DORA – cybersikkerhed i den finansielle sektor

Martin Christian Kruhl
Partner

Anders Hosbond Nielsen
Advokat, Senior Associate

Introduktion

Vedtagelsen af Digital Operational Resilience Act (også kendt som "DORA") vil i den kommende tid få væsentlig betydning for finansielle virksomheder i hele EU, herunder også forvaltere af alternative investeringsfonde (FAIF'ere).

DORA gælder dog ikke for *registrerede* forvaltere af alternative investeringsfonde. Det er således alene forvaltere med *tilladelse* efter FAIF-lovens § 11, der omfattes af de nye regler.

Formålet med DORA er at styrke de omfattede virksomheders digitale operationelle modstandsdygtighed for at undgå cybertrusler og håndtere dem på passende vis. Målet er at fastsætte en række detaljerede og omfattende minimumskrav, især med hensyn til risikostyring på området for informationsteknologi og tredjepartsstyring af IT. DORA indebærer derudover en række omfattende opgaver og beføjelser for tilsynsmyndighederne i hver medlemsstat, der bliver ansvarlige for at overvåge overholdelse af DORA, ligesom reglerne introducerer detaljerede rapporteringsforpligtelser for de omfattede virksomheder i tilfælde af sikkerhedshændelser.

DORA er trådt i kraft den 16. januar 2023 og skal være fuldt implementeret i finansielle virksomheder senest den *17. januar 2025*.

Du kan i dette indlæg læse mere om, hvilke pligter der er særligt vigtige at efterleve samt hvordan I som FAIF med tilladelse arbejder med efterlevelse af DORA.

Baggrund

Med udgangspunkt i et stigende trusselsbillede inden for cybersikkerhed, er målet for DORA at etablere ensartede regler i hele Europa. I erkendelse af at cyberisici i høj grad er grænseoverskridende, har de eksisterende nationale reguleringer og tilsyn kun haft en begrænset effekt i beskyttelsen mod cyberangreb. Det har også vist sig, at EU-medlemsstaternes egne initiativer har båret præg af, at regler har overlappet, haft uoverensstemmelser og medført et betydeligt ekstra administrativt arbejde og omkostninger for de omfattede virksomheder i deres håndtering af cyberrisici. Formålet med DORA har været at afbøde disse negative virkninger og tilvejebringe et fælles regelsæt.

For at nå dette formål, har DORA introduceret en række minimumskrav med hensyn til risikostyring på *informations- og kommunikationsteknologi ("*IKT*")*. Alle omfattede virksomheder skal etablere de nødvendige tiltag, som styrker deres digitale operationelle stabilitet, muligheden for at opdage cyberangreb og identificere øvrige IT-risici rettidigt, samt afbøde deres negative virkninger.

Det medfører blandt andet, at IKT-systemer skal revideres løbende og sikkerhedshændelser skal rapporteres til de relevante tilsynsmyndigheder. Dette svarer i vidt omfang til det rapporteringsregime, der allerede eksisterer i relation til sikkerhedsbrud i databeskyttelsesforordningen (GDPR).

Finanstilsynet får som tilsynsmyndighed mulighed for at anmode om oplysninger og gennemføre inspektioner på området. I lighed med andre områder får Finanstilsynet derudover også en række sanktionsbeføjelser, såsom muligheden for at udstede påbud eller kræve ophør af en praksis eller adfærd. Et eksempel herpå kan være helt eller delvist ophør af en outsourcet IT-drift. Mange af de formål som søges imødegået med DORA, herunder f.eks. sikre fortroligheden og tilgængeligheden af data, er også relevante beskyttelsesformål efter andre regelsæt.

DORA introducerer pligter inden for en række hovedområder, som vil blive kort introduceret i det følgende:

- Risikostyring
- Hændelsesrapportering
- Test, beredskab og mitigering
- Tredjepartsrisikostyring
- Informationsdeling

Risikostyring

De omfattede virksomheder skal indføre en robust, omfattende og veldokumenteret ramme for IKT-risikostyring, som medvirker til, at virksomheden kan håndtere en IKT-risiko hurtigt, effektivt og fyldestgørende og som sikrer et højt niveau af digital operationel modstandsdygtighed. Minimumskravene til dette kræver, at der fastsættes strategier, politikker, procedurer, IKT-protokoller og værktøjer m.v., som er nødvendige for at beskytte alle informationsaktiver og IKT-aktiver mod skade. Disse dokumenter vedrørende risikostyringen skal gennemgås og dokumenteres mindst én gang årligt og revideres internt regelmæssigt.

Det er væsentligt at holde sig for øje, at DORA opererer med en risikobaseret tilgang og et proportionalitetsprincip, hvilket afspejles i forordningens krav, der fastsætter nogle generelle standarder og overordnede retningslinjer for de omfattede virksomheders arbejde. Den nærmere udfyldning og fastlæggelse af kravene beror derfor på en række vurderinger, herunder særligt risikovurderinger, som foretages af den

enkelte virksomhed i lyset af de oplysninger som skal beskyttes samt omfanget af kritiske IKT-funktioner og sårbarheder.

Hændelsesrapportering

DORA fastlægger en række pligter i relation til styring, klassificering og indberetning af IKT-relaterede hændelser. De omfattede virksomheder skal etablere og vedligeholde en proces for håndtering af IKT-risici. Dette omfatter identifikation, vurdering og styring af risici samt fastlæggelse af ansvar og kompetencer.

De omfattede virksomheder skal derudover klassificere opståede IKT-hændelser baseret på væsentlighed samt indberette større IKT-hændelser til kompetente myndigheder. Mindre væsentlige hændelser bør dokumenteres internt. Der skal ske en indledende, foreløbig og endelig indrapportering af de omfattede sikkerhedshændelser.

Test af digital operationel modstandsdygtighed

For at sikre et højt beskyttelsesniveau samt at de omfattede virksomhed er rustet mod nye eller ændrede trusler inden for cybersikkerhed, skal virksomhederne løbende gennemføre tests af deres operationelle modstandsdygtighed.

De omfattede virksomheder er derfor forpligtede til at implementeret et program for test af dets digitale operationelle modstandsdygtighed, som kan identificere svagheder, mangler og huller samt træffe de nødvendige korrigerende foranstaltninger herfor. Arbejdet med test af den digitale modstandsdygtighed skal ske med udgangspunkt i en risikobaseret tilgang, men bør generelt tage stilling til tests såsom sårbarhedsvurderinger og -scanning, open source-analyser, vurderinger af netsikkerheden, mangelanalyser, fysiske sikkerhedsgennemgange, spørgeskemaer og scanningssoftwareløsninger, gennemgange af kildekoder, scenariebaserede tests, kompatibilitetstests, præstationstest, end-to-end-test og penetrationstest.

Der skal udføres trusselsbaserede penetrationstests (TLPT) for IKT-tjenester, der påvirker kritiske funktioner mindst hvert tredje år.

Tredjepartsrisikostyring

DORA stiller krav om, at tredjepartsudbydere af IKT-tjenester deltager og samarbejder i test af de omfattede virksomheders cyberberedskab. Det påhviler dog de omfattede virksomheder at sikre løbende overvågning af de risici, som relaterer sig til tredjepartsudbydere, samt foretage indberetning af et register over de outsourcede aktiviteter.

