DORA – ny EU-forordning rettet mot finanssektoren

Digital Operational Resilience Act (DORA) er en ny EU-forordning rettet mot finanssektoren som stiller nye og strengere krav til hvordan foretakene som omfattes, skal arbeide for å sikre digital robusthet. Forordningen vil omfatte en stor del av foretakene som i dag er underlagt IKT-forskriften.

Legal & Privacy Officer
Andreas Forbech Havre
Intility

Berørte foretak burde derfor allerede nå starte arbeidet med å avklare hvilke områder de må forbedre seg på før det nye regelverket trer i kraft.

Bakgrunn og formål

Etter en lengre periode med digitalisering av samfunnet, har den operasjonelle driften i økende grad blitt avhengig av informasjons- og kommunikasjonsteknologi. Digitaliseringen har ført til en effektivisering, men skaper også nye risikoer som gjør seg gjeldende på tvers av ulike bransjer. Det har vært flere eksempler på at cyberangrep og IKT-relaterte hendelser har forstyrret og påvirket den daglige driften til virksomheter og deres kunder. Når en hendelse først har funnet sted, har det vist seg at det kan få store konsekvenser og ta tid før driften er i gang igjen. Reguleringen av operasjonell motstandsdyktighet har også vært fragmentert. Videre har det vært ulike krav på tvers av landegrensene i EU.

Disse utfordringene behandler EU med et initiativ hvor man ønsker å styrke den digitale operasjonelle motstandsdyktigheten og robustheten ved ulike funksjoner i samfunnet. Samtidig ønsker man i større grad å harmonisere kravene, for å oppnå en mer konsistent og enhetlig regulering på tvers av det indre marked. Som en del av dette initiativet er DORA-forordningen vedtatt. Formålet med dette regelverket er at finanssektoren skal ha et høyt nivå av digital operasjonell motstandsdyktighet slik at kontinuitet og stabilitet sikres. Et annet eksempel på ny lovgivning fra EU er NIS2-direktivet. NIS2 stiller krav til det som kategoriseres som essensielle tjenester og andre viktige tjenester. Direktivet treffer derfor på tvers av ulike sektorer, som for eksempel både bank og finansmarkedenes infrastruktur, men også andre sektorer som avfallshåndtering. Noen virksomheter vil derfor omfattes av begge lovverkene. I en slik situasjon vil DORA som spesiallovgivning ha forrang foran NIS2-direktivet.

Sammenlignes med GDPR

DORA-forordningen føyer seg dermed inn i rekken av regulatoriske krav stilt mot finanssektoren. Den stiller en rekke krav til hva foretakene må implementere og gjennomføre i egen virksomhet, og blir gjerne sammenlignet med GDPR. Til tross for at DORA på mange måter er forholdvis konkret sammenlignet med annen lovgivning, vil det nok for mange oppstå noe usikkerhet om hva som kreves for å innfri kravene i forordningen. Hvilket nivå den enkelte virksomheten skal legge seg på i implementeringen og gjennomføringen av forpliktelsene i DORA, vil også variere. Forpliktelsene til den enkelte virksomhet må vurderes ut ifra en proporsjonalitetsvurdering hvor man blant annet tar hensyn til foretakets størrelse, risikoprofil og kompleksitet.

DORA i norsk rett

I EU vil forordningen tre i kraft i alle medlemslandene 17. januar 2025. Regelverket er av Finansdepartementet antatt å være EØS-relevant, og foreslått gjennomført i norsk rett gjennom ny lov om digital operasjonell motstandsdyktighet i finanssektoren. I forslaget legges det opp til at Finanstilsynet blir nasjonal tilsynsmyndighet for DORA. Tilsynet har gitt uttrykk for at det er forventet at DORA blir gjennomført i norsk rett uten vesentlige forsinkelser sammenlignet med EU. Norske virksomheter bør derfor belage seg på at DORA også i Norge trer i kraft 17. januar 2025. I forslaget legges det opp til at tilsynet kan ilegge overtredelsesgebyr på inntil 50 millioner kroner til fysiske personer eller foretak ved overtredelse av forordningen.

DORAs fem pilarer

1. Styring av IKT-risiko
2. Hendelseshåndtering og rapportering
3. Testing av motstandsdyktighet
4. Styring av leverandørrisiko
5. Informasjonsdeling om trusler og etterretning

Fem pilarer

De ulike kravene som følger av DORA, kan deles i fem overordnede pilarer:

1. Styring av IKT-risiko
   Foretakene som omfattes må implementere et rammeverk for IKT-risikostyring som en integrert del av virksomhetens overordnede risikostyringssystem. Hensikten med rammeverket er å sikre en høy grad av operasjonell sikkerhet ved å gjøre virksomhetene i stand til å hensynta IKT-risikoer raskt og effektivt på en dekkende måte. Dette innebærer for eksempel krav knyttet til identifisering, klassifisering og dokumentering av IKT-støttede forretningsprosesser, oversikt over virksomhetens informasjons- og IKT-aktiva og krav til monitorering, deteksjon og beskyttelse i virksomheten.

2. Hendelseshåndtering og rapportering
   Det kreves blant annet at foretakene skal ha en prosedyre for å oppdage, håndtere og varsle om IKT-relaterte hendelser. Prosessen for hendelseshåndtering skal blant annet inneholde prosedyrer for å identifisere, spore, logge, kategorisere og klassifisere IKT-relaterte hendelser basert på deres alvorlighetsgrad. Alvorlighetsgraden vil igjen være avhengig av kritikaliteten (konsekvens/hyppighet) til de påvirkede systemene.

3. Testing av motstandsdyktighet
   Det vil for de fleste virksomhetene som omfattes av DORA stilles krav om at virksomheten har et program for testing av digital operasjonell motstandsdyktighet som en del av sin styring av IKT-risiko. For flere virksomheter blir det også stilt krav om at det minimum hvert tredje år gjennomføres en trusselbasert penetrasjonstest (TLPT).

4. Styring av leverandørrisiko
   Leverandører av IKT-tjenester får en større og større rolle for finansforetakenes drift. DORA stiller derfor krav til virksomhetenes risikostyring knyttet til sine IKT-leverandørene. Kravene stiller for eksempel krav til hva kontraktene med disse leverandøren skal inneholde, krav til evaluering og oppfølging av leverandørene, samt rapportering. Enkelte IKT-leverandører vil også bli ansett som kritiske IKT-leverandører. Disse vil følges opp på EU-nivå.

5. Informasjonsdeling om trusler og etterretning
   DORA legger opp til at finansforetakene seg imellom og med myndighetene, kan utveksle informasjon knyttet til cybertrusler, som for eksempel erfaringer, prosedyrer, trusler, sårbarheter, teknikker og konfigurasjoner m.m. I nordisk sammenheng vil for eksempel organisasjoner som Nordic Financial CERT (NFCERT) kunne spille en rolle.

DORA-forordningen er rettet mot finanssektoren og blir gjerne sammenlignet med GDPR.

Hvordan forberede virksomheten for DORA?

Forstå hva DORA krever

Først og fremst er det viktig at man bruker tid på å sette seg inn i DORA, og forstår hva som kreves. I denne sammenheng vil Regulatory Technical Standards (RTS) være til hjelp. Dette er støttedokumentasjon som utbroderer nærmere hva som ligger i de ulike kravene. Videre må man på bakgrunn av proporsjonalitetsprinsippet ta stilling til hvilket nivå man skal legge seg på for sin virksomhet.

Gjennomføring av GAP-analyse

Etter at kravene er klarlagt, må det foretas en vurdering av hvor virksomheter er sett opp mot de ulike kravene. Det må lages et bilde av hvor det er mangler og hvor det allerede anses å være godt dekket.

Legg en plan for det videre arbeidet

I det videre arbeidet er det lurt å ha en strukturert plan for hvordan man skal jobbe videre. Først og fremst for å oppfylle kravene som forordningen stiller, og senere finne områder som kan forbedres. I dette arbeidet vil det også være lurt å ha et forhold til hvilke tiltak som anses mer kritisk enn andre, for så å prioritere disse.