# Cyber Resilience Act – Fra advokatens og teknikerens perspektiv

Jeppe Bjerre, specialist, Force Technology
Jesper Løffler Nielsen, IT-advokat, Focus advokater

# Cyber Resilience Act – Fra advokatens og teknikerens perspektiv

- Lovgivningsprocessen frem til i dag
- De største “knaster“ undervejs
- Den endelige forordning
- Forordningens scope, opbygning og indhold
- De materielle sikkerhedskrav – Annex 1
- Conformity Assesment, standarder og CE-mærkning
- Foreløbige tanker om CRA’s rolle nu og i fremtiden

# Lovgivningsprocessen frem til i dag

**2020-2022: EU erkender behov for at stille cybersikkerheds-krav til producenter af produkter/software**

- Ekspertstudie bestilt af Kommissionen: Study on the need of Cybersecurity requirements for ICT products
- Kommissionens Impact assesment: Cyber Resilience Act - Impact assessment

**2022-2024: Kommissionens udkast og forhandlinger i EU**

- Kommissionens udkast (september 2022): EUR-Lex - 52022PC0454 - EN - EUR-Lex (europa.eu)

*"The proposal for a regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act, bolsters cybersecurity rules to ensure more secure hardware and software products."*

- Forhandlinger i Parlamentet og Rådet – se næste slide om "de største knaster"

# De største "knaster" undervejs

**Uklart scope**

Digitaliserings- og ligestillingsministeriet, Samlenotat, maj 2023:

*"Både erhvervsliv og medlemsstater har overordnet taget positivt imod forslaget. Det gælder særligt det høje ambitionsniveau, hvor forslaget dækker produktområdet bredt. Der ses dog et behov for yderligere klarhed over forordningens anvendelsesområde, fx i forhold til om digitale tjenester og processer er omfattet"*

**Konsekvenser for Open Source-industrien, jf. utallige høringssvar mv:**

- The EU's Proposed Cyber Resilience Act Will Damage the Open Source Ecosystem - Internet Society
- EU's Proposed Cyber Resilience Act Raises Concerns for Open Source and Cybersecurity | Electronic Frontier Foundation (eff.org)
- EUs nye cyberlov er landet: Open source-udviklere »sover roligt« igen | Version2
- Open source foundations unite on common standards for EU's Cyber Resilience Act | TechCrunch

# Den endelige forordning

**Fakta:**

- Officiel dansk titel: ”*Forordning om horisontale cybersikkerhedskrav til produkter med digitale elementer*”
- Omfang: ca. 71 artikler + 8 bilag (334 sider i aktuel udgave, ender formentlig omkring 100 i kondenseret form)
- Type af regulering: Produktsikkerhedsregulering (NLF)
- Risikobaseret: Forskellige krav alt efter hvilken kategori af AI system, der er tale om
- Materielle krav: ”Security by Design”, uddybet i Annexes, særligt Annex 1 (omfattende og detaljerede), herunder krav til SBOM.
- Pligtsubjekter: Både producenter (”*manufacturer*”) samt andre led i forsyningskæden (”*importer*”, ”*distributor*” mv) + særregulering af Open Source-miljøet (”*Open Source Steward*”)

**Tidslinje**:

- Endelig vedtagelse i parlamentet i juli 2024 – forventes publiceret i EU-tidende i løbet af efteråret.
- Størstedelen af forordningen finder anvendelse fra 2027

# Scope

**CORRIGENDUM**
**18.7.2024**

*Article 2*

*Scope*

1. *This Regulation applies to **products with digital elements** made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network*
2. *(…)*

*Article 3*

*Definitions*

*For the purposes of the Regulation, the following definitions apply:*

1. ***'product with digital elements'** means a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately;*
2. *(…)*

| Kapitel / Afdeling (Chapter) | Artikel |
|---|---|
| **Preamble** | N/A |
| **Chapter I: General provisions** | **Art. 1 – 12** |
| **Chapter II: Obligations of economic operations and provisions in relation to free and open-source software** | **Art. 13 – 26** |
| **Chapter III: Conformity of the product with digital elements** | **Art. 27 – 34** |
| **Chapter IV: Notification of conformity assessment bodies** | **Art. 35 – 51** |
| **Chapter V: Market surveillance and enforcement** | **Art. 52 – 60** |
| **Chapter VI: Delegated powers and committee procedure** | **Art. 61 – 62** |
| **Chapter VII: Confidentiality and penalties** | **Art. 63 – 65** |
| **Chapter VIII: Transitional and final provisions** | **Art. 66 – 71** |

| |
|---|
| **ANNEX I:** Essential Cybersecurity requirements |
| **ANNEX II:** Information and instructions to the user |
| **ANNEX III:** Important products with digital elements |
| **ANNEX IV:** Critical products with digital elements |
| **ANNEX V:** EU declaration of conformity |
| **ANNEX VI:** Simplified EU declaration of conformity |
| **ANNEX VII:** Contents of the technical documentation |
| **ANNEX VIII:** Conformity assessment procedures |

# De materielle sikkerhedskrav – Annex 1

Del I

1) Produkter med digitale elementer skal designes, udvikles og produceres på en sådan måde, at de sikrer et passende cybersikkerhedsniveau baseret på risiciene.

2) På grundlag af den cybersikkerhedsrisikovurdering, der er omhandlet i artikel 13, stk. 2, og hvor det er relevant, skal produkter med digitale elementer....

Del II

Håndtering af sårbarheder

- Software BoM
- Software opdatering
- Regelmæssige test af sikkerhed i produkt
- Offentliggørelses politik

*Security by design*

# Conformity Assesment, standarder og CE-mærkning

**Basic products**

- Module A
- Module B+C
- Module H
- EU Cybersecurity certification scheme

**Important products Class I**

- Module A (Full hEN)
- Module B+C
- Module H
- EU Cybersecurity certification scheme (AL Substantial)

**Important products Class II**

- Module B+C
- Module H
- EU Cybersecurity certification scheme (AL Substantial)

**Critical products**

- EU Cybersecurity certification scheme (AL >= Substantial) for the specific product type
- As Class II, if no scheme exists

FOCUS ADVOKATER

# Foreløbige tanker om CRA's rolle nu og i fremtiden

1. CRA får en bred anvendelse og de fleste producenter af helt eller delvist digitale produkter vil blive omfattet

2. CRA er EU's svar på en global bevægelse i retning mod mere "Security by Design" – cybersikkerhed skal, ligesom privatlivsbeskyttelse, være en integrereret del af design- og udviklingsprocessen.

3. CRA er på mange måder "the missing link" ift. GDPR, NIS2 og DORA – hvor de tre regelsæt rammer kundesiden hardest, vil CRA pålægge det primære ansvar på leverandørsiden.

4. Store dele af CRA's krav er sund fornuft og afspejler god cybersikkerhed anno 2024 – den store forskel ligger i, at det nu bliver et lovkrav, og overholdelse af kravene skal dokumenteres.

5. Start med at få overblik over hvilke elementer, der vil tage længst tid at få implementeret. For nogen er det sårharhedshåndtering, for andre vil det være udfordrende at få teknikken til at være i overenstemmelse.

# SPØRGSMÅL?



FOCUS ADVOKATER

# Jesper Løffler Nielsen

## Profil

- Certificeret IT-advokat og associeret partner hos Focus Advokater P/S
- Leder af Tech Teamet – specialiser i digital regulering

**Forskning og undervisning**

- Erhvervs-PhD i IT-ret (2013 – 2016)
- Ekstern lektor i IT-ret, Persondataret mv. (2010 -)
- Underviser på IT Vest's Master IT-fagpakke:

*"Cybersikkerhed, Privacy og Regulering"*

**Andet**

- Bestyrelsesmedlem i Danske IT-Advokater
- Netværksleder for Technology Denmarks netværk: *"Innovation & Compliance"*
- Udpeget til EDPB "Pool of Experts" ift. digitale teknologier
- Medlem af Dansk Standards AI-udvalg



FOCUS ADVOKATER