



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"

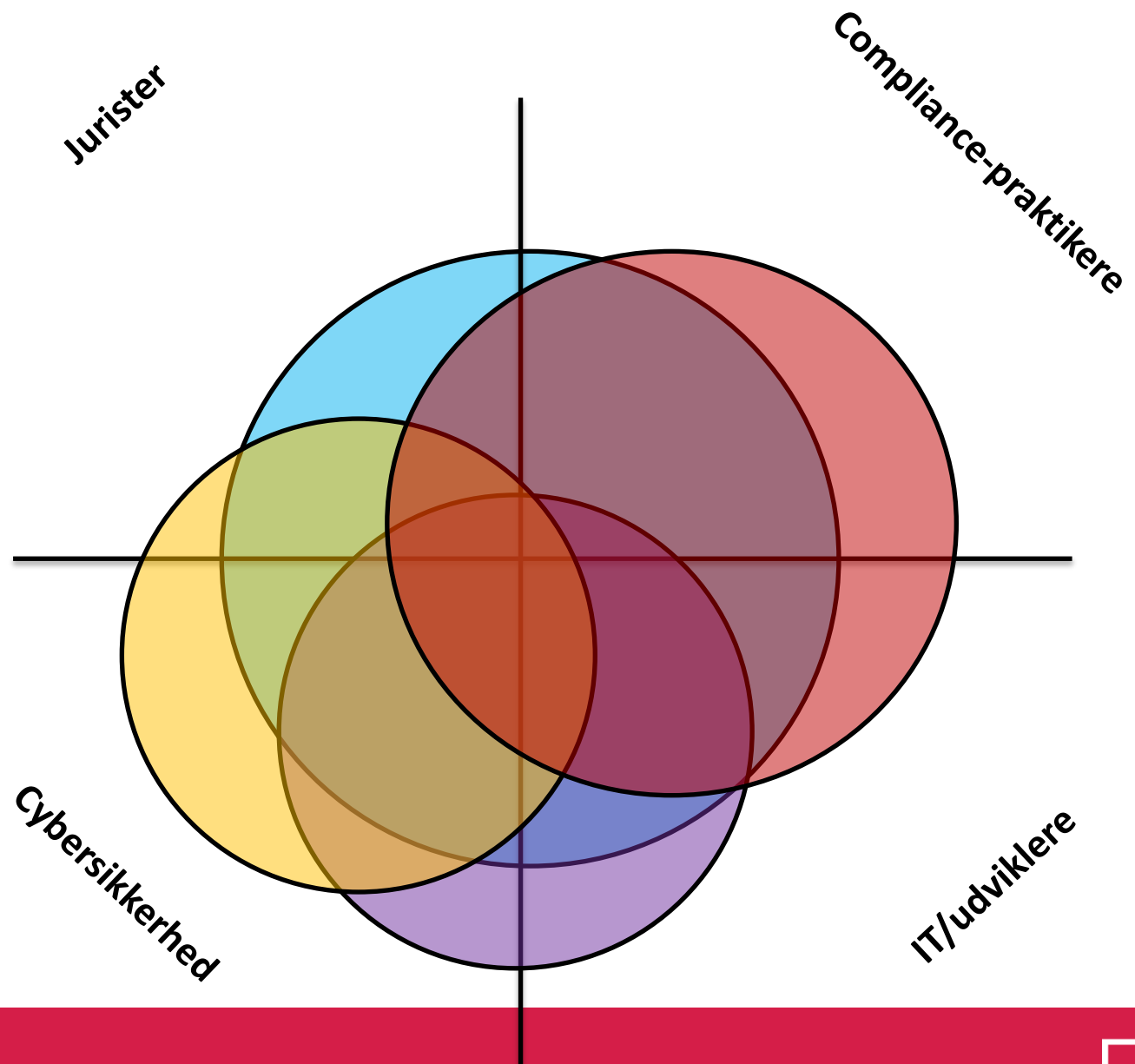
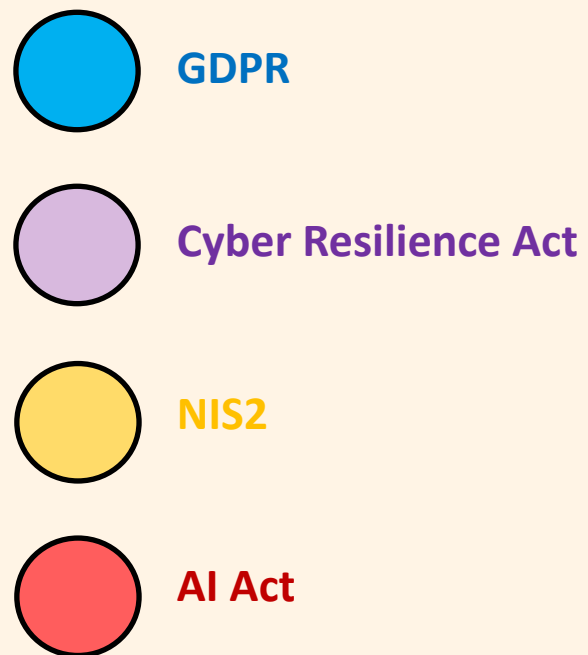
Andet

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

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



HISTORIK FOR REGULERING AF DIGITALE TEKNOLOGIER

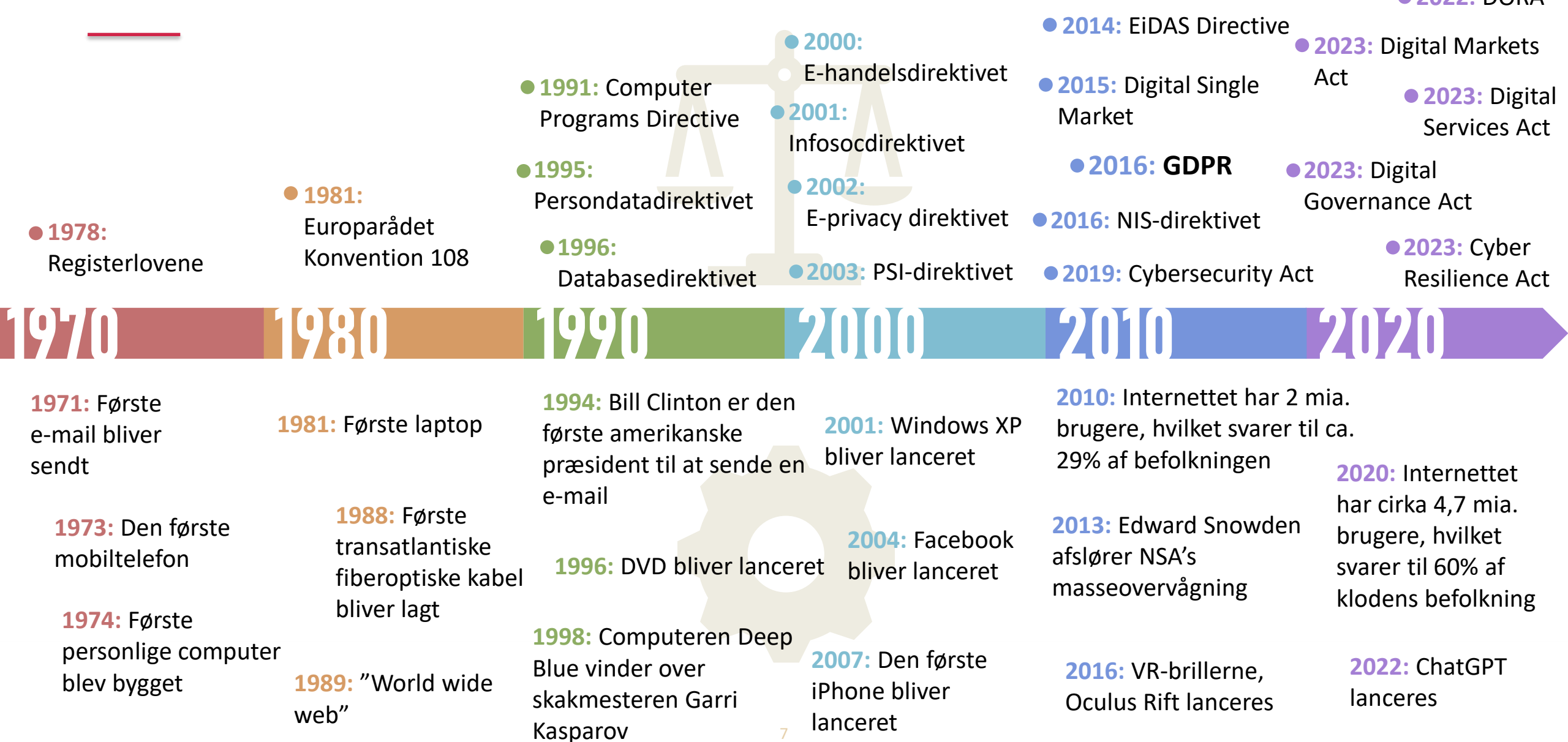
Grundlæggende udfordring: Teknologien udvikler sig hurtigere end juraen



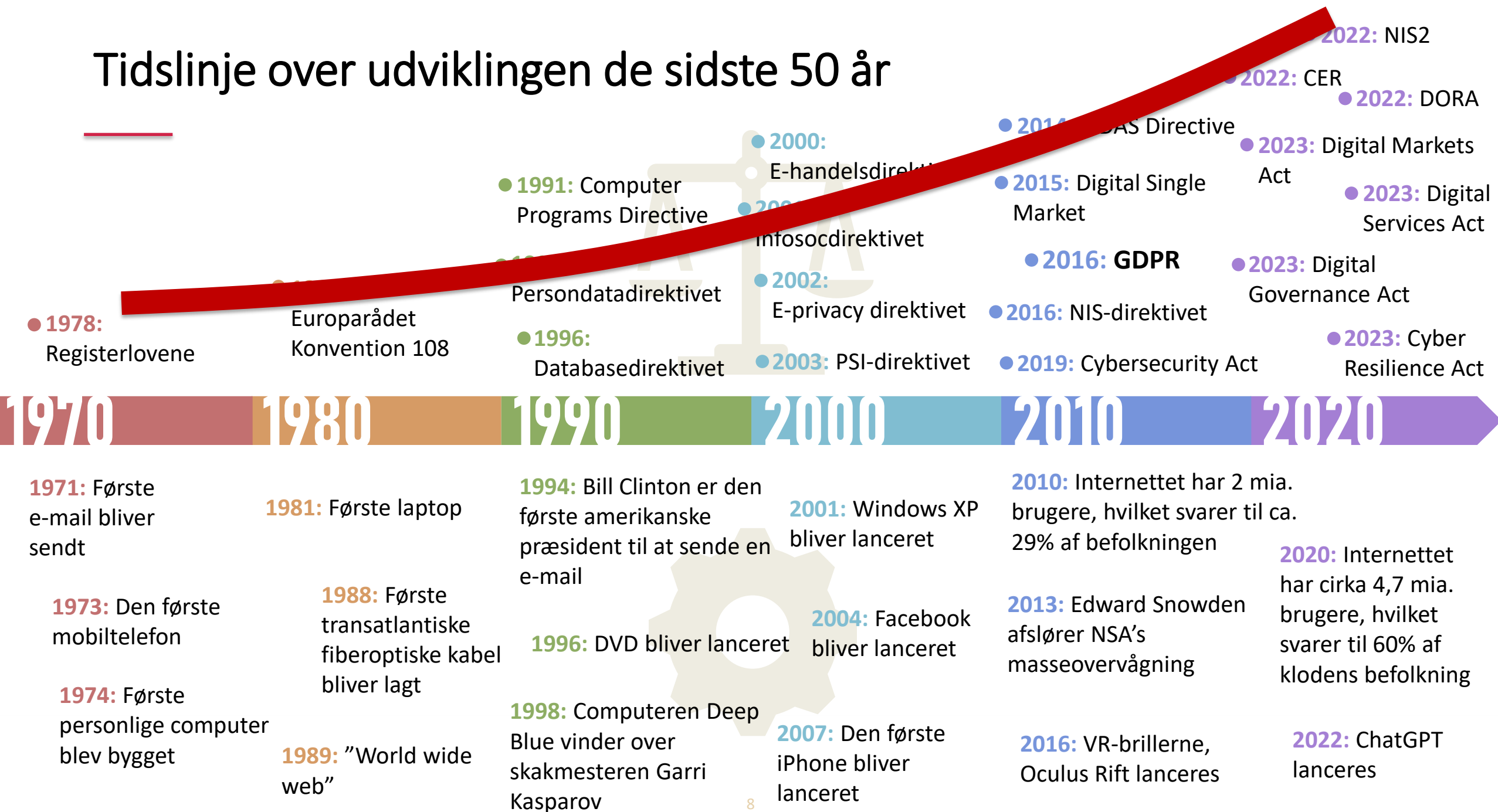
"Man ser i vore dage, at den tekniske udvikling skånselsløst sprænger de forudsætninger, som retsordenen har indrettet sig under, og tvinger juristerne til at foretage en omvurdering af hidtil uanfægtede retsprincipper, undertiden endog således, at man alvorligt må overveje at bygge systemet inden for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

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

Tidslinje over udviklingen de sidste 50 år

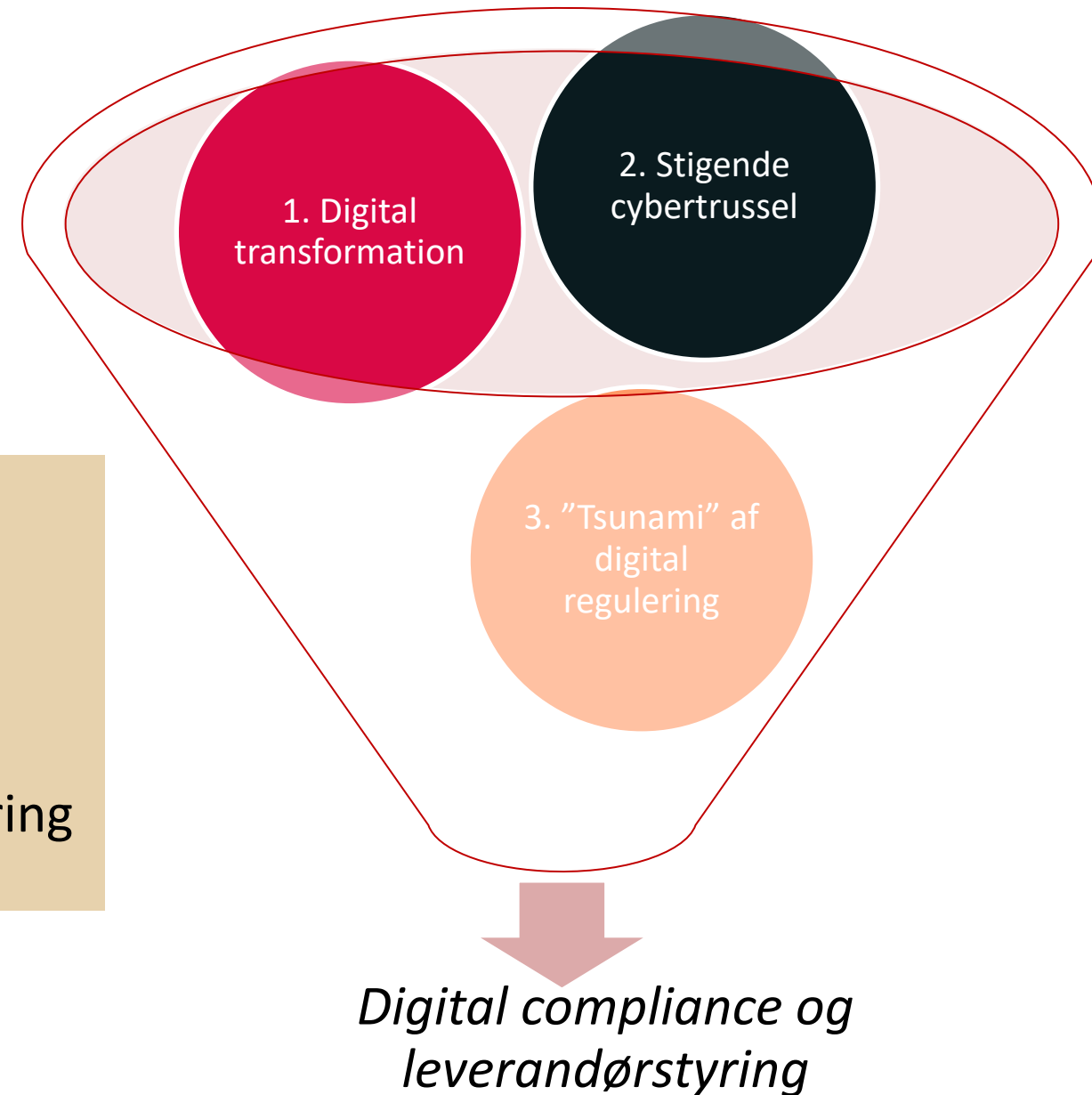


Tidslinje over udviklingen de sidste 50 år



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



DIGITAL DECADE

2030 DIGITAL DECADE



Digital
Principles
Digital
Compass

People at
the Centre
Solidarity
and Inclusion
Freedom
of Choice

Participation
Safety and
Security
Sustainability

Democracy

Artificial
Intelligence

Data
Governance

Data
Spaces

Online Platforms
(DSA/DMA)

Cybersecurity

Media Freedom
/ Pluralism

Rules

Digital
Twins

High-Performance
Computing

Digital
Wallet

Quantum

Microelectronics

Blockchain

5G

Cutting-edge
technologies
for people

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)**."

- 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**

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

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 Assessment

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

BEHOV FOR HÅNDTERING AF DEN
VOKSENDE MÆNGDE
CYBERRISICI

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
- + Common European Data Spaces

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

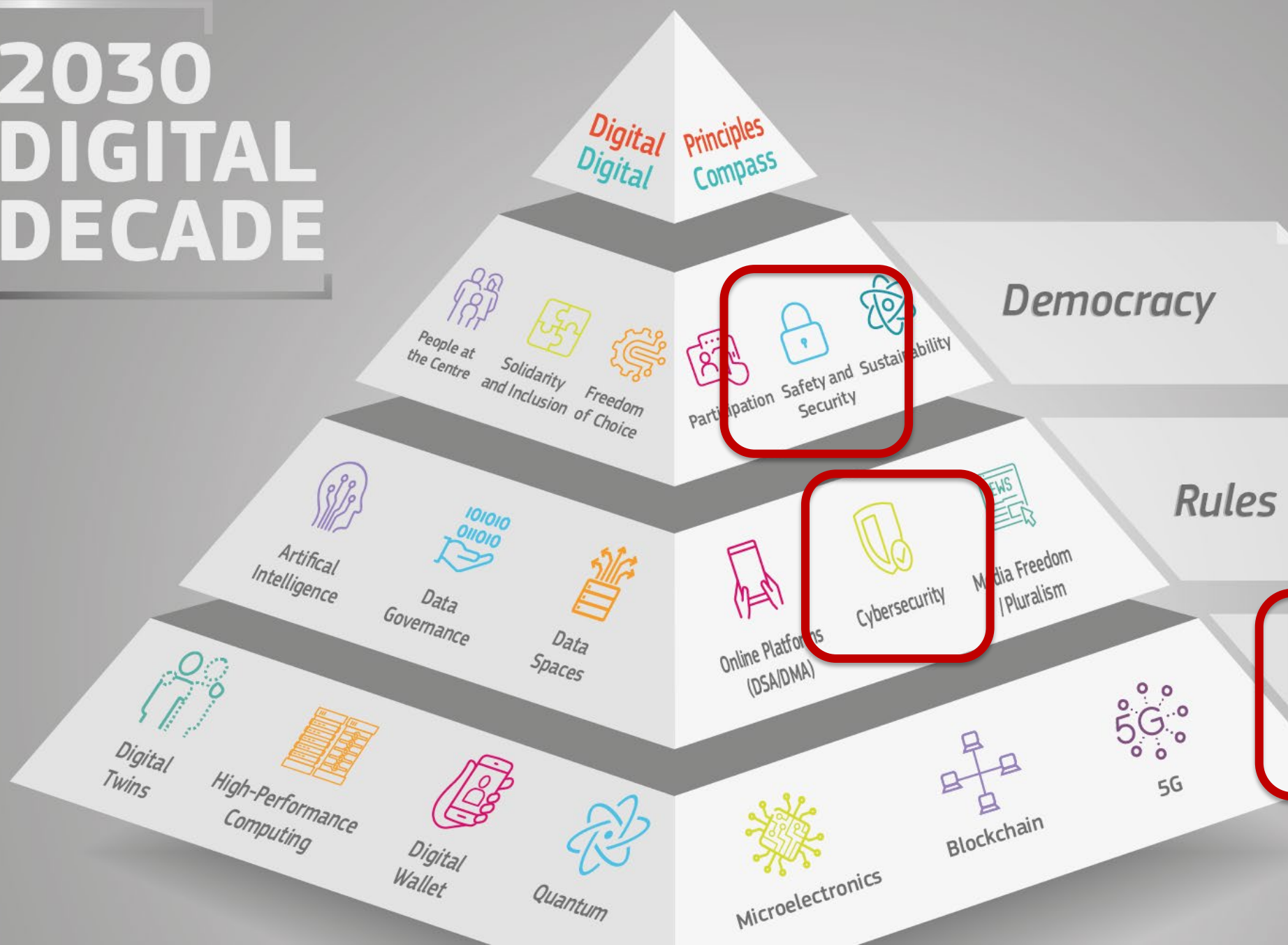
Teknologier og ansvar

- 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

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

CYBERSIKKERHEDSREGULERING

2030 DIGITAL DECADE



Democracy

Rules

*Cutting-edge
technologies
for people*

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

SPØRGSMÅL

Vi hører ofte begreberne "Cybersikkerhed", "Informationssikkerhed" og "IT-sikkerhed". Disse begreber er dog ikke helt det samme. Brug 2-3 min. med jeres sidemand på at drøfte forskellen på disse begreber.

GDPR

De registreredes
rettigheder

ISO 2700X

Forretningsmål

Persondatabeskyttelse

Cybersikkerhed

It-sikkerhed

Informationssikkerhed



Udvalgte regler fra EU med fokus på cybersikkerhed

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



NIS2



- **Formål:** At sikre et højt **fælles niveau af cybersikkerhed i hele EU** – særligt i kritiske sektorer
 - Styrket cybersikkerhed i kritisk infrastruktur
- **Baggrund:** Det tidligere direktiv (NIS1) var utilstrækkelig
 - Fragmenteret **implementering**
 - **Manglende effektivitet** på tværs af medlemslande.
- **Mål:**
 - Harmonisering: Ensretter krav og tilsyn på tværs af EU for at mindske kompleksitet og øge modstandsdygtighed.
- **Omfatter flere sektorer og aktører:**
 - Rammer en nærmere defineret række af aktører fra EU medlemsstaterne (næste slide)
- **Krav:**
 - Implementering af cybersikkerhedsforanstaltninger i organisationerne
 - Hændelsesrapportering
 - Ledelsesansvar og tilsyn (Næste slide)

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 hændeshåndtering og f.eks. Driftskontinuitet efter hændelser.

POLITIKKER, STRATEGIER & EVALUERING

Risikoanalyse, informationssikkerhed, samt effektiviteten af foranstaltninger

Cyber Resilience Act



- **Formål:** At sikre, at 'produkter med digitale elementer' er cybersikre
- **Baggrund**
 - Sikkerhedsniveau 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

Cyber Resilience Act

- **Cybersikkerheden i produkter med digitale elementer:**

- **Security by design** er hovedkonceptet

Article 1:

(a) rules for the making available on the market of products with digital elements to ensure the cybersecurity of such products;

(b) essential cybersecurity requirements for the **design, development** and **production** of products with digital elements, and obligations for economic operators in relation to those products with respect to cybersecurity;

- **Definition?**

For the purposes of this 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;

Eksempler: Robotstøvsuger

Opsummering på cybersikkerhed

Key takeaways ift. Cybersikkerhed:

- Integration af cybersikkerhed på virksomhedsniveau og i selve produkterne er essentiel ift. compliance
 - **Cybersikkerheden i enheder** omfattet af NIS2, skal sikre de kritiske sektorer og derved samfundssikkerheden.
 - **Cybersikkerheden i produkter med digitale elementer**, skal sikre at produkterne i EU har et tilstrækkeligt niveau af cybersikkerhed og derved mindske risici samt angrebsflader.
- Kræver at man indrager overvejelser om **teknisk**, **operationelt** og **organisatorisk** sikkerhed

DATAREGULERING

Det nye olie?

BRIEFING



Is data the new oil?

Competition issues in the digital economy

In this Briefing

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

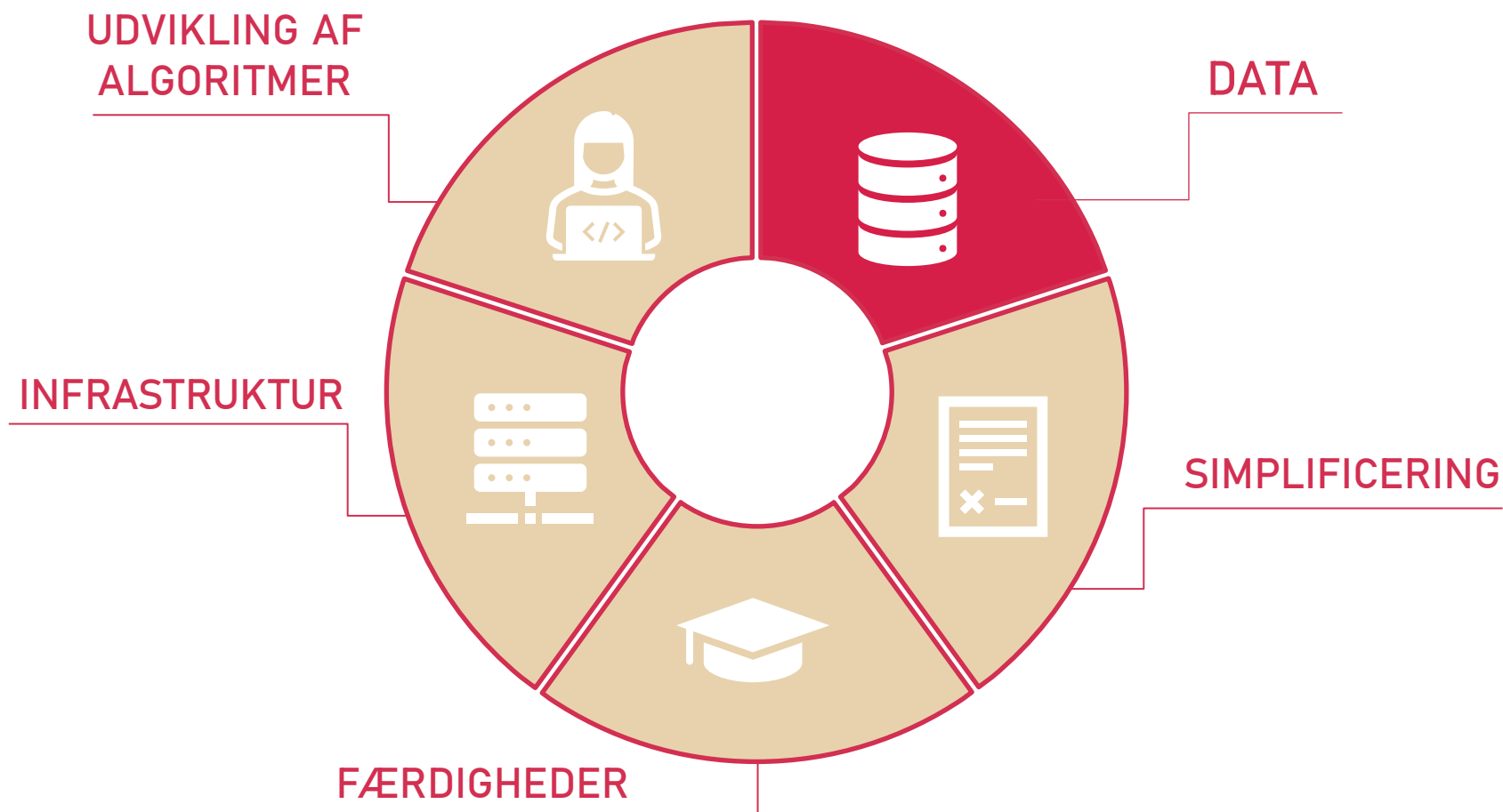
Datadeling vil i de kommende år blive fundamental for europæiske økonomi, hvor data vil bidrage med mindst **1 billion euro i 2030**. (European Commission, 2022, [European Data Market study 2021-2023](#), højvækst scenariet)

Ingen AI uden data(regulering)

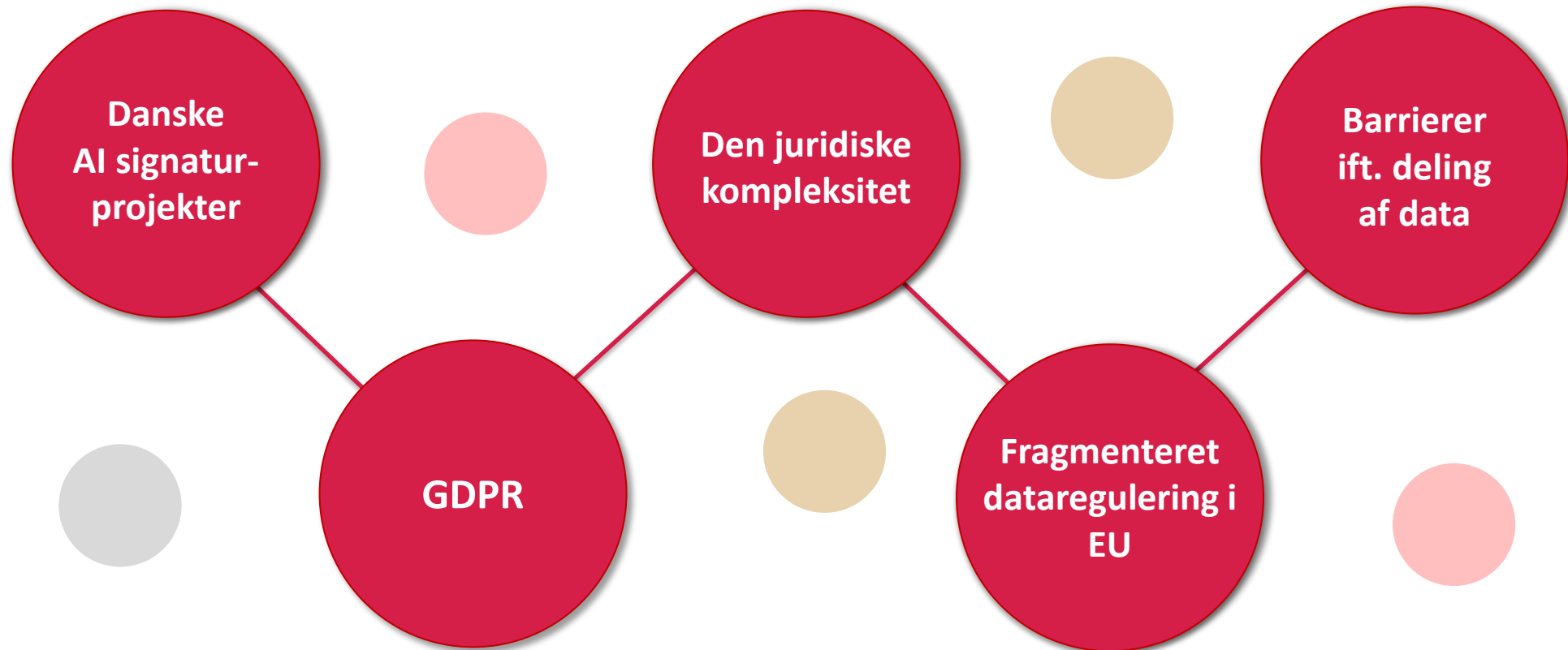
AI Act, præambelbetragtning 68

*”Med henblik på udvikling og vurdering af højrisiko-AI-systemer bør visse aktører, som for eksempel udbydere, bemyndigede organer og andre relevante enheder såsom europæiske digitale innovationsknudepunkter, afprøvnings- og forsøgsfaciliteter og forskere, **have adgang til og kunne anvende datasæt af høj kvalitet** inden for aktivitetssområderne for de aktører, som er relateret til denne forordning. **Fælles europæiske dataområder**, som Kommissionen har oprettet, **og lettelse af datadeling** mellem virksomheder og med myndigheder i samfundets interesse **vil være afgørende for at sikre pålidelig, ansvarlig og ikkeforskelsbehandlende adgang til data af høj kvalitet til træning, validering og afprøvning af AI-systemer...**”*

AI Continent Action Plan (maj 2025)



Udvalgte udfordringer



Danske AI-signaturprojekter

Erfaringer fra 40 danske projekter på tværs af kommune, region og stat (18 er fortsat i gang)

Erfaringsopsamling 2021:

“Data: En betydelig udfordring... omhandler manglende teknisk adgang til data i eksisterende systemer.

Jura: Den største oplevede udfordring vedrører usikkerhed om fortolkning af GDPR.”

Erfaringsopsamling 2022:

“Projekternes største udfordringer opleves i forbindelse med data, infrastruktur og jura i tråd med temperaturmålingens konklusioner.”

Erfaringsopsamling/evaluering 2024:

“De fleste kommuner og regioner oplever dataudfordringer, både i form af utilstrækkelige datamængder og lav datakvalitet...”

“Juridisk fortolkning og manglende klarhed om hjemler har været den næsthyppigste udfordring blandt AI-signaturprojekterne...”

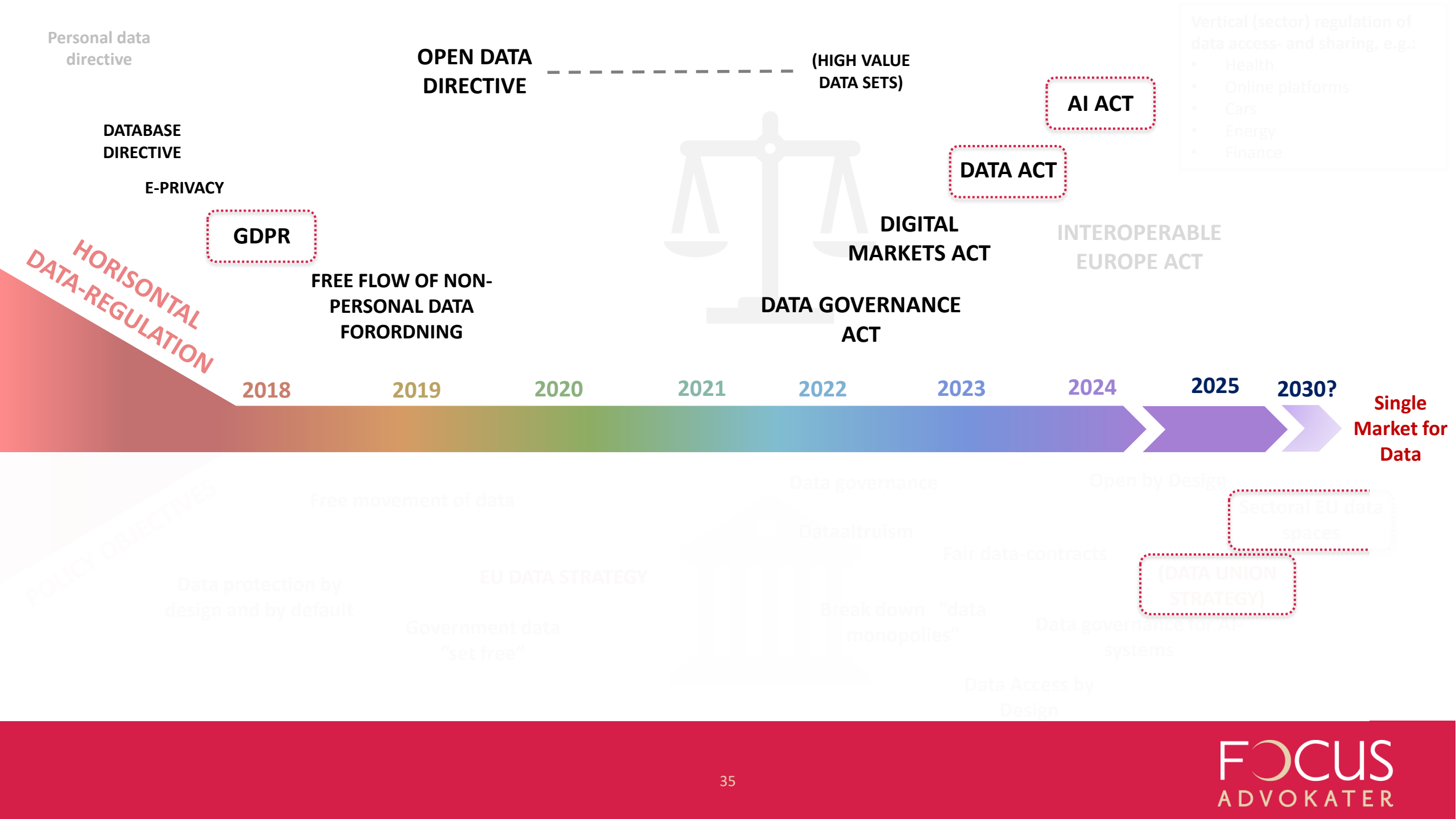
Den juridiske kompleksitet for data er høj i EU...

	USA	Kina	EU
Antal retssystemer	1 (+ stater)	1	27 + EU
Regler om databeskyttelse	Få og lempelige	Få og lempelige	Mange og strenge!
Regler om cybersikkerhed	(primært på sektorniveau, fx sundhed)	(primært begrænsninger ift. adgang fra/til udlandet)	(GDPR, ePrivacy, NIS2, CRA, sektorregler mv)
Øvrige lovgivningsmæssige begrænsninger			

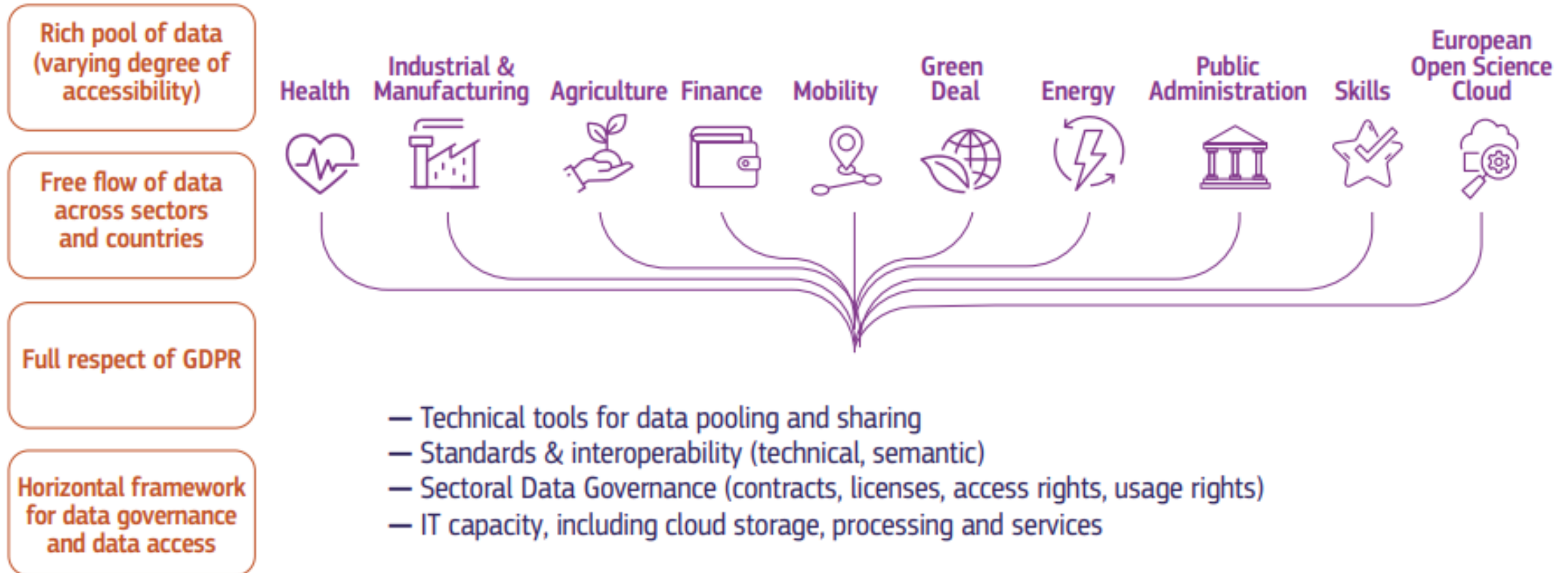
Hvilke udfordringer ser I relateret til øget udnyttelse af AI?

- GDPR?
 - Manglende adgang til data?
 - Data er ikke struktureret/af en egnet kvalitet?
 - AI-løsninger begrænses af hensyn til sikkerhed?
 - Andet?
-
- *Link til Slido:*
<https://wall.sli.do/event/kBf1XyndmMR4QGkod8jdXH?section=7cacfd46-095c-4ef6-9908-46d398b84184>





EU Data Spaces



AI-REGULERING

AI giver bekymringer...

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

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 offentlige sagsbehandling.

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

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



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

March 22, 2023

PDF created

May 5, 2023

Signatures

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

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.”*

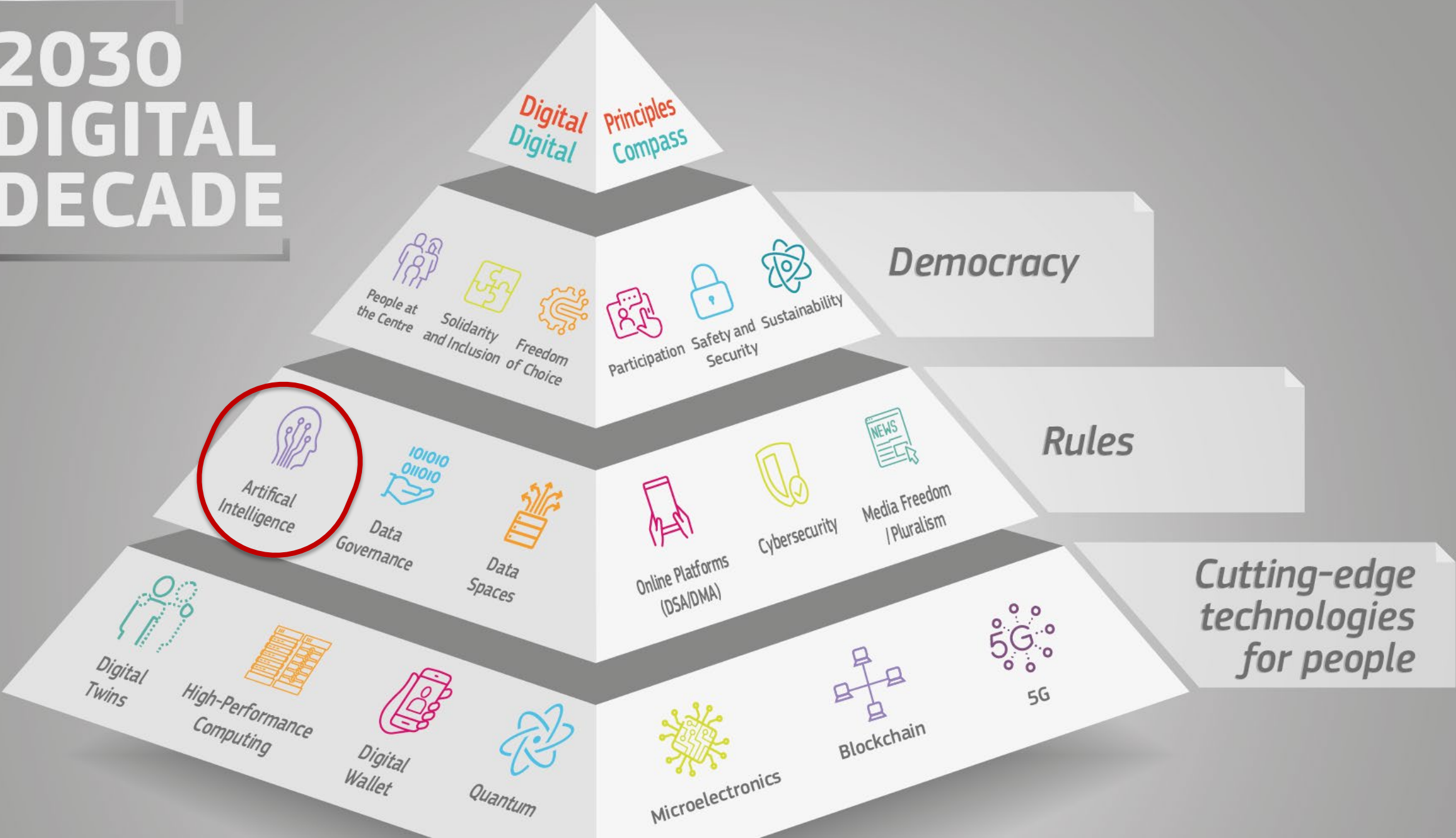
AI Act, art. 3(1)

International regulering AI

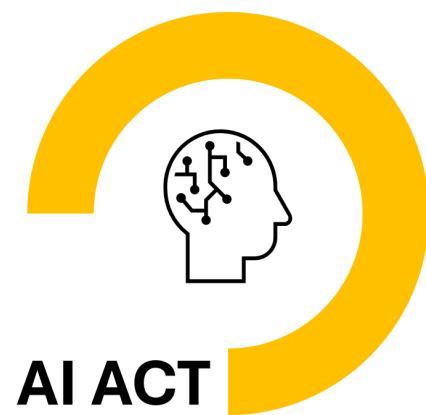
- **OECD:**
 - [AI Principles](#) (2019)
 - [Definition of AI](#) (November 2023 update)
- **Council of Europe:**
 - [Recommendation of the Committee of Ministers to member States on the human rights impacts of algorithmic systems](#) (2020)
- **Trade and Technology Council (TTC) (EU/US)**
 - [Roadmap](#) (2022) + [AI taxonomy](#) (2023-)
- **G7:**
 - ["International Draft Guiding Principles for Organisations Developing Advanced AI systems"](#) (October 2023)
 - [Statement on the Hiroshima Process](#) (October 2023)
- **Countries attending the AI Safety Summit:**
 - [The Bletchley Declaration](#) (November 2023)
- **UK:**
 - [A pro-innovation approach to AI regulation - GOV.UK \(www.gov.uk\)](#) (March 2023)
 - [Artificial Intelligence \(Regulation\) Bill \[HL\] - Parliamentary Bills - UK Parliament](#) (November 2023)
- **US:**
 - [Blueprint for an AI Bill of Rights](#) (October 2022)
 - [Executive Order to Strengthen Racial Equity and Support for Underserved Communities Across the Federal Government](#) (February 2023)
 - [White House "Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence"](#) (October 2023)

→ Efterhånden konsensus om: 1) *risici reglateret til AI*, 2) *generelle (softlaw) principper* og 3) *Terminologi*

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** ("udbydere") og **kunder** ("idriftsættere")
- **Håndhævelse** nationalt (Digitaliseringsstyrelsen, Datatilsynet mfl.) og på EU-plan ("European AI Board" og "AI Office")

Titel	Artikler
CHAPTER I: GENERAL PROVISIONS	Art. 1 - 4
CHAPTER II: PROHIBITED ARTIFICIAL INTELLIGENCE PRACTICES	Art. 5
CHAPTER III: HIGH-RISK AI SYSTEMS	Art. 6 - 49
CHAPTER IV: TRANSPARENCY OBLIGATIONS FOR PROVIDERS AND DEPLOYERS OF CERTAIN AI SYSTEMS	Art. 50
CHAPTER V: GENERAL PURPOSE AI MODELS	Art. 51 - 56
CHAPTER VI: MEASURES IN SUPPORT OF INNOVATION	Art. 57 - 63
CHAPTER VII: GOVERNANCE	Art. 64 - 70
CHAPTER VIII: EU DATABASE FOR HIGH-RISK AI SYSTEMS LISTED IN ANNEX III	Art. 71
CHAPTER IX: POST-MARKET MONITORING, INFORMATION SHARING, MARKET SURVEILLANCE	Art. 72 - 94
CHAPTER X: CODES OF CONDUCT AND GUIDELINES	Art. 95 - 96
CHAPTER X: DELEGATION OF POWER AND COMMITTEE PROCEDURE	Art. 97 - 98
CHAPTER XI: PENALTIES	Art. 99 - 101
CHAPTER XII: ENTRY INTO FORCE AND APPLICATION	Art. 102 - 113
ANNEX I-XIII	N/A



@AI-Regulation.Com - Inspired by the Commission's initial graphic

Overblik over forordningens forpligtelser

Forpligtelse	Artikler	Uddybning	Pligtssubjekter	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 oplyste 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 interagerer 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!
