EU Forslag

Digital Operational Resilience Act (DORA)

Ny regulering knyttet til digitalt forsvar for finansnæringen

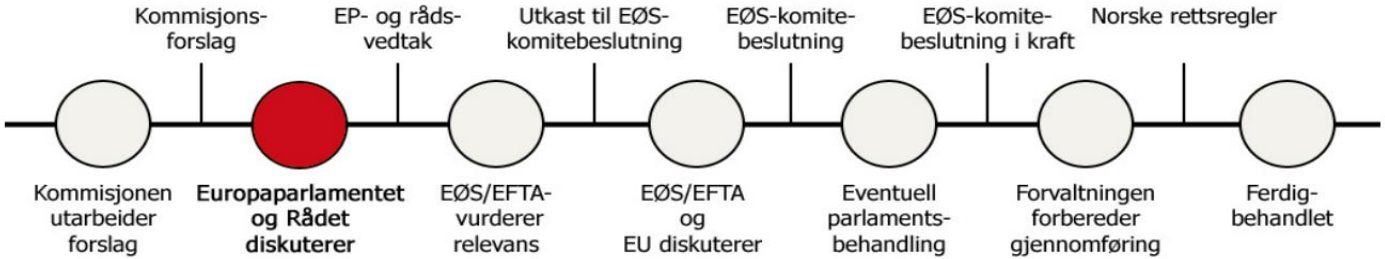
Digital Operational Resilience Act (DORA)

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)
  - Redusere (konsekvensen av) digitale angrep og andre risikoer
  - Håndtere alle typer driftsforstyrrelser

Prosessen med fastsettelse av regelverket



- *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.

DORA versus IKT-forskriften

DORA	IKT-forskriften
Governance	§ 2 Organisering
Styring av IKT-risiko	§ 3 Risikoanalyse, § 5 Sikkerhet, § 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

Proporsjonalitet

- Ved utarbeidelsen av regelverket er det lagt til grunn at det er betydelige forskjeller mellom foretak når det gjelder størrelse, forretningsprofiler og foretakenes eksponering for digital risiko.

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

FINANSTILSYNET

THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY