EU-specialudvalget for den finansielle sektor

Sendt e-mail til:
jesu@ftnet.dk
ama@em.dk

Kopi til:
eu.mail@ftnet.dk

Forsikring & Pension

07.10.2020

Forsikring & Pension
Philip Heymans Allé 1
2900 Hellerup
Tlf.: 41 91 91 91
fp@forsikringogpension.dk
www.forsikringogpension.dk

Henriette Günther Sørensen
Chefkonsulent
Dir. 41 91 91 74
hgs@forsikringogpension.dk

Sagsnr. GES-2020-00258
DokID 410898

Digital Operationel Resilience Act – DORA - høringssvar

EU-specialudvalget for den finansielle sektor anmoder om input til EU-Kommissionens lovforslag på området for cybermodstandsdygtighed (Digital Operational Resilience Act - DORA). EU-specialudvalget udarbejder herefter et grund- og nærhedsnotat til lovforslaget til Kommissionen. Forsikring & Pension (F&P) værdsætter muligheden for at komme med input, som en del af F&P's indsats på cyberområdet.

EU-Kommissionen har den 24. september 2020 præsenteret deres 'Digital Finance Strategi for Europe'. Digital Finance-strategien blev ledsaget af et forslag til en forordning på området for cybermodstandsdygtighed 'Digital Operational Resilience' (DORA). DORA omhandler cybermodstandsdygtighed i den finansielle sektor. EU vil samle den eksisterende regulering, så der kommer en samlet tilgang til regler og lovgivning på området for cyber- og informationssikkerhed på det finansielle område.

Lovforslaget har fokus på, hvordan den europæiske indsats styrkes i den finansielle sektor ved at løfte robustheden på tværs af EU. Det primære håndtag i lovforslaget er regulering inden for den stadigt stigende brug af 'Information and Communication Technology' (ICT) og de deraf affødte sikkerhedsudfordringer.

Lovforslaget sætter retningslinjer og stiller minimumskrav inden for seks hovedtemaer:

1. Governance og organisering (artikel 4)
2. ICT risikostyring (artikel 5-14)
3. Hændelsesrapportering vedr. ICT (artikel 15-20)
4. Test af cyberrobusthed (artikel 21-24)
5. Risikovurdering af 3. parts-leverandører af ICT (artikel 25-39)
6. Deling af viden og information om cyberhændelser (artikel 40)

Tilgangen i lovforslaget er risikobaseret og vil følge proportionalitetsprincippet.

Generelle og overordnede bemærkninger

Der er stor opbakning fra F&P til en mere fokuseret EU-indsats, der bidrager til at øge modstandsdygtigheden over for cyberangreb i den finansielle sektor i EU og Danmark. Formålet med lovforslaget er at skabe en robust og sikker finansiel sektor med ensartet regulering på tværs af EU. Forsikrings- og pensionsbranchen imødeser harmonisering af regler for cybermodstandsdygtighed, hvorfor DORA generelt anses som et positivt initiativ. Det er i branchens interesse med konsolidering af krav og regler. Med DORA vil EU konsolidere den eksisterende regulering og skabe ensretning i forhold til arbejdet med cybersikkerhed og brugen af internationale standarder. Det arbejde deltager forsikrings- og pensionsbranchen gerne i, og vi støtter EU's dagsorden om at håndtere den stadig stigende brug af ICT i den finansielle sektor og de deraf affødte sikkerhedsudfordringer.

Cybersikkerhedsdagsordenen er højt prioriteret i den danske forsikrings- og pensionsbranche. Der er tæt koordinering og videndeling i branchen, og branchen arbejder for at sikre den samlede finansielle sektor i et tæt samarbejde med Nationalbanken (gennem Finansielt Sektorforum for Operationel Robusthed, FSOR), Finanstilsynet via Decentral enhed for Cyber- og Informationssektoren for finanssektoren (DCIS) og med Center for Cybersikkerhed (CFCS). De enkelte selskaber bruger store ressourcer på at forebygge cyberhændelser, værne om borgernes personoplysninger og klæde medarbejderne godt på. Cyber- og informationssikkerheden har meget høj prioritet i branchen.

F&P's høringsinput går på det nye lovforslag og forholder sig ikke til eventuelle ændringer i Network and Information Security (NIS)-direktivet. Det er for nuværende en smule uklart, hvordan det nye lovforslag spiller sammen med NIS-direktivet. F&P finder det væsentligt at sikre, at de to lovgivninger spiller sammen og at virksomhederne ikke bliver pålagt dobbelte rapporteringsforpligtelser under den nuværende og kommende regulering.

Forsikrings- og pensionsbranchens påvirkning på finansiel stabilitet

Det overordnede formål med - og udgangspunkt for - den nye sektorlov, er at *sikre finansiel stabilitet* i EU i en sektor, som bliver mere og mere digital afhængig og forbundet på tværs af enheder, lande og grænser. En cyberrisikoanalyse af forsikrings- og pensionsbranchen - udarbejdet som en del af den nationale cyber- og informationsstrategi i regi af FSOR - viser, at branchen ikke truer finansiel stabilitet. Branchen er til gengæld meget afhængige af, at banksektoren er stabil og tilgængelig, for at branchen kan gennemføre sine forretningskritiske funktioner. Det er den vej rundt, kæden hænger sammen; er banksektoren (herunder værdipapirhandler m.v.) nede eller ude af funktion, så har forsikrings- og pensionsbranchen ringe vilkår for at opretholde sine forretningsfunktioner- og forpligtelser over for kunderne. Hvis alle forsikrings- og pensionsbranchens kritiske forretningsfunktioner blev sat ud af spil, ville branchen stadig ikke true den finansielle stabilitet på et niveau, hvor det er samfundskritisk på den korte bane. Forsikrings- og pensionsbranchen er naturligvis opmærksomme på, at vi er en del af den samlede værdikæde.

F&P efterspørger derfor, at lovforslaget også anvender proportionalitetsprincippet i forhold til forskellige dele af den finansielle sektor, så den afspejler, at forsikrings- og pensionsbranchen har en anden risikoprofil end fx banksektoren. Kritikaliteten af forsikrings- og pensionsbranchen er ikke sammenlignelig med fx kritiske betalingstjenester eller fælles værdipapirinfrastruktur. Det må derfor være

rimeligt at vurdere, om forsikrings- og pensionsbranchen skal være omfattet af de samme regler, retningslinjer og minimumskrav som banksektoren, når forsikrings- og pensionsbranchen ikke er kritiske på samme niveau. Eller om forsikrings- og pensionsbranchen i det hele taget skal være omfattet af hele lovforslaget.

Nedenstående sammenfatter F&P's overordnede kommentarer til lovforslaget:

- Materialet er yderst detaljeret og stiller meget præcise og detaljerede krav. Der anvendes helt grundlæggende en risikobaseret tilgang, hvor kravene til sikkerhed stiger med størrelsen af risici. Flere artikler indeholder sprogbrug, som fx skal, straks og uden ugrundet ophold. Eksempler på dette ses af formuleringerne i artiklerne 9, 10 og 11, omhandlende detektion, respons og backup.
- Materialet er tydeligt inspireret af ISO 27001/02/05, NIST, CIS20 og andre best practice-frameworks.
- Der er overlap til tidligere materiale fra EBA og EIOPA.
- Det er branchens vurdering og bekymring, at implementering af lovforslagets krav pålægger selskaberne udgifter, der er unødigt høje i forhold til den reelle risikoreduktion. Ændringerne er detaljerede krav, der kræver yderligere og store investeringer målt i både tid, ressourcer og økonomi, fx investering i ny teknologi, og i yderligere formalia og dokumentation. Herunder er F&P også bekymret for forventningerne til implementeringshastigheden i organisationerne ift. de mange nye krav.
- Lige så meget som branchen imødeser udviklingen af fælles EU-standarder og retningslinjer, bør det fremhæves, at nye EU-standarder bør afspejle de eksisterende og gennemtestede internationale standarder på området, fx ISO27001, CIS20, NIST, m.v. for at undgå unødige omkostninger og værdispild for de organisationer, som allerede har implementeret de nødvendige tiltag.
- Der er umiddelbart et vist overlap mellem outsourcingreglerne (fx i forhold til underretning om outsourcing af kritisk/vigtig aktivitet), EIOPAs nye cloud-outsourcing retningslinjer og de nye initiativer i DORA. F&P opfordrer til at forholdet mellem regelsættene bør afstemmes og tydeliggøres.

F&P's mere detaljerede kommentar til hovedtemaerne

F&P har samlet mere detaljerede kommentarer til de seks hovedtemaer.

AD 1 Governance og organisering (Artikel 4)

- De krav, der stilles til governance og organisering i lovforslaget, er omfattende og komplekse. Det kræver dedikerede ressourcer (sandsynligvis flere end i dag), klare (nye) roller og ansvar for cyber- og informationssikkerhed og risk management med en forankring i toppen af organisationen.
- F&P bemærker, at lovforslaget lægger op til, at der kommer en dedikeret rolle i organisationen, som følger op på 3. parts-leverandører og de krav, der bliver stillet til dem, jf." Risikovurdering af 3. parts-leverandører af ICT". F&P så hellere, at opgaven med at monitorere og 'føre tilsyn' med 3. parts-leverandører er en opgave, der bliver håndteret på centralt hold i stedet for at uddelegere opgaven til de enkelte selskaber.

Ad 2 ICT risikostyring (Artikel 5-14)

- Lovforslaget stiller meget detaljerede krav til styring og kontrol af IT-risici, definition af politikker og procedurer samt tekniske og organisatoriske kontroller bredt set. F&P bemærker, at det umiddelbart svarer til internationale standarder (ISO 27001/02/05, NIST, Cobit, CIS20), men det bør afdækkes, om der er skærpelser ift. eksisterende lovgivning.
- Lovforslaget stiller krav om, at de finansielle enheder anvender et ICT-rammeværk til risikostyring og -vurdering, og at governance og organiseringen tager afsæt heri. Det er uklart, om der bliver lagt op til, at enhederne/virksomhederne anvender det samme ICT-rammeværk, eller om der er flere mulige rammeværk at vælge i mellem, jf. proportionalitetsprincippet, og at virksomhederne har forskellige risikoprofiler. F&P afventer nærmere information om rammeværker, der kan anvendes, lige så vel som F&P også gerne vil spørge ind til, hvordan kravene håndhæves af myndighederne?

Ad 3 Hændelsesrapportering vedr. ICT (artikel 15-20)

- DORA fastlægger tidsfrister for rapportering i forhold til sikkerhedshændelser, monitorering og rapportering til myndigheder, kunder og samarbejdspartnere. Der er tale om skærpelser, som kræver implementering af nye procedurer i mange organisationer.
- DORA lægger op til, at sikkerhedshændelser skal rapporteres til EIOPA. Samtidig vil hændelsen, såfremt den involverer persondata, også skulle rapporteres til Datatilsynet afledt af persondatalovgivningen, fordi sikkerhedshændelsen ofte er et brud på persondatasikkerheden. F&P finder det er centralt, at der sker en grundig overvejelse af, hvordan krav om indrapportering af samme hændelse til flere myndigheder håndteres. Særligt, når der er forskellige krav til hastigheden, hvormed indrapporteringen skal ske.
- Den initiale rapportering til brugere, kunder og myndigheder skal ske inden for få timer, hvilket kan afføde, at fokus på at løse hændelsen fjernes for at kunne sikre korrekt rapportering. Desuden er der ingen angivelse af, hvorvidt den initiale rapportering først skal ske, når det endeligt er konstateret, at der er sket en hændelse, som det er gældende i GDPR. I lovkrav om rapportering af hændelser er der desuden behov for en definition af, hvad en hændelse er, for at det er underlagt disse lovkrav.

Ad 4 Test af cyberrobusthed (artikel 21-24)

- DORA lægger op til implementering af et omfattende "digital resilience testing programme" a la TIBER. Test skal udføres af uafhængige aktører minimum årligt, herunder krav om en advanced "threat led penetration test" minimum hvert 3. år, hvorefter rapporten skal sendes til kompetent myndighed, som skal validere og udstede attest herfor, jf. art. 23.2. Det er en klar skærpelse af kravene til test og desuden en ikke uvæsentlig cost driver, idet der også stilles krav til kvaliteten af personale eller leverandør, der skal udføre testen, herunder akkreditering m.v.
- F&P bør undersøge, hvorvidt branchen kan blive omfattet af TIBER-DK, der foregår i regi af FSOR, Nationalbanken, i en form tilpasset branchen og risikoprofilen.

Ad 5 Risikovurdering af 3. parts leverandører af ICT (artikel 25-39)

- Der stilles mange og detaljerede krav til risikovurdering, opfølgning og exitplaner, ligesom der stilles høje krav til løbende monitorering af sikkerheden hos 3. part, særligt i regi af cloud.
- Reglerne er meget dybdegående og har umiddelbart udvidelser/skærpelser i forhold eksisterende outsourcing-regler. Der er dog et vist overlap mellem outsourcingreglerne (underretning om outsourcing af kritisk/vigtig aktivitet) og nærværende regler om ICT-aktiviteter. Definitionen af kritisk/vigtig i nærværende regler stemmer overens med definitionen i EIOPAs guidelines om outsourcing arrangements, men det bør tydeligt fastlægges, om vurderingen er identisk. I bekræftende fald bør det desuden afstemmes, om processer, fx dokumentation, orientering til kompetent myndighed, m.v., kan kombineres/ensrettes eller ej for at forsimple proces herunder sikre, at der ikke sker ressourcespild.
- Det bør afdækkes, om indholdskravene alene finder anvendelse i relation til vigtige/kritiske ICT-funktioner eller også ved alle øvrige ikke-vigtige ICT-funktioner. Kravene udgør en udfordring i relation til anvendelse af standard ICT-funktioner, SaaS-løsninger, m.v., der som udgangspunkt købes på leverandørens standardvilkår. Kravene bør afspejle en risikobaseret tilgang.
- Art.25.7-25.9: audit, hæveadgang og exitplaner:
  - Kravene vedr. audit-adgang, hæveadgang og udarbejdelse af exitplaner bør kvalificeres til alene at omfatte væsentlige forhold eller forhold relateret til væsentlige dele af ICT-funktioner. Den nuværende ordlyd er ikke proportionel og kan potentielt blive administrativt og kommercielt uforholdsmæssigt tung.
- Art. 27: krav til kontraktens indhold:
  - Overlap med tilsvarende outsourcingkrav, men kravene i DORA går dybere, fx ift. hændelser.
- Lead Overseer:
  - DORA lægger op til, at myndighederne skal udpege en Lead Overseer for at sikre tilstrækkeligt sikkerhedsniveau hos 3. parts-leverandører med systemiske risici og koncentrationsrisici.
  - Lead Overseer får bemyndigelse til at få indsigt i data hos leverandøren og til at få udleveret kopier af data. For finansielle selskaber vil behandlingen af data placeret hos en 3. part typisk være reguleret af en databehandleraftale mellem selskabet og 3. parts-leverandøren. Der er i databehandleraftaler en regulering af, hvorvidt databehandleren må udlevere data til myndigheder. Den regulering, der er lige nu, kan komme i konflikt med reguleringen omkring databehandlingen i selskabernes databehandleraftaler.
  - Bemyndigelsen til at få indsigt i data og få udleveret kopi af data kan desuden potentielt komme i strid med forbuddet mod videregivelse af fortrolige oplysninger i medfør af lov om finansielvirksomhed § 117.
- Garanti i dataoverførsler:
  - DORA beskriver, at selskaberne skal kunne garantere beskyttelse af data i dataoverførsler. Der er ingen angivelse af, at beskyttelsen skal være proportional med de data, der overføres, samt om data overføres på et internt netværk eller over Internettet.

Ad 6 Deling af viden og information om cyberhændelser (artikel 40)

- Der opfordres til øget informationsdeling mellem myndigheder og finansielle institutioner inden for området cyber- og informationssikkerhed. Dette anses som et positivt initiativ.

Generel opsamling for Ad 1 til Ad 6

Det udestår, at lovforslaget bliver mere konkret på, hvordan proportionalitetsprincippet spiller ind rent praktisk, og hvad det betyder for kravene. Det er også uklart, hvordan tilsynet fra myndighedernes side gennemføres i praksis. F&P er også bekymret for de øgede omkostninger, selskaberne vil have til at implementere tiltagene i lovforslaget.

F&P påpeger igen, at branchen generelt har en anden risikoprofil end banksektoren, og at forsikrings- og pensionsbranchen ikke er sammenlignelig med banksektoren. Et solidt sikkerhedsniveau på tværs af sektoren er i alles interesse, men nye krav, og eventuelle øgede investeringer og ressourcer, skal stå i et rimeligt forhold til den reelle risikoreduktion.

Forståelse af specifikke krav

I fx. artikel 14 og 25 er angivet krav til myndighederne for, hvordan - og særligt hvornår - de skal have defineret tilstrækkelige teknologiske løsninger eller nødvendige risikostyringsprocesser i de finansielle virksomheder. I disse artikler er angivet, at kravene skal være på plads 1 år efter lovgivningen træder i kraft. Dermed bliver selskaberne efterladt med at skulle lave egen tolkning på implementering og dermed i risiko for enten over- eller underimplementering.

Med venlig hilsen

Henriette Günther Sørensen