Vad behöver man göra om man omfattas av DORA?

Av:
Johan Gnosspelius

2024

Författare

Johan Gnosspelius
Senior Partner på Pro4u
Johan har lång erfarenhet av arbete inom finans och fintech. Johan har lett projekt inom produktutveckling, regelverksuppfyllnad och implementation av lösningar hos kund.
E-post: johan.gnosspelius@pro4u.com
Mobiltelefon: 073 - 925 99 33

Inledning

Banker, försäkringsbolag, pensionsinstitut och andra finansiella företag och deras underleverantörer måste efter 17 januari 2025 följa ett EU-regelverk för digital motståndskraft.
Med tanke på den senaste tidens många angrepp från ryska hackergrupper är detta område högst aktuellt.

Vad är DORA?

DORA, Digital Operational Resilience Act, är ett finansiellt regelverk inom EU.Kort täcker DORA följande:

- **Krav som är tillämpliga på finansiella entiteter i fråga om:**
- riskhantering inom informations- och kommunikationsteknik (IKT),
- rapportering av allvarliga IKT-relaterade incidenter och på frivillig grund, underrättande om, betydande cyberhot till behöriga myndigheter
- rapportering av allvarliga betalningsrelaterade operativa incidenter eller säkerhetsincidenter till behöriga myndigheter
- testning av digital operativ motståndskraft,
- utbyte av information och underrättelser i samband med cyberhot och cybersårbarheter,
- åtgärder för en sund hantering av tredjepartsrelaterad IKT-risk.

Eftersom DORA är en "regulation" är det applicerbart i alla EUs medlemsstater. DORA-regelverket ersätter NIS 2-direktivet för finansiella entiteter.

I regelverket finns en lång lista av organisationer som betraktas som finansiell entitet. Tredjepartsleverantörer av IKT-tjänster omfattas av regelverket men betraktas inte som finansiella entiteter.

Regelverket gäller finansiella entiteter och träder i kraft den 17 januari 2025.

Vad behöver man göra om man omfattas av DORA?

En första bedömning är att avgöra vilken typ av finansiell entitet man betraktas som. Detta styr vilken omfattning av aktiviteter som krävs. En liten finansiell entitet behöver inte uppfylla så mycket. Ett andra steg kan vara att gå igenom områdena nedan för att identifiera vad som redan finns på plats och vilka förändringar som behövs.

Riskhantering

Finansiella entiteter måste etablera och underhålla effektiva och proportionerliga riskhanteringsstrategier, policyer, procedurer och system. Detta inkluderar att identifiera, dokumentera och hantera informations-säkerhetsrisker. Regelverket beskriver principer och man kan stödja sig på relevanta modeller och praxis för IKT-risker.

Styrning

Finansiella entiteter måste ha en lämplig governance-struktur för att säkerställa att IKT-risker hanteras effektivt. Detta kan inkludera att inrätta särskilda kommittéer eller funktioner som fokuserar på digital motståndskraft.

Incidenthantering

Det är viktigt att ha planer och processer på plats för att snabbt kunna identifiera, rapportera och hantera IKT-incidenter.

Testning av motståndskraft

Man behöver planera och genomföra regelbunden testning av IT-systemen för att säkerställa att de kan motstå olika typer av cyberattacker och andra störningar. Detta kan inkludera penetrationstester, stresstester och scenariobaserade övningar. Hur avancerad testning som krävs beror på typ av finansiell entitet. Riskbaserad testning skall göras årligen medan mer avancerad hotbildstestning skall göras vart tredje år.

Riskhantering av tredje part

Finansiella entiteter måste övervaka och hantera risker kopplade till tredjeparts-leverantörer, särskilt de som tillhandahåller kritiska IT-tjänster. Avtal med underleverantörer måste formuleras för att möte kraven i regelverket och innehålla bestämmelser om t.ex. skydd av funktioner, tjänster och information övervakning, säkerställande av att återta information om leverantören upphör och samarbete.

Datahantering och säkerhet

Strikta åtgärder för dataskydd och säkerhet för att skydda känslig information, inklusive personuppgifter.

Rapportering

Att säkerställa överensstämmelse med DORA-kraven kräver regelbunden rapportering och kommunikation med tillsynsmyndigheter.

Utbildning och medvetenhet

Att investera i utbildning och medvetenhet om cyberhot och digital motståndskraft bland personalen är också viktigt.

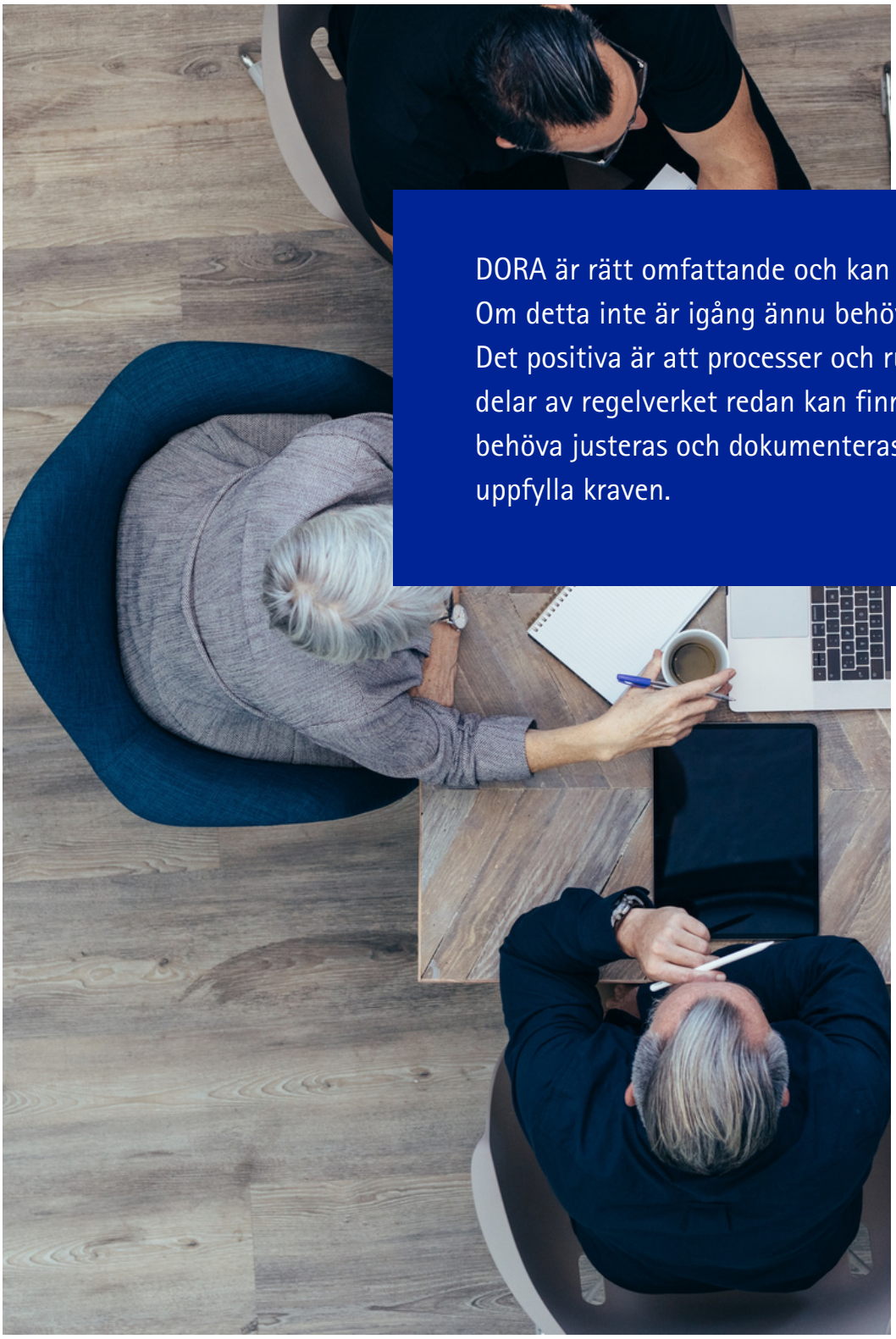
Utbyte av information

Regelverket ger också möjlighet till utbyte av information om hot, erfarenheter, mm. Detta informationsutbyte mellan finansiella entiteter är frivilligt men uppmuntras så att man gemensamt skall kunna upprätthålla god motståndskraft..

Viktiga datum

- 17 januari 2024: Utkast till tekniska standarder presenteras.
- 17 juli 2024: Riktlinjer för kostnadsberäkning relaterat till IKT-incidenter.
- 17 januari 2025: DORA träder i kraft.

Slutsats / Sammanfattning



DORA är rätt omfattande och kan kräva mycket arbete. Om detta inte är igång ännu behöver det börja snarast. Det positiva är att processer och rutiner för många delar av regelverket redan kan finnas på plats. De kan behöva justeras och dokumenteras för att fullt uppfylla kraven.

Källa: Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance)