FOCUS
ADVOKATER

Historisk og aktuel regulering af digitale teknologier

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

Planen for dagen:

- **Generelt om regulering af digitale teknologier og EU's "Digitale Årti"**

- **Indledende overblik:**
  - Cybersikkerhedsregulering
  - Dataregulering
  - AI-regulering

→ Der dykkes mere ned i emnerne på kommende undervisningsgange

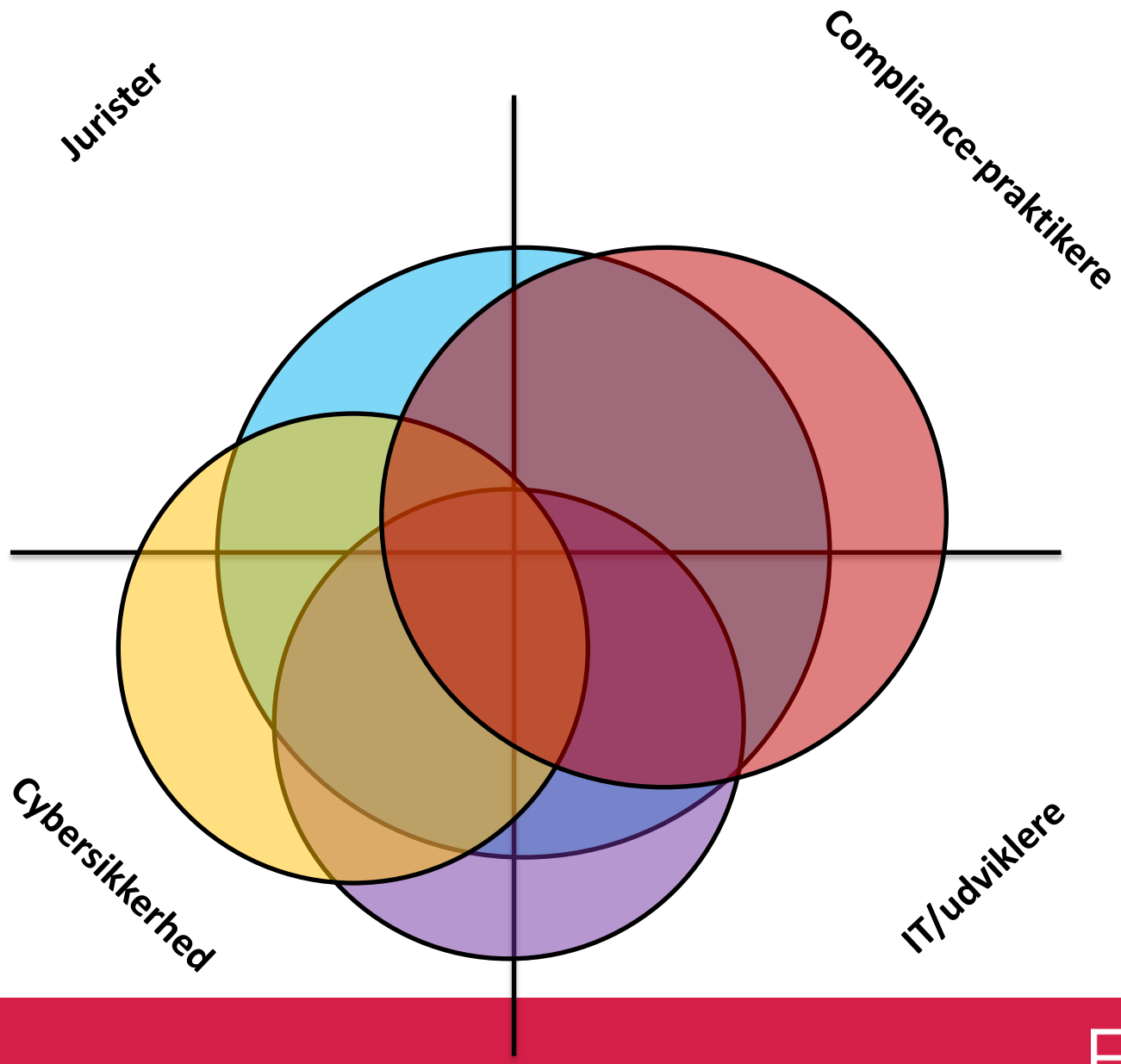
Digital regulering og behovet for forskellige kompetencer

GDPR

Cyber Resilience Act

NIS2

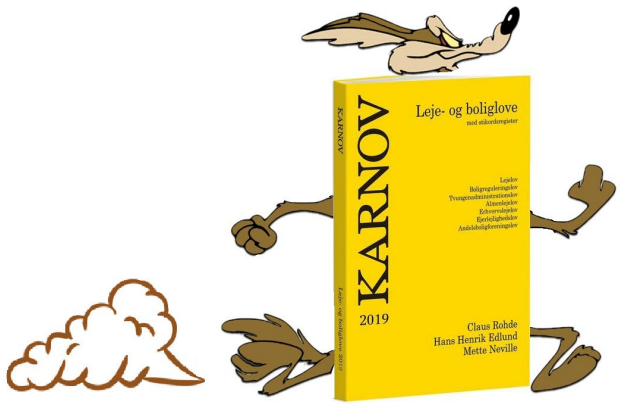
AI Act

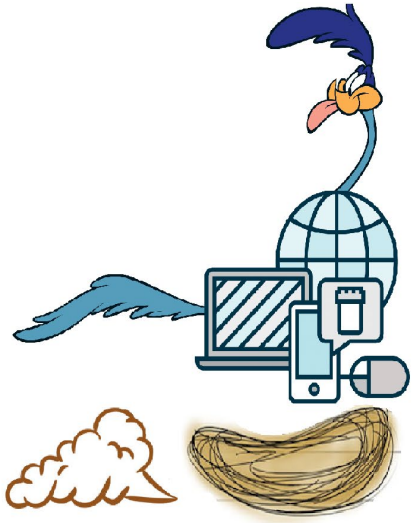


FOCUS ADVOKATER

HISTORIK FOR REGULERING AF DIGITALE TEKNOLOGIER

Grundlæggende udfordring: Teknologien udvikler sig hurtigere end juraen





”Man ser i vore dage, at den tekniske udvikling skånselsløst sprænger de forudsætninger, som retsordenen har indrettet sig under, og tvinger juristerne til at foretage en omvurdering af hidtil uanfægtede retsprincipper, undertiden endog således, at man alvorligt må overveje at bygge systemet inden for et retsområde op fra bunden for at bevare balancen på området.”

Fra artiklen ”*Magnetofoner* [spolebåndoptager, red.] *i ophavsretlig belysning*”, 1955

FOCUS ADVOKATER

Tidslinje over udviklingen de sidste 50 år

1978: Registerlovene

1981: Europarådet Konvention 108

1991: Computer Programs Directive

1995: Persondatadirektivet

1996: Databasedirektivet

2000: E-handelsdirektivet

2001: Infosocdirektivet

2002: E-privacy direktivet

2003: PSI-direktivet

2014: EiDAS Directive

2015: Digital Single Market

2016: GDPR

2016: NIS-direktivet

2019: Cybersecurity Act

2022: NIS2

2022: CER

2022: DORA

2023: Digital Markets Act

2023: Digital Services Act

2023: Digital Governance Act

2023: Cyber Resilience Act

1971: Første e-mail bliver sendt

1973: Den første mobiltelefon

1974: Første personlige computer blev bygget

1981: Første laptop

1988: Første transatlantiske fiberoptiske kabel bliver lagt

1989: ”World wide web”

1994: Bill Clinton er den første amerikanske præsident til at sende en e-mail

1996: DVD bliver lanceret

1998: Computeren Deep Blue vinder over skakmesteren Garri Kasparov

2001: Windows XP bliver lanceret

2004: Facebook bliver lanceret

2007: Den første iPhone bliver lanceret

2010: Internettet har 2 mia. brugere, hvilket svarer til ca. 29% af befolkningen

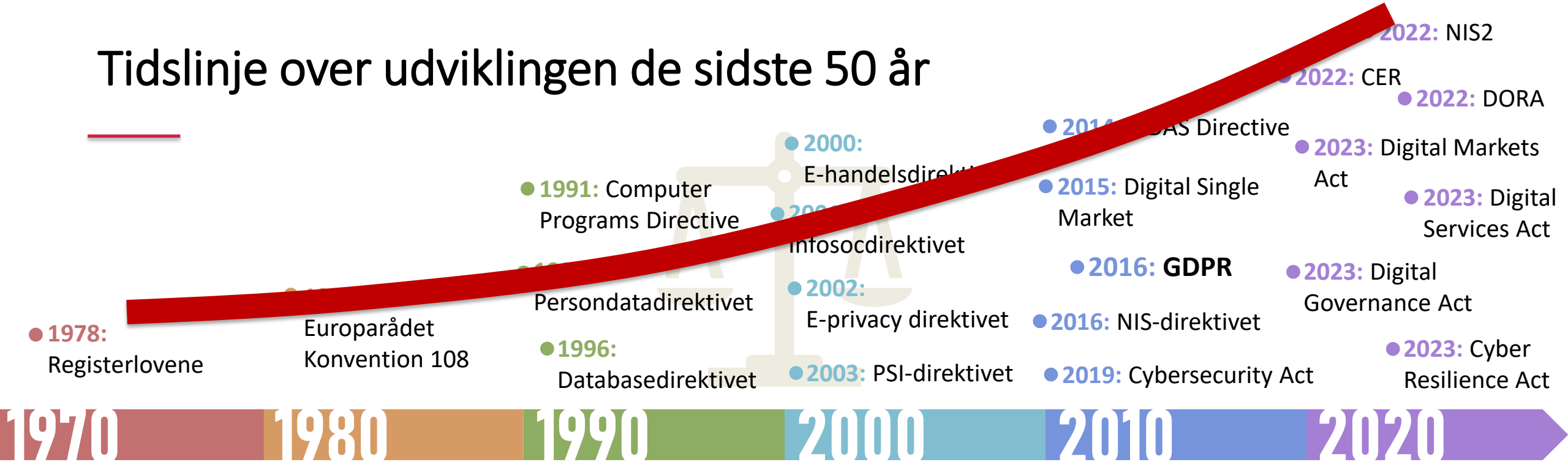
2013: Edward Snowden afslører NSA’s masseovervågning

2016: VR-brillerne, Oculus Rift lanceres

2020: Internettet har cirka 4,7 mia. brugere, hvilket svarer til 60% af klodens befolkning

2022: ChatGPT lanceres

Tidslinje over udviklingen de sidste 50 år



1978: Registerlovene

Europarådet Konvention 108

1991: Computer Programs Directive

1996: Databasedirektivet

2000: E-handelsdirektiv

Persondatadirektivet

Infosocdirektivet

2002: E-privacy direktivet

2003: PSI-direktivet

2014: BAS Directive

2015: Digital Single Market

2016: GDPR

2016: NIS-direktivet

2019: Cybersecurity Act

2022: NIS2

2022: CER

2022: DORA

2023: Digital Markets Act

2023: Digital Services Act

2023: Digital Governance Act

2023: Cyber Resilience Act

1970 | 1980 | 1990 | 2000 | 2010 | 2020

1971: Første e-mail bliver sendt

1973: Den første mobiltelefon

1974: Første personlige computer blev bygget

1981: Første laptop

1988: Første transatlantiske fiberoptiske kabel bliver lagt

1989: ”World wide web”

1994: Bill Clinton er den første amerikanske præsident til at sende en e-mail

1996: DVD bliver lanceret

1998: Computeren Deep Blue vinder over skakmesteren Garri Kasparov

2001: Windows XP bliver lanceret

2004: Facebook bliver lanceret

2007: Den første iPhone bliver lanceret

2010: Internettet har 2 mia. brugere, hvilket svarer til ca. 29% af befolkningen

2013: Edward Snowden afslører NSA’s masseovervågning

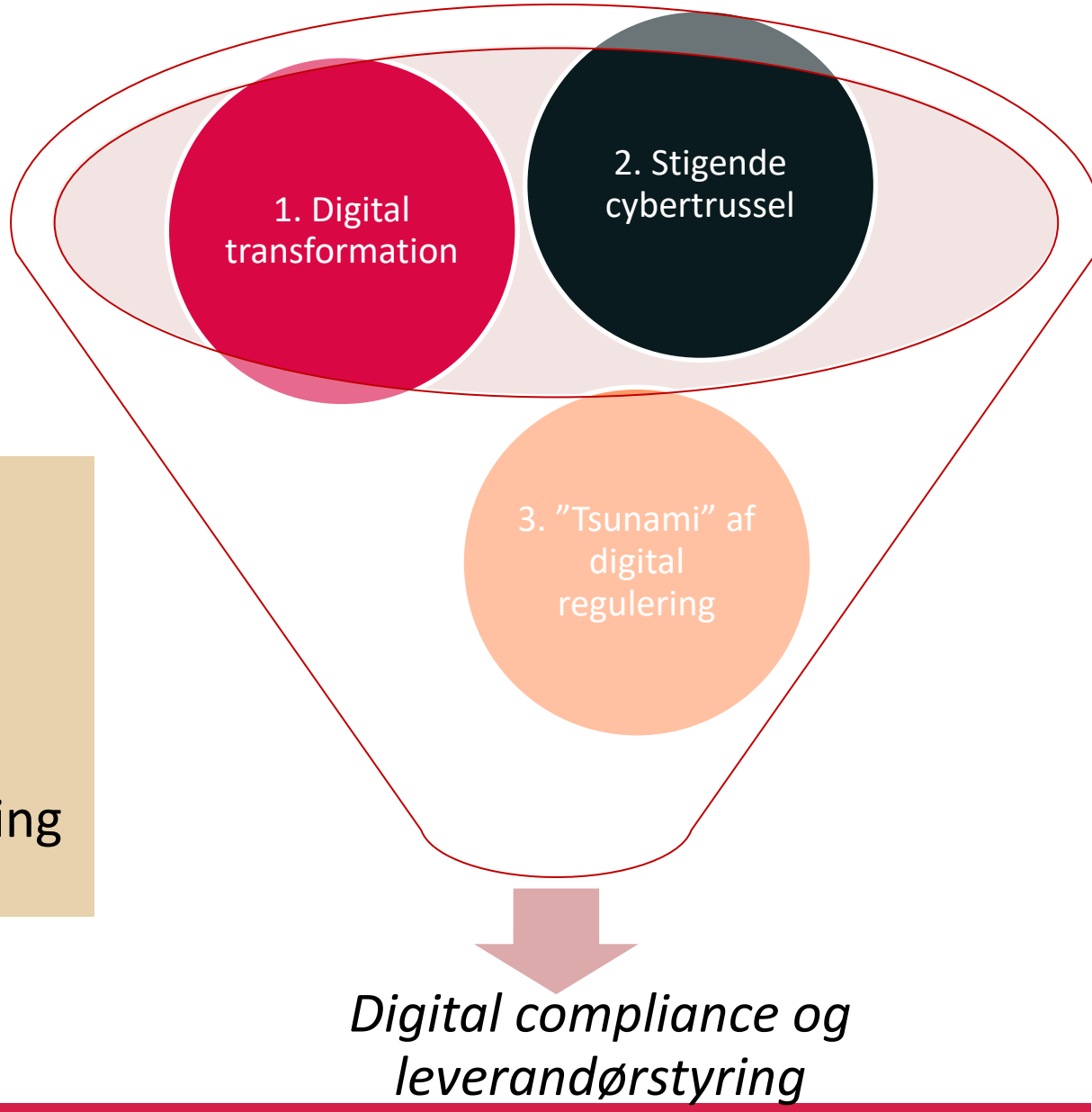
2016: VR-brillerne, Oculus Rift lanceres

2020: Internettet har cirka 4,7 mia. brugere, hvilket svarer til 60% af klodens befolkning

2022: ChatGPT lanceres

Stigende krav til digital compliance og leverandørstyring

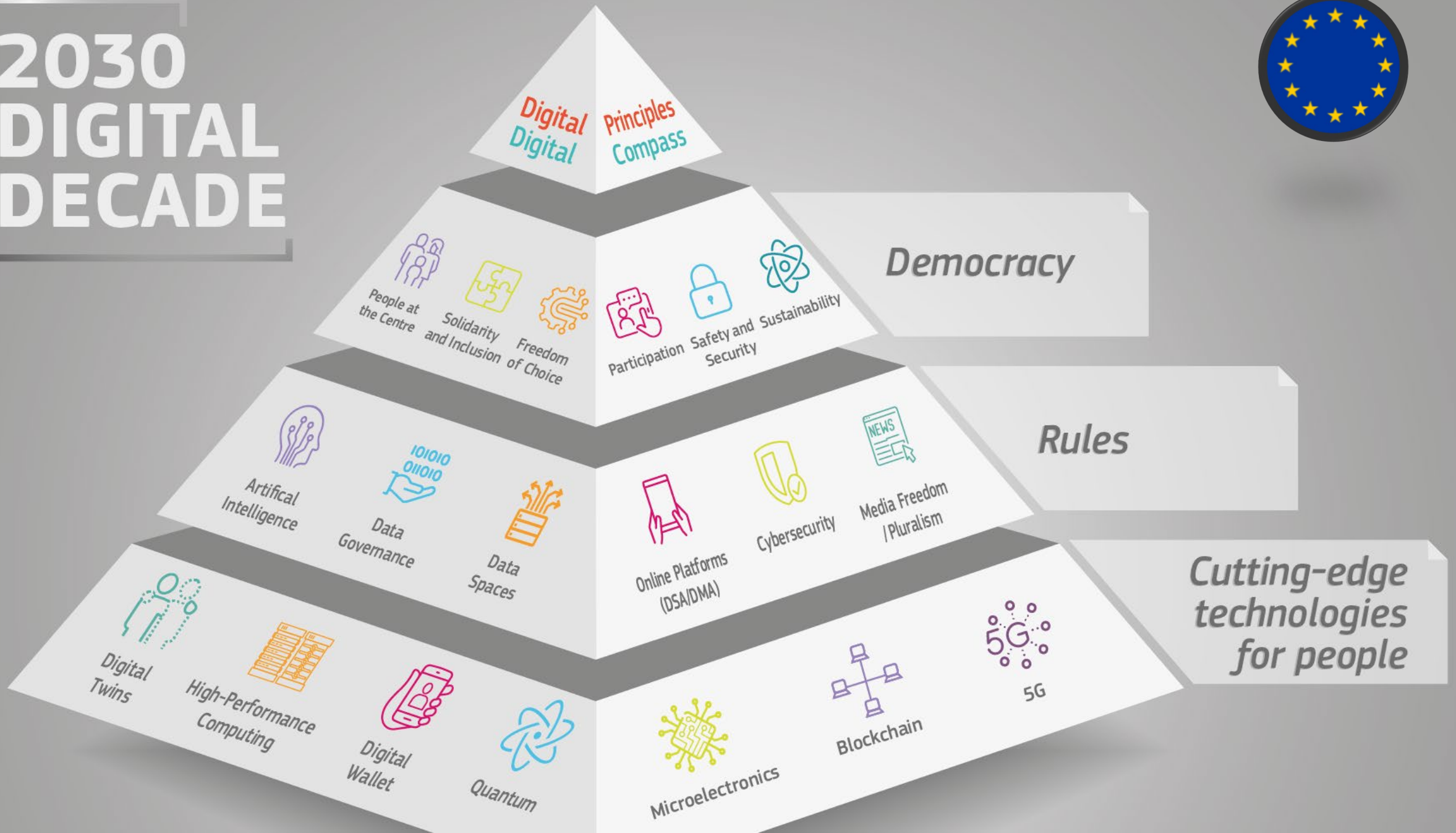
1. Trend nr. 1: Digital transformation
2. Trend nr. 2: Stigende cybertrussel
3. Trend nr. 3: En ”tsunami” af digital regulering



FOCUS ADVOKATER

DIGITAL DECADE

2030 DIGITAL DECADE



Hvorfor har EU taget teten på stort set al regulering af digitale teknologier?

- Regulering af digitale teknologier har tæt tilknytning til EU's vitale interesser og arbejdsområder:

"EU ønsker at styrke sin digitale selvstændighed og fastsætte standarder, fremfor at følge standarder, som andre har fastsat, for at gøre Europa klar til den digitale alder.
Til at styre EU's digitale omstilling fremlagde Europa-Kommissionen sit politikprogram Europas Digitale Årti, der indeholder konkrete mål og objektiver for 2030 på områder som færdigheder, sikre og bæredygtige digitale infrastrukturer, digital omstilling for virksomheder og digitalisering af offentlige ydelser.
I maj 2021 vedtog Parlamentet en rapport om, hvordan Europas digitale fremtid skal se ud og opfordrer Kommissionen til yderligere at tackle de udfordringer, som den digitale omstilling har især med hensyn til at drage fordele af mulighederne ved et digitalt indre marked og ved at forbedre brugen af kunstig intelligens (KI)."

"Hvordan ser EU's strategi for den digitale omstilling ud?", Europa Parlamentet, 2021

- **Digital selvstændighed** er bl.a. et sikkerhedsanliggende.
- **Global leder** indenfor teknologi og **teknologiregulering**
- Fremme den digitale sikkerhed da det både vil beskytte EU-borgernes rettigheder og **EU's-sikkerhedspolitik**
- Fremme udvikling af europæernes **færdigheder** i den digitale verden
- Sikre **bæredygtighed**
- Skabelse af et stærkt **digitalt indre marked**
- Udvikling af teknologi, særligt **kunstig intelligens**

EU's "Digital Decade" – nye regler siden 2019

Cybersikkerhed

- **S: Cybersecurity Strategy**
- F: Cybersecurity Act
- D: NIS2
- F: DORA (finanssektor)
- D: Critical Entities Resilience/CER
- F: Cybersecurity Regulation
- F: Cyber Resilience Act
- F: Cyber Solidarity Act
- F: Information Security Regulation

Data (adgang og deling)

S: Data Strategy
F: Free Flow of Data
D: Open Data
F: Data Governance Act
F: Data Act
F: Interoperable Europe Act
F: Data Collection and Sharing Relating to Short-Term Accommodation Rental Services Act (!)
F: European Health Data Space
F: Financial Data Access

Teknologier og ansvar

S: AI Strategy + Blockchain Strategy
F: Platform-to-Business forordning/P2B
F: Digital Services Act
F: Digital Markets Act
F: MICA (kryptoaktiver)
F: AI Act
F: European Identity Wallet (!)
F: Machinery Regulation
D: Product Liability Directive (revision)
F: General Product Safety Regulation
~~D: AI Liability Directive~~

Type af dokument

S = Strategi
F = Forordning
D = Direktiv

Status

Almindelig tekst = Endeligt vedtaget
(!) = Politisk enighed, endelig ordlyd mangler
Blå = Forhandles pt. i EU
Grå = Varslede regler/Impact Assesment

EU's "Digital Decade" – nye regler siden 2019

Cybersikkerhed

- D: NIS2
- F: Cyber Resilience Act

Data (adgang og deling)

S: Data Strategy

F: Data Act

+ Common European Data Spaces

Teknologier og ansvar

S: AI Strategy + Blockchain Strategy

F: AI Act

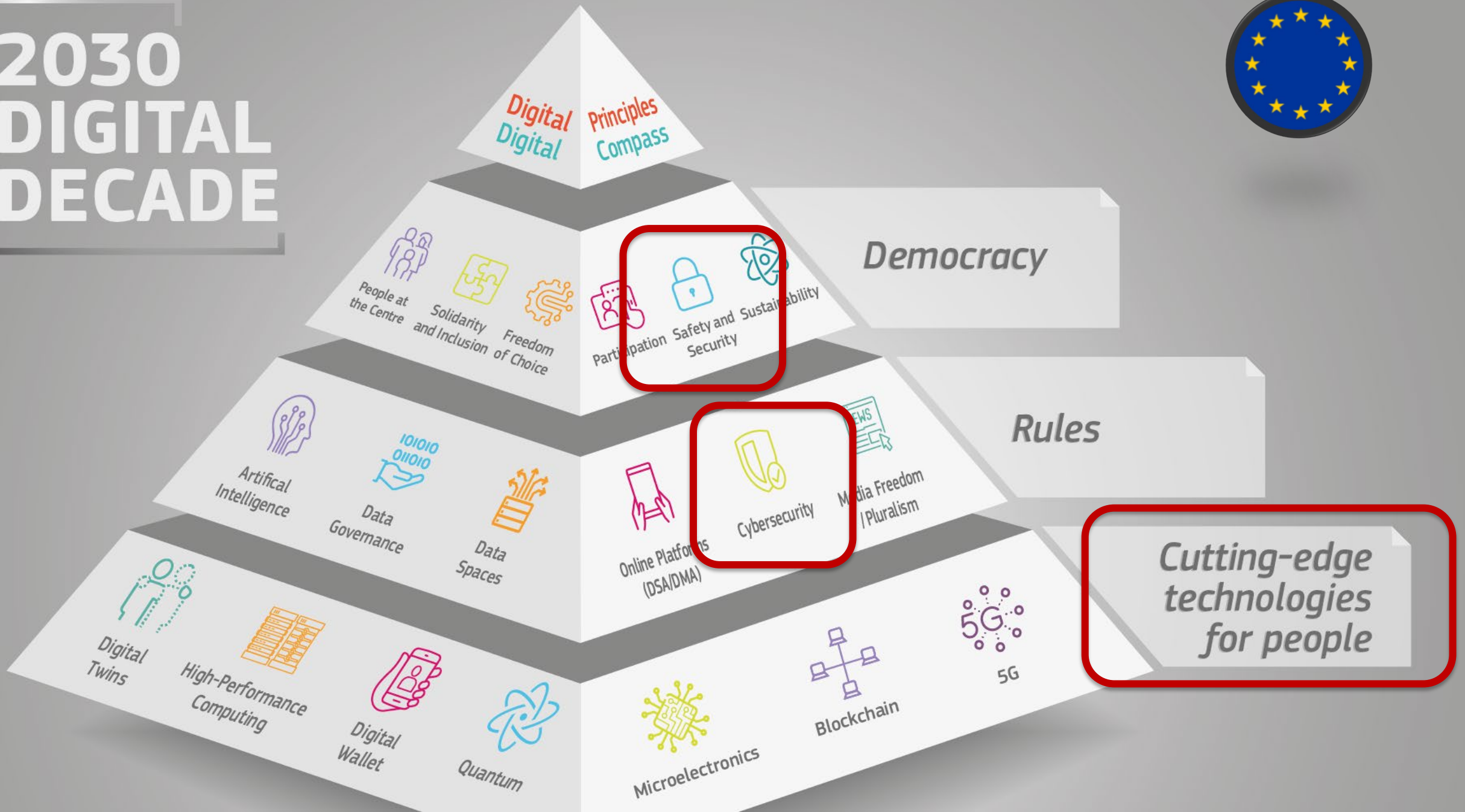
BEHOV FOR HÅNDTERING AF DEN VOKSENDE MÆNGDE CYBERRISICI

DER SKAL DRAGES NYTTE AF DATA, OG DET SKAL SKE MED RESPEKT FOR BL.A. PRIVATLIVET

AI OG FREMTIDENS TEKNOLOGIER, SKAL VÆRE SIKRE VÆRE I OVERENSSTEMMELSE MED EU'S VÆRDIER.

CYBERSIKKERHEDSREGULERING

2030 DIGITAL DECADE



Cybersikkerhed bliver i stigende krav et juridisk anliggende

Generelle krav

- Databeskyttelsesreglerne,
  inkl. en række sikkerhedsrelaterede krav

Sektorspecifikke krav

- Krav om/anbefaling ift. offentlige myndigheders efterlevelse af informationssikkerhedsstandarden ISO 2700X
- En række særregler for visse sektorer, herunder tele-, medie- og IT-sektoren, den finansielle sektor, forsyningsvirksomheder, transport, bankvæsen, sundhedssektoren mv.

Indirekte "krav" ift. sikkerhed

- IT-sikkerhed er (i stigende grad) et ledelsesanliggende, også juridisk set
  - F.eks. selskabslovens §115, nr. 2: *"sikre en forsvarlig organisation… etableret de fornødne procedurer for risikostyring og interne kontroller"*
- Kun beskyttelse af forretningshemmeligheder, hvis tilstrækkelig sikkerhed
  - Lov om forretningshemmeligheder § 2, nr. 1, litra c

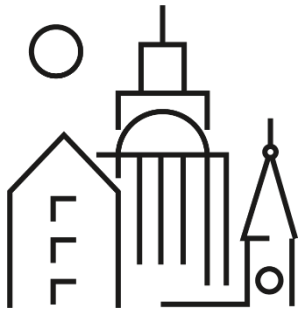
Udvalgte regler fra EU med fokus på cybersikkerhed

Lovgivning	Indhold
Databeskyttelsesforordningen (GDPR) Vedtaget – Finder anvendelse nu	Krav ved **behandling af personoplysninger**, herunder sikkerhedskrav
Cybersecurity Act Vedtaget – Finder anvendelse nu	Styrket **samarbejde mellem EU-lande**, flere beføjelser til **ENISA,** og nye **cybersikkerheds-certificeringsordninger** (certificeringer er dog fortsat under udarbejdelse).
NIS 2-direktivet Vedtaget – Finder anvendelse fra 18.10.2024	Konkrete cybersikkerhedskrav til **en lang række sektorer**. Opfølgning på NIS 1-direktivet fra 2018.
DORA-forordningen Vedtaget – Finder anvendelse fra 17.1.2025	Cybersikkerhedskrav til **finanssektoren** (skærpede sammenlignet med NIS 2).
Cyber Resilience Act (CRA) Vedtaget – Finder anvendelse 36 måneder efter ikrafttræden	Krav til cybersikkerhed i **produkter med "digitale elementer"** (software, IoT, robotter, droner, mv.).
Critical Entities Resilience (CER) Vedtaget – Finder anvendelse fra 18.10.2024	Krav til **fysisk modstandsdygtighed** over for (natur)katastrofer i en række kritiske sektorer.
Radioudstyrsdirektivet (RED) Vedtaget – Finder anvendelse fra 1.8.2024	Krav til **cybersikkerhed i radioudstyr** (både kommerciel og industriel).
Produktansvarsdirektivet (PLD) Vedtaget – Finder anvendelse 24 måneder efter ikrafttræden	"**Software**" indgår i begrebet "**produkt**", så producenter kan blive objektivt ansvarlige for **cybersikkerhedsdefekter** eller manglende/mangelfulde softwareopdateringer.
Den generelle produktsikkerhedsforordning (GPSR) Vedtaget – Finder anvendelse fra 13.12.2024	Cybersikkerhed vil indgå som en del af, om et **produkt** er "**sikkert**" for forbrugere.
Maskinforordningen Vedtaget – Finder anvendelse fra 20.1.2027	Cybersikkerhedskrav til at **maskiner** skal sikres mod **hacking** og **nedbrud.**

To retsakter med stor betydning for de kommende års cybersikkerhed

CRA

NIS2



FOCUS ADVOKATER

RISIKOVURDERINGER: ALL HAZARD APPROACH

Alle farer inkl. fysiske

LEVERANDØRSTYRING

Forsyningskæde-sikkerhed samt sikkerhed ved erhvervelse og udvikling IT-systemer.

TEKNISKE LØSNINGER

Brug af f.eks. multifaktor autentifikation, kryptografi og kryptering. Hertil medfølgende politikker.

UDDANNELSE AF PERSONALE

Personalesikkerhed, grundlæggende cyberhygiejne, politikker og uddannelse

HÅNDTERING AF HÆNDELSER

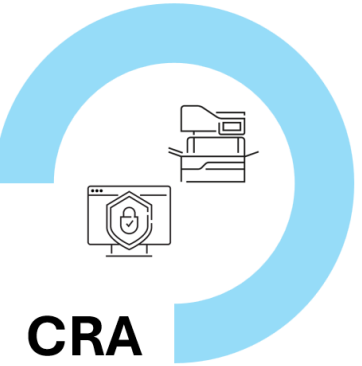
Omfatter både hændelseshåndtering og f.eks. Driftskontinuitet efter hændelser.

POLITIKKER, STRATEGIER & EVALUERING

Risikoanalyse, informationssikkerhed, samt effektiviteten af foranstaltninger

FOCUS ADVOKATER

Cyber Resilience Act



- **Formål**: At sikre, at 'produkter med digitale elementer' er cybersikre
- **Baggrund**
  - Sikkerhedsniveaut af mange produkter er utilstrækkelig
  - Et af problemerne er bl.a. manglende softwareopdateringer af produkter i deres 'levetid'
  - Forbrugerne er ikke bekendte med cybersikkerhedsmæssige risici knyttet til produkterne.
- **Omfattede aktører:**
  - Producenter, udviklere, distributører og importører af produkter i EU:
- **Krav**
  - Cybersikkerheden skal indbygges i designet, således at produkterne har et acceptabelt niveau af cybersikkerhed.
  - Løbende sikkerhedsopdateringer
  - Risikovurdering af produkter og eventuelt behov for udarbejdelse af overensstemmelsesvurderinger
  - Rapporteringsforpligtelser
- **Mål**:
  - Færre sikkerhedshændelser
  - Harmonisering af regler i hele EU – Fælles tilgang til cybersikkerheden af produkter med digitale elementer
  - Samspil med GDPR og NIS2

DATAREGULERING

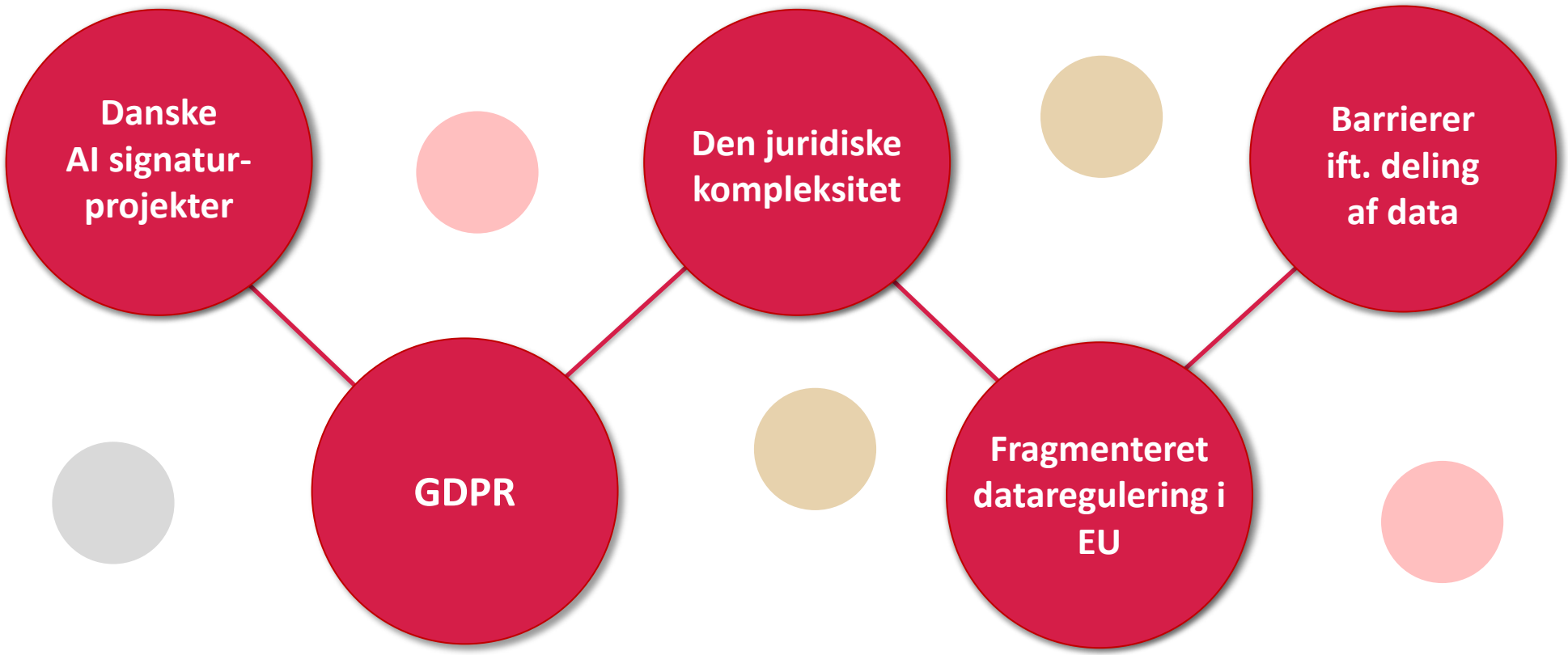
Det nye olie?

In this Briefing

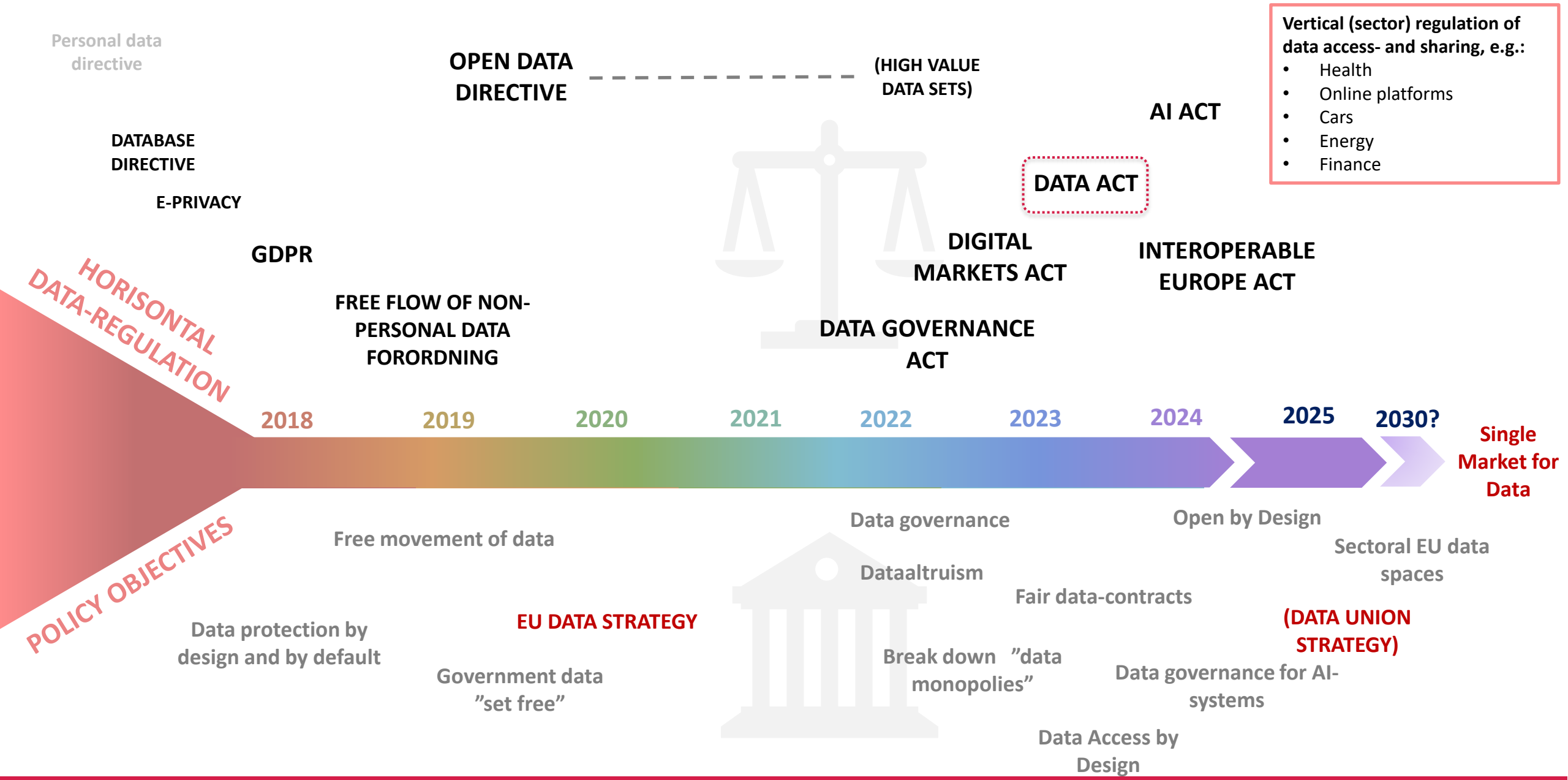
- Context
- What makes the digital economy distinct?
- Economic significance of data
- Competition issues
- Data sharing

Datadeling vil i de kommende år blive fundamental for europæiske økonomi, hvor data vil bidrage med mindst **1 billion euro i 2030**. (European Commission, 2022, European Data Market study 2021-2023, højvækst scenariet)

Udvalgte udfordringer



FOCUS ADVOKATER



FOCUS ADVOKATER

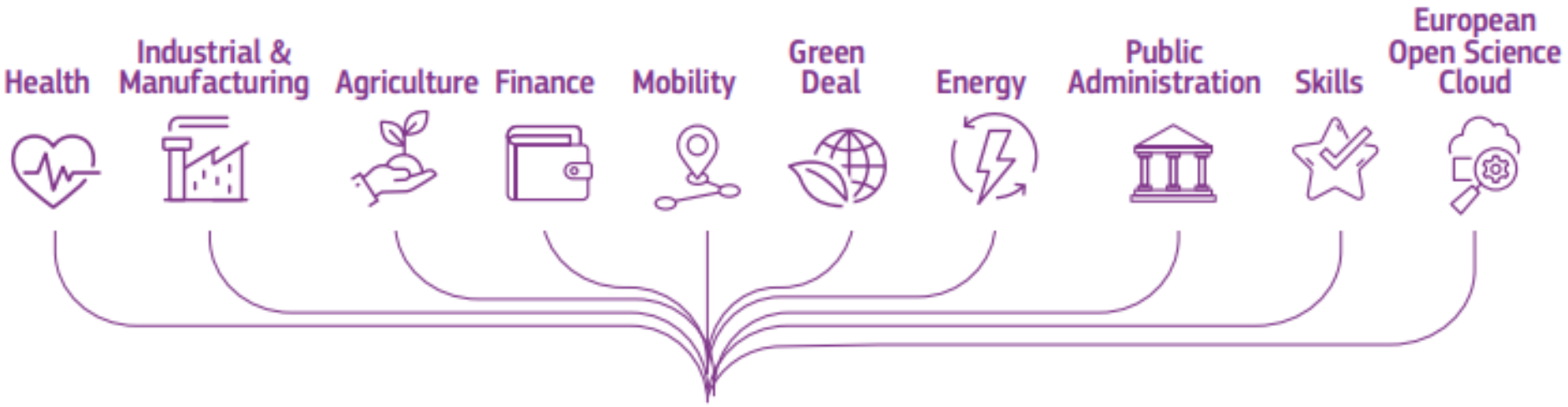
EU Data Spaces

Rich pool of data (varying degree of accessibility)

Free flow of data across sectors and countries

Full respect of GDPR

Horizontal framework for data governance and data access



— Technical tools for data pooling and sharing
— Standards & interoperability (technical, semantic)
— Sectoral Data Governance (contracts, licenses, access rights, usage rights)
— IT capacity, including cloud storage, processing and services

AI-REGULERING

AI giver bekymringer…

Gladsaxe taler ud om dataovervågning: Vi vil gerne lave en 'black box'

Kan algoritmer se ind i et barns fremtid? I Hjørring og Silkeborg eksperimenterede man på udsatte børn

Undersøgelse: Hver tredje dansker stoler ikke på kunstig intelligens i det offentlige

En undersøgelse lavet af Version2 i samarbejde med Ingeniørforeningen IDA viser, at mere end hver tredje dansker ikke har tillid til anvendelsen af kunstig intelligens i det offentliges sagsbehandling.

Leverandør: Pressen skræmmer det offentlige fra AI-projekter

Det er blandt andet dårlig presseomtale, der får det offentlige til at holde sig fra AI-projekter, mener Simon Svarrer, direktør i Schultz og udvalgsformand i IT-Branchen.

Algoritmer, Data & Demokrati (ADD-projektet) arbejder for, at demokratiet styrkes af den digitale udvikling gennem forskning, øget teknologiforståelse, digital dannelse og dialog.

… og behov for regulering

Debatten: Klar til kunstig intelligens?

DR2 | 2 SÆSONER

AFSPIL NU MIN LISTE

S2023:E11 Klar til kunstig intelligens?

Udviklingen i kunstig intelligens brager af sted. Nogle hylder teknologien, andre råber vagt i gevær - for har vi styr på konsekvenserne? Skal udviklingen sættes i bero, eller skal vi byde teknologien velkommen med åbne...

Pause Giant AI Experiments: An Open Letter

We call on all AI labs to immediately pause for at least 6 months the training of AI systems more powerful than GPT-4.

View this open letter online.

Published	PDF created	Signatures
March 22, 2023	May 5, 2023	27565

AI systems with human-competitive intelligence can pose profound risks to society and humanity,

Mens Digitaliseringsministeren vil vente på EU, lancerer SF dansk AI-udspil: »The honeymoon is over«

PLUS | Regulering af AI | 18. maj kl. 06:00 | 13

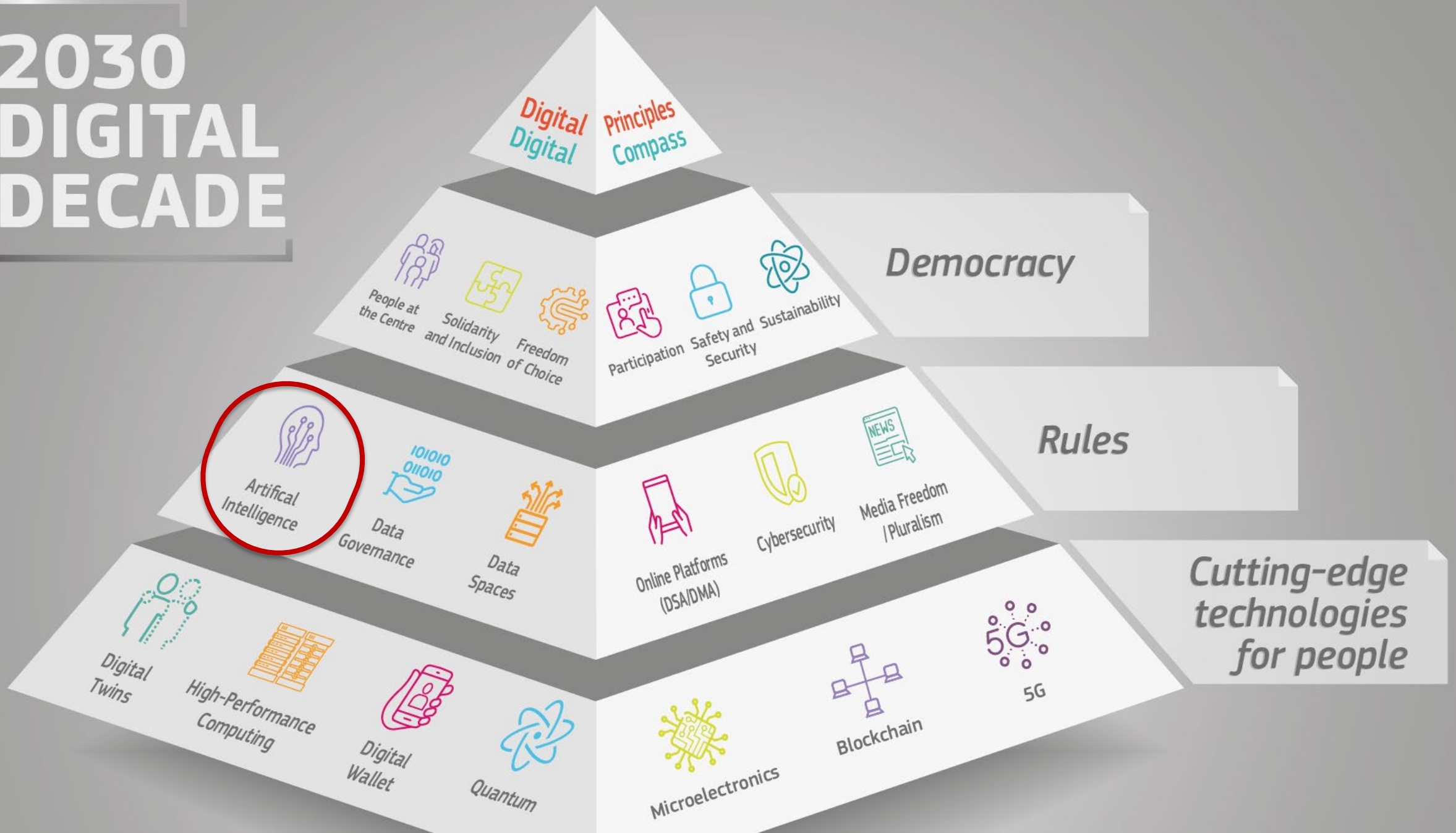
FOCUS ADVOKATER

Den juridiske definition på AI

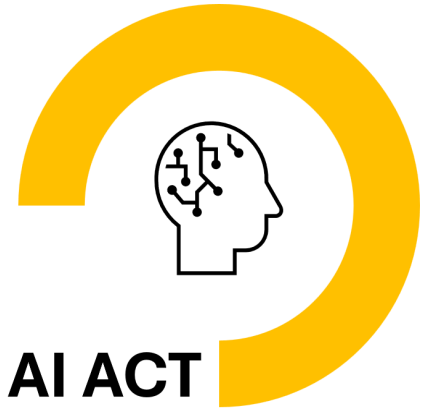
"'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."

AI Act, art. 3(1)

2030 DIGITAL DECADE



AI Act / AI forordningen



- AI-forordningen, som regulerer ansvarlig brug af kunstig intelligens i Europa, er den første lovgivning i verden på dette område.

- Relevant for mange – men stor forskel på, hvem der skal vide hvad.

Overskrifter

- Vedtaget sommer 2024, og herefter trinvis ikrafttræden fra februar 2025 og frem.
- 113 artikler og 13 bilag
- Krav afhænger af risiko – særligt tunge krav til højrisiko AI samt udbydere af AI modeller til generel brug (ChatGPT mv)
- Forpligtelser for både leverandører (”*udbyder*”) og kunder (”*idriftsætter*”)
- Håndhævelse nationalt (Digitaliseringsstyrelsen, Datatilsynet mfl.) og på EU-plan (”*European AI Board*” og ”*AI Office*”)

Overblik over forordningens forpligtelser

Forpligtelse	Artikler	Uddybning	Pligtsubjekter	Ikrafttræden
AI-færdigheder (literacy)	4	Overblik over AI-systemer, målrettet uddannelse i risici og AI Act, risikovurderinger mv	Udbydere og idriftsættere	2. februar 2025
Forbudte AI-praksisser	5	Hvis brugen af AI falder indenfor de oplistede cases, er det forbudt	Udbydere og idriftsættere	2. februar 2025
Højrisiko	6-49	Efterlevelse af materielle krav til AI-systemet (art. 9-15), kvalitetsstyring (art. 17) samt udarbejdelse af relevant dokumentation mv (art. 16-50)	Udbydere og idriftsættere - flest forpligtelser på udbydere	2. august 2026 (dog 2027 fsva. Annex I)
Gennemsigtighed	50	Der skal fremgå klart, når en bruger interagere med AI	Udbydere og idriftsættere	2. august 2026
AI-modeller til generel brug	51-56	Skærpede krav til udbydere af AI-modeller til generel brug (GPT 4.0 mv)	Udbydere af de helt store modeller (OpenAI, Google, Meta mv)	2. August 2025

TAK FOR I DAG!