

Kunstig intelligens / Cybersikkerhed / NIS2 -  
bestyrelsesrelevance i lyset af den stigende regulering  
af digitale teknologier.

Indlæg på foreningen af bestyrelsesadvokater's  
bestyrelsesdag den 12. maj 2023 af

Advokat Jesper Løffler Nielsen, Focus Advokater og  
Advokat Henrik Mansfeldt Witt, Aumento  
Advokatfirma

12. maj 2023

# Dagens agenda

---

1. Introduktion
2. Overblik over EU's regulering af cybersikkerhed, AI og andre digitale teknologier
3. Deep dive: Regulering af cybersikkerhed
4. Deep dive: Regulering af AI
5. Det ledelsesmæssige/kontraktmæssige perