandør-risiko, inkl. inngåelse og terminering (exit-planer) av avtaler
- Krav til kontraktene, bl.a. sikkerhetskrav, ytelseskrav, gjenopprettingskrav, rapporteringsforpliktelser og rett til informasjon, inspeksjon og revisjon

- Kritiske leverandører underlegges et rammeverk for felles overvåkingstilsyn
- Ledes av de overnasjonale tilsynsmyndighetene

## Informasjonsdeling

- Mål er å øke bevisstheten om IKT-risiko, øke defensive evner og evne til trussel detektering
- Finansielle foretak etabler samhandlingsordninger for å utveksle informasjon om cybertrusler og etterretning mellom seg

❖ **Bestemmelser for myndighetene, bl.a. sektorovergripende beredskapstesting og sanksjoner**

# Utarbeiding Nivå 2 regelverk iht DORA

| | | 01-Sep-23 | 01-Mar-24 | 01-Sep-24 | 01-Mar-25 | 01-Sep-25 |
|---|---|---|---|---|---|---|
| 1 | RTS on ICT risk management framework (art.14) | | ● | | | |
| 2 | RTS on simplified ICT risk management framework (art. 14a.3) | | ● | | | |
| 3 | RTS to specify threat led penetration testing aspects (art. 23.4a-c) | | | ● | | |
| 4 | RTS to specify the policy on ICT services (art. 25.11) | | ● | | | |
| 5 | RTS to specify elements when sub-contracting critical or important functions (art. 27.4) | | | ● | | |
| 6 | RTS on criteria for the classification of ICT-related incidents (art. 16.2) | | ● | | | |
| 7 | RTS on specifying the reporting of major ICT-related incidents (art. 18.1a) | | | ● | | |
| 8 | ITS to establish the reporting details for major ICT-related incidents (art. 18.1b) | | | ● | | |
| 9 | Guidelines on the estimation of aggregated annual costs/losses caused by major ICT incidents (art. 10.9a) | | | ● | | |
| 10 | Feasibility report for establishing a single EU Hub for major ICT-related events (art. 19.1) | | | | ● | |
| 11 | ESRB recommendation A1 + A2 + B | ● | | ● | | ● |
| 12 | ITS to establish the templates for the Register of information (art. 25.10) | | ● | | | |
| 13 | GL on cooperation between ESAs and CAs regarding the structure of the oversight (art. 29.5) | | | ● | | |
| 14 | RTS to specify information on oversight conduct (art. 36.1) | | | ● | | |

# Pågående kartlegging vedr bruk av IKT-leverandører

- Innsamling av utkontrakteringsinformasjon ved bruk av felles mal ESMA, EIOPA, EBA
- Utvalgte foretak innenfor alle områder tilskrevet
  - Verdipapir, fond, bank, forsikring, betaling mv
- Informasjonen hjelp til å utarbeide RTS/ITS for krav til informasjon i leverandørregister
- Bidra til å etablere kriteria for utvelgelse kritiske leverandører og identifisere disse
- Gi en oversikt over type IKT-tjenester leverandører tilbyr

# Organisering av arbeidet

- Etablering av en sub-gruppe under JC / ESA
- Undergrupper skal jobbe med de forskjellige nivå 2 mandatene
- Deltakelse fra
    - ESAene (ESMA / EIOPA / EBA)
    - ECB
    - Nasjonale tilsynsmyndigheter
    - Observatører fra div. EU organer, eks. ENISA

FINANSTILSYNET

THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY