FINANSTILSYNET

DORA status

F&P Webinar - DORA og tilhørende retsakter

19. december 2024

Jan Jans | Finanstilsynet

DORA 17. januar 2025

1. Tilsynsmæssig konvergens
2. Register of Information (IKT-leverandører) til CTPP udpegning
3. Rapporteringssystemer er på vej
4. Leverandørregistret (RoI) skal sendes i marts
5. TLPT vil muligvis blive forsinket lidt
6. CTPP (Big Tech) Oversight vil tage tid
6. Alle reglerne gælder fra 17. januar, men …
7. Betragtning 69 er lidt uklar;

   »Når finansielle enheder og tredjepartsudbydere af IKT-tjenester genforhandler kontraktlige ordninger…«
8. Udtalelse fra ESA'erne om tilgangen
   1. Risk based
   2. Pragmatic
   3. Outcome focused
9. USSP fra EIOPA og ESMA og EBA ESEP
10. Der er udsendt DORA Q&A'er – flere er på vej

Proportionalitet

1. Proportionalitet er overordnet princip (Art. 4)

2. De vigtigste RTS'er skal håndhæves proportionalt

3. Størrelse, samlet risikoprofil, karakter, omfang og kompleksitet af tjenester mv.

4. Complianceopgaver kan også delegeres

5. Virksomheder tilsluttet en FDI-operatør (datacentral):
    1. Forpligtelse for operatører til at dokumentere "DORA-rammer" (§ 333 c)
    2. Leverandørregister RoI kan sendes af operatøren
    3. Hændelsesrapportering kan også ske fra operatøren

Register of Information (RoI)

1. Register med information om kontraktlige ordninger med IKT-tredjepartsudbydere

2. Registret skal bl.a. omfatte data om:
   1. Parterne i kontrakterne
   2. De forretningsfunktioner som er omfattet
   3. Leverandører og underleverandører
   4. De ultimative ejere af leverandørerne

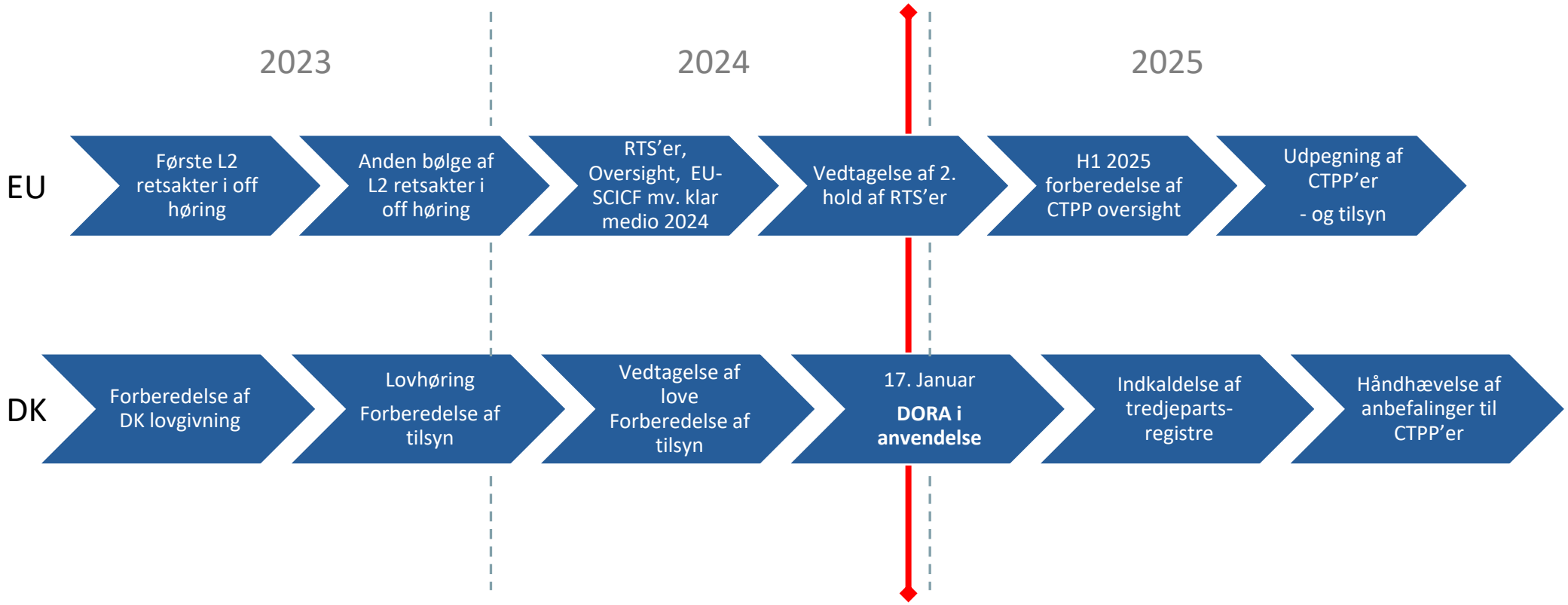
3. LEI koder er obligatorisk for finansielle enheder

4. For leverandører er der valg mellem LEI koder og EUID

DORA Status på delegerede retsakter

Delegated act	WG	ESA lead	Status
Call for advice on criteria for designation of CTPPs	3	EIOPA	Published
Call for advice on oversight fees	3	ESMA	Published
RTS on ICT risk management framework	1	ESMA	Published
RTS on simplified ICT risk management framework	1	ESMA	Published
RTS on criteria for the classification of ICT-related incidents	2	EBA	Published
ITS to establish the templates for the Register of Information	3	EIOPA	Scrutiny
RTS to specify the policy on ICT services performed by 3rd party	1	EBA	Published
ESRB recommendation - interim A(1) and B	2	EIOPA	Adopted
RTS on specifying the reporting of major ICT-related incidents	2	EBA	Scrutiny
ITS to establish the reporting details for major ICT-related incidents + Annex	2	EBA	Scrutiny
Guidelines on the estimation of aggregated costs/losses caused by major ICT related incidents (FINAL REPORT)	2	EBA	jul-24
RTS to specify threat led penetration testing aspects (FINAL REPORT)	1	DB/BaFin	jul-24
RTS to specify elements when sub-contracting critical or important functions (FINAL REPORT)	1	EBA	jul-24
Guidelines on cooperation between ESAs and CAs regarding the structure of the oversight	3	EIOPA	Published
RTS harmonisation of conditions enabling the conduct of the oversight activities	3	EIOPA	Scrutiny
Feasibility report on single EU Hub for major ICT-related events	2	ESMA	jan-25

Status for overgangen til DORA



Forkortelser

DORA	Digital Operational Resilience Act
ESA'er	European Supervisory Authorities, samlebetegnelse for EBA, ESMA og EIOPA
EBA	Den europæiske myndighed for bank- og betalingsområdet
ESMA	Den europæiske myndighed for kapitalmarkedsområdet
EIOPA	Den europæiske myndighed for forsikring og pension
JC	Joint Committee - Fælles komité for de tre ESA'er
JC SC DOR	Joint Committee, Sub Committee; Digital Operational Resilience – ESA'ernes fælles komité med ansvar for DORA implementering
RTS	Reguleringsmæssig Teknisk Standard – en gennemførelsesforordning med samme status som en lov
ITS	Implementeringsmæssig Teknisk Standard – en gennemførelsesforordning som en RTS, men normalt med mere teknisk indhold
GL	Guideline – (ikke-bindende gennemførelsesretsakt)
ECB	Den Europæiske Centralbank
BoS	Board of Supervisors – Det styrende organ i hver enkelt ESA
CTPP	Critical Third Party Provider – It-leverandører, som er udpeget som kritiske for den finansielle sektor på EU-niveau
RoI	Register of Information – Register med information om kontraktlige ordninger med IKT-tredjelpartsudbydere
TLPT	Threat Led Penetration Testing – Test hvor cyber specialister udfører aftalte test-angreb på virksomheder
CfA	Call for Advice – en delegeret retsakt med virkning tilsvarende RTS'er og ITS'er, dvs. en gennemførelsesforordning
NIS2	Det andet Netværks- og informationssikkerhedsdirektiv (erstatter NIS, som gælder i dag)
PSD2	Det andet betalingsservicedirektiv
OES	Operator of Essential Service – en operatør af en væsentlig tjeneste iht. NIS (1) direktivet
CER	Direktivet om kritiske europæiske infrastrukturers modstandsdygtighed (som afløser ECI-direktivet)
TIBER-EU	Threat Intelligence Based Red teaming. I Danmark i form af TIBER-DK – et rammeværk fra ECB og centralbankerne til TLPT i systemiske virksomheder
NCA'er	National Competent Authorities – Nationale tilsynsmyndigheder
CA'er	Competent Authorities (samme som NCA'er)
Kom.	EU-Kommissionen
ENISA	Den Europæiske Cybersikkerhedsmyndighed
ESRB	European Systemic Risk Board - Det Europæiske Systemiske Risikoråd
SRB	Single Resolution Board – Den fælles bankafviklingsmyndighed indenfor bankunionen
EU-SCICF	EU Systemic Cyber Incident Coordination Framework - Et rammeværk foreslået af ESRB til koordinering ved større cyberhændelser
ICT ell. IKT	Det samme som IT ell. it
IR	Incident Reporting (hændelsesrapportering)
ICT RMF	ICT Risk Management Framework (rammer ell. rammeværk for it-risikostyring)
TPSP	Third party service providers, tredjepartsleverandører (it-leverandører)
TPRM	Third party risk management, risikostyring ift. tredjeparter (NIST , C-SCRM)
CSIRT	Computer Security Incident Response Team
L1/L2 retsakter	Level 1: Direktiver og forordninger fra Rådet og EP; Level 2: Gennemførelsesforordninger mv. fra Kommissionen
NIST	National Institute for Standards and Technology, US regeringsorgan, som bl.a. har udarbejdet rammer for styring af cyberrisici

FINANSTILSYNET

Tak!

Jan Jans | jja@ftnet.dk