

Til  
Forsvarsministeriet

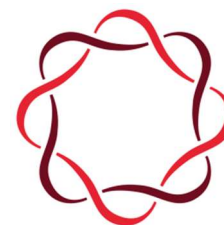
Sendt til:

Nicklas Schreiber Echsner-Rasmussen ([ner@fmn.dk](mailto:ner@fmn.dk)),

Thomas Balslev Rosenzweig ([thr@fmn.dk](mailto:thr@fmn.dk)),

Nikolaj Højer ([nhj@fmn.dk](mailto:nhj@fmn.dk))

Ann-Sofie Koutsis Olsen ([aso@fmn.dk](mailto:aso@fmn.dk))



---

**FINANS  
DANMARK**

## **Høringsvar til Europa-Kommissionens forslag til direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen (NIS 2.0) og om ophævelse af direktiv (EU) 2016/1148**

### **Høringsvar**

Europa-Kommissionen har den 16. december 2020 offentliggjort forslag til Europa-Kommissionens direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen.

3. februar 2020

Dok: FIDA-151247800-701473-v1

Kontakt Torben Nielsen

Finans Danmark finder det positivt, at Europa-Kommissionen fastholder fokus på et højt sikkerhedsniveau for de europæiske samfundskritiske funktioner og digitale infrastrukturer.

Finans Danmark finder det positivt, at kommissionens forslag udvider anvendelsesområdet for det nuværende NIS-direktiv ved at tilføje nye sektorer baseret på deres kritiske indflydelse på økonomien og samfundet. Vi finder det videre positivt, at der indføres et klart størrelsesloft - hvilket betyder, at alle mellemstore og store virksomheder i udvalgte sektorer vil blive omfattet. Det er vigtigt, at det er entydigt, hvem der er omfattet.

Vi bemærker os tillige, at forslaget fjerner sondringen mellem operatører af væsentlige tjenester og udbydere af digitale tjenester. Aktører klassificeres på grundlag af deres betydning og opdeles i henholdsvis væsentlige og vigtige kategorier med den konsekvens, at de underkastes forskellige tilsynsordninger.

Finans Danmark anbefaler, at der her sigtes mod en differentiering baseret på et proportionalitetsprincip, således at relevante krav målrettes den faktiske risiko. Finans Danmark finder det tilsvarende positivt, at forslaget styrker sikkerhedskrav for berørte virksomheder ved at indføre krav om en risikostyringstilgang.

Som en del af initiativerne, der samlet set skal medvirke til at højne den europæiske cyberrobusthed og beskytte kritisk infrastruktur, skal der oprettes et antal nye organer (f.eks. Den fælles cyberenhed). I denne henseende er det vigtigt at

undgå overlappende ansvar, især mellem nationale organer og overnationale organer. Vi anbefaler, at der er fokus på ikke at skabe et meget komplekst, fragmenteret og besværligt rapporterings-økosystem

Finans Danmark bemærker bestemmelserne vedrørende IKT-certificering og finder, at det både er positivt og proportionalt, at det er leverandøren, der skal sikre, at sikkerheden er på plads gennem en certificeringsordning.

#### *Sammenhæng til øvrig EU-regulering*

Finanssektoren er omfattet af NIS 2.0 og forventes også omfattet af DORA ("Digital Operational Resilience Act"), der bliver en Lex specialis for finansielle institutioner/finansmarkedets infrastruktur. Finans Danmark finder det afgørende, at der i den forbindelse undgås dobbeltregulering eller skabes usikkerhed.

Det bemærkes videre, at der i direktivet om kritiske enheders modstandsdygtighed henvises til cyber- og ikke-cybermodstandsdygtighed. Finans Danmark finder det også afgørende, at der også i denne forbindelse undgås dobbeltregulering eller skabes usikkerhed. Konkret anbefaler Finans Danmark, at der foretages en yderligere afgrænsning af de 'væsentlige', 'kritiske' og 'vigtige' enheder som fremhævet i NIS 2.0-direktivet og direktivet om kritiske enheders modstandsdygtighed, da det vil være gavnligt for at sikre tilstrækkelig forståelse og anvendelighed.

Finanssektoren er underlagt en række rapporteringskrav på cybersikkerhedsområdet og forventes i fremtiden at blive underlagt flere rapporteringskrav til flere agenturer/myndigheder og lande, men med forskellige tidslinjekrav osv. Dette risikerer at blive ineffektivt for alle involverede parter. Finans Danmark anbefaler derfor, at regeringen arbejder for, at rapporteringskrav i videst muligt omfang harmoniseres. For at sikre en sammenhængende europæisk rapporteringsramme og for at undgå fragmentering anbefaler vi etablering af et reguleringsinitiativ for en tværgående "cybersikkerhedsrapporteringsforordning" (og ikke et direktiv), der skal omfatte alle rapporteringsforpligtelser og gælde på EU-niveau. Dette ville være særligt vigtigt for finansielle institutioner, der opererer i flere lande. Det vil lette finanssektorens samlede rapporteringsforpligtelser på cybersikkerhedsområdet. Derudover kunne en sådan forordning med fordel sikre yderligere harmonisering af (hændelses-)rapporteringsforpligtelser (inkl. væsentlighed, tærskel, tidslinje, rapporteringsformat) på tværs af forskellige regler, herunder især PSD2-direktivet, DORA-forordningen, NIS 2.0, direktivet om modstandsdygtighed hos kritiske enheder og GDPR. Dette ville samlet set kunne indebære en betydelig forbedring, der samtidig ville muliggøre en mere effektiv og rettidig rapportering til

## Høringsvar

3. februar 2020

Dok. nr.:

FIDA-151247800-701473-v1



relevante nationale myndigheder/EU-myndigheder. Ovenstående forslag er inspireret af den danske FLIS-indberetningsløsning (Fælles Løsning til Indberetning af IT-sikkerhedshændelser (FLIS)) på [virk.dk](http://virk.dk).

Finans Danmark står naturligvis til rådighed i forhold til evt. opfølgende spørgsmål til ovenstående bemærkninger.

Med venlig hilsen

Torben Nielsen

Direkte: 30161087

Mail: [tni@fida.dk](mailto:tni@fida.dk)

## Hørings svar

3. februar 2020

Dok. nr.:

FIDA-151247800-701473-v1