Pligterne relateret til outsourcing af funktioner pålægger desuden den enkelte virksomhed at tage højde for risici ved videreoutsourcing. Det vil i praksis medføre krav om, at hele leverandørkæden er kendt og er en del af den omfattede virksomheds risikovurdering. Desuden stilles der krav til de kontraktvilkår, der indgås med tredjepartsudbyderen, der blandt andet skal indeholde bestemmelser om det aftalte serviceniveau, tilgængelighed og genopretning af data og persondata, oplysninger om leveringssted og lokationer for datalagring. Dette er også tilfældet ved anvendelsen af kritiske og vigtige leverandører af IKT-tjenester, hvor der også stilles større krav til kontraktvilkårene, herunder for at sikre en hurtig og effektiv genopretning, hvis de aftalte serviceniveauer ikke nås og undgå leverandørafhængig ved at indføre exitstrategier (ophørsassistance).

Informationsdeling

DORA giver de omfattede virksomheder adgang til indbyrdes at udveksle oplysninger og efterretninger om cybertrusler, eksempelvis hvor en sådan udveksling har til formål at forbedre modstandsdygtigheden, øge bevidstheden om cybertrusler eller understøtte forsvaret mod disse trusler.

Ved deltagelse i en ordning for informationsudveksling skal den omfattede virksomhed underrette tilsynsmyndigheden herom, ligesom enhver informationsudveksling skal ske uden at kompromittere virksomhedernes forretningshemmeligheder eller føre til overtrædelser af konkurrenceretten eller databeskyttelseslovgivningen.

Ansvaret for gennemførelse af IKT-risikostyring

Det er det øverste ledelsesorgan (dvs. i praksis ofte bestyrelsen) i de omfattede virksomheder, som bærer det overordnede ansvar for gennemførelsen af den korrekte IKT-risikostyring. Ansvaret omfatter dels en pligt til at fastlægge rammerne og godkende de interne forretningsgange og politikker, som finder anvendelse for risikostyringen af IKT og dels en pligt til at føre tilsyn med, at organisationens risikostyring finder sted i overensstemmelse med de fastlagte rammer.

Det øverste ledelsesorgan skal også sikre, at der indføres tilstrækkelige indberetningskanaler på virksomhedsniveau, der gør det muligt at få underretning om væsentlige informationer om virksomhedens egen og tredjeparts IKT-tjenester.

Implementeringen og efterlevelse af DORA

DORA er introduceret som endnu et regelsæt inden for kategorien af regulatoriske pligter for virksomheder i den finansielle sektor, herunder FAIF'er. DORA fastsætter dog en ramme for arbejdet med informationssikkerhed og håndtering af cyberrisici, som for mange af de omfattede virksomheder ikke tidligere har været systematiseret eller dokumenteret.

For at kunne leve op til forordningens krav inden 17. januar 2025, bør de omfattede virksomheder være i proces eller påbegynde deres arbejde for at sikre compliance allerede i løbet af 2024. Erfaringen fra implementeringsforløb med andre sammenlignelige regelsæt, fx GDPR, har vist, at i en situation, hvor alle markedsaktører og leverandører skal efterleve det samme regelsæt inden for samme tidsfrist, kan kontraktforhandlinger og markedstilpasninger tage tid.

Vores anbefaling er, at der i første omgang foretages en kortlægning af virksomhedens modenhedsniveau gennem en GAP-analyse, hvor der skabes klarhed over, hvilke procedurer og krav der er mulighed for at efterleve – og hvilke nye foranstaltninger der bør iværksættes.

Herefter skal konklusionerne fra analysen adresseres og der vil være en række direkte pligter, som skal udmøntes i organisationen, herunder f.eks.:

- Gennemførelse af de relevante risikovurderinger,
- Indgåelse, ajourføring og vurdering af de relevante leverandør- og outsourcingkontrakter for at sikre efterlevelse af DORA,

- Udarbejdelse og implementering af de relevante politikker og forretningsgange,
- Fastlæggelse af strategi for digital operationel modstandsdygtighed.

Vores specialister inden for området står klar til at hjælpe jer med implementeringen af kravene fra DORA. Kontakt os gerne for en nærmere afklaring af, hvilke områder vi kan hjælpe jer med.