KROMANN
REUMERT

Ledelsens juridiske ansvar for

Cybersikkerhed i IoT produkter

v/ Christel Teglers og Lasse Vibjerg

Oplæg hos Dansk Standard 24. januar 2023

En flodbølge af digital regulering er på vej

"*A Europe fit for the digital age*" er ét EU Kommissionens seks strategiske fokusområder for 2019-2024. Derfor er iværksat et ambitiøst og omfattende lovprogram med en lang række fokusområder og konkret lovgivning, som vil ramme det digitale marked over de næste år.

Digital Services Act

Ensuring a safe and accountable online environment

Digital Markets Act

Ensuring fair and open digital markets

DATA ACT

Europe aims to empower businesses and people in a human-centred, sustainable and more prosperous digital future.

European Commission

The Cybersecurity Strategy

EU Cybersecurity Act

NIS2 Directive

THE EUROPEAN DATA STRATEGY

SHAPING EUROPE'S DIGITAL FUTURE

Digital inclusion

A Europe fit for the digital age

Empowering people with a new generation of technologies

A European cybersecurity certification framework

Skills

20 million employed **ICT specialists**, more graduates + gender balance

80% of adults can **use tech** for everyday tasks

Government

Key Public Services - 100% online

Everyone can **access health records online**

Everyone can use **eID**

Infrastructure

Gigabit connectivity for everyone, **high-speed mobile coverage** (at least 5G) everywhere

EU produces 20% of world's **semiconductors**

10 000 **cloud edge nodes** = fast data access

EU **quantum computing** by 2025

Business

75% of companies using **Cloud, AI or Big Data**

Double the number of **unicorn startups**

90% of **SMEs taking up tech**

Shaping Europe's digital future

Artificial Intelligence

Achieving better healthcare, safer and cleaner transport, more efficient manufacturing, and cheaper and more sustainable energy through AI

A European approach to excellence in AI

EU Cyber Resilience Act

For safer & more secure digital products

Kilde: EU Kommissionens hjemmeside

EU tager affære, fordi utilstrækkelig cybersikkerhed i IoT produkter har samfundsmæssige konsekvenser

IoT produkterne vælter ud i vores hjem og i industrien

"*The rollout of over 41 billion IoT devices is expected by 2025*"

(EU Kommissionen med henvisning til International Data Corporation)

Produkterne er allerede nu mål for cyberangreb

"*Hardware and software products are increasingly subject to successful cyberattacks, leading to an estimated global annual cost of cybercrime of EUR 5.5 trillion by 2021*" (Explanatory memorandum til Cyber Resilience Act)

Med store samfundsmæssige omkostninger til følge

"*In a connected environment, a cybersecurity incident in one product can affect an entire organisation or a whole supply chain, often propagating across the borders of the internal market within a matter of minutes. This can lead to severe disruption of economic and social activities or even become life threatening.*" (Explanatory memorandum til Cyber Resilience Act)

Cyber Resilience Act er EU's svar

- Forslag til en **forordning**
- Fremsat af **EU Kommissionen** den 15. september 2022
- Skal opfylde **to overordnede formål**:

Produkter med tilstrækkelig cybersikkerhed igennem hele deres livscyklus

Tilstrækkelig information og instruktion til brugerne om cybersikkerhed

- Når/hvis forslaget vedtages, finder reglerne anvendelse **2 år** efter vedtagelsen (rapporteringskrav efter 1 år)
- Men virksomheder, der har berøring med IoT produkter, skal begynde at **forberede sig allerede nu**

Forordningen omfatter (stort set) alle produkter, som er forbundet med et andet produkt eller et netværk

"This Regulation applies to products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network" (artikel 2)

Hvad er et produkt?

"'product with digital elements' means any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately"

Hvad er ikke omfattet?

- Cloud services (Saas)
- Open source
- Visse produkter omfattet af anden lovgivning, fx medicinsk udstyr og køretøjer

Produkterne skal leve op til krav om cybersikkerhed og procedurer for løbende håndtering af sårbarheder

Indbygget cybersikkerhed
Produkterne skal være designet, udviklet og produceret på en måde, som sikrer tilstrækkelig cybersikkerhed baseret på en risikovurdering

Håndtering af sårbarheder
Producenten skal have procedurer og politikker for løbende håndtering af sårbarheder, herunder sikkerhedsopdateringer og informationer til myndigheder og brugerne

Forordningen er en del af EU's produktsikkerhedslovgivning

Overensstemmelsesvurdering

Produkterne skal undergives en overensstemmelsesvurdering, før de sættes på markedet

Bemyndigede organer

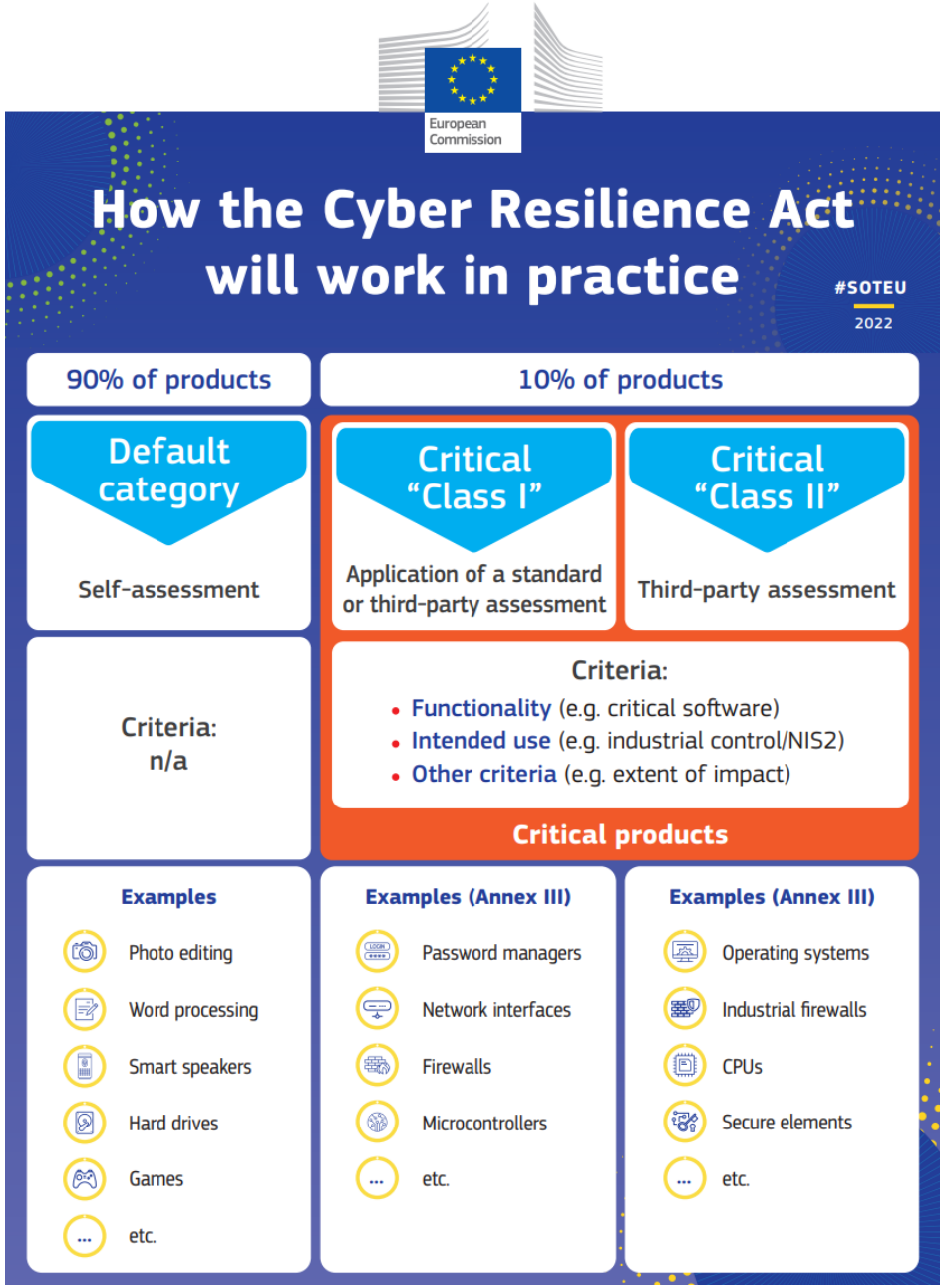
For visse kritiske produkter skal bemyndigede organer (tredjeparter) inddrages i vurderingen

CE mærkning

Produkterne skal CE mærkes som bekræftelse på, at de opfylder forordningens krav

Standarder

Produkterne formodes at opfylde kravene, hvis producenten har fulgt EU harmoniserede standarder



Kilde: EU Kommissionen, Cyber Resilience Act Factsheet

Forordningen placerer det primære ansvar hos producenten, men også importører og distributører har forpligtelser

Producent

- ✓ Cybersikkerhed i planlægning, design, udvikling, produktion og vedligeholdelse
- ✓ Risikovurdering
- ✓ Politikker og procedurer for løbende håndtering af sårbarheder igennem hele produktets livscyklus, herunder sikkerhedsopdateringer
- ✓ Teknisk dokumentation
- ✓ Overensstemmelsesvurdering
- ✓ Overensstemmelseserklæring
- ✓ CE mærkning
- ✓ Information og instruktion til brugerne
- ✓ Rapportering om angreb og sårbarheder
- ✓ Samarbejde med myndigheder

Importør/ distributør

- ✓ Sikre at producenten har opfyldt sine forpligtelser (importører)
- ✓ Agere med ”due care” i relation til forordningens krav (distributører)
- ✓ Sikre at produktet er CE mærket og ledsaget af informationer og instruktioner
- ✓ Reagere, hvis der er grund til at tro, at produktet ikke lever op til forordningen
- ✓ Samarbejde med myndigheder

Kunde/ slutbruger

- ✓ Efterleve instruktionerne og bruge produktet på en sikker måde i overensstemmelse med formålet og den tiltænkte anvendelse

Utilstrækkelig cybersikkerhed kan medføre bødeansvar, erstatningsansvar, ledelsesansvar og ”interne tab”

Cyber Resilience Act medfører bødeansvar

Overtrædelse	Bødeniveau
Grundlæggende krav til cybersikkerhed og procedurer for håndtering af sårbarheder	Op til EUR 15 mio. eller 2,5 % af årlig omsætning (højeste af de to)
Andre forpligtelser i forordningen	Op til EUR 10 mio. eller 2 % af årlig omsætning (højeste af de to)
Ukorrekt information til myndigheder eller bemyndigede organer	Op til EUR 5 mio. eller 1 % af årlig omsætning (højeste af de to)

Det samlede ansvars- og risikobillede

Producent

Importør/ distributør

- **Bødeansvar** – NIS2, CRA og GDPR
- **Erstatningsansvar** – Indkapsle risici gennem kontraktregulering
- **Produktansvar** – Objektivt ansvar for ”defekte” produkter
- **Ledelsesansvar** – Ansvar for at føre kontrol med virksomhedens risici

Kunde/ slutbruger

- **Interne tab og omkostninger** – Risiko for tab af data, oprydning og retssager mv.
- **Muligheder for kompensation** – Særligt fokus på kontraktregulering
- **Ledelsesansvar** – Ansvar for at føre kontrol med virksomhedens risici

Ledelsen har bredt skøn for kontrol med cybersikkerhed

– men det kræver et oplyst grundlag og et blik for, at IoT indebærer særlige ansvarsproblematikker (som lovgiver endnu ikke har en løsning på)

- Selve ledelsesansvaret er et civilretligt culpaansvar efter dansk ret
  - Herunder overholdelse af selskabslovens §115 om etablering af "*fornødne procedurer for risikostyring og interne kontroller*"
- Relativ ansvarsnorm – krav om "forsvarlig adfærd" der ikke er "uagtsom"
- Bred margin for forretningsmæssige beslutninger, forudsat at de er baseret på et forsvarligt grundlag (business judgment rule)

  MEN
  - kræver et oplyst grundlag!

  OG
  - overholdelse af minimumskrav i lovgivning er ikke underlagt et skøn, og er dermed heller ikke underlagt business judgment rule, og på den måde stiller (flere og skærpede) regler for virksomheden også krav til bestyrelsen og direktionen

Praktiske kontrolspørgsmål fra ledelsen i relation til IoT

- ***Fejl i udstyr***: Systemfejl eller produktnedbrud kan forårsage (fysiske) skader på ting eller personer. Hvem har ansvaret, hvis 1) noget vi producerer eller distriberer går galt, eller 2) hvis en medarbejder eller en kunde kommer til skade på grund af et defekt produkt, vi har købt og anvender? Det kan f.eks. være en remote blodtryksmåler, der måler forkert, eller en varmetermostat, der fejler, og ødelægger produktionsudstyr.
- ***Databeskyttelse***: IoT produkter kan indsamle store mængder (bruger)data. Brud på sikkerhed i netværk eller produkter kan føre til læk af data, der kan bruges til f.eks. identitetstyveri, cyberstalking og ulovlig markedsføring. Hvor hører vi til i kæden: Er vi dataansvarlig eller databehandler? Hvem opbevarer data? Har vi styr på vores forpligtelser overfor de personer, hvis data vi indsamler eller opbevarer? Hvem har ansvaret, hvis (person)data lækkes?
- ***Cybersikkerhed***. IoT produkter er afhængig af software, og software kan hackes. Har vi beskyttet os med gængse sikkerhedsforanstaltninger, f.eks.:
  - Built-in Security – f.eks. såkaldte "hardened" produkter hvor sikkerhed er integreret med hardware og firmware.
  - Kryptering – implementeret af producenten og går igennem systemer
  - Risikoanalyse – identificeret og begrænset trusler i design og produktvalg
  - Autentificering – privilegerede rettigheder og adgangskontrol
- ***Forsikring / kontrakter***: Har vi forsikring i dag, der dækker vores ansvar som producent, distributør eller (bruger)virksomhed hvis der sker skade på ting eller personer, vi er ansvarlige for – og er ansvaret håndteret i vores kontrakter?

KROMANN
REUMERT

Spørgsmål

Kontakt os

Christel Teglers
Partner, København

Dir. +45 38 77 46 93
Mob. +45 61 61 30 34

cht@kromannreumert.com

Lasse Vibjerg
Advokat, København

Dir. +45 38 77 42 07
Mob. +45 20 19 74 54

lvi@kromannreumert.com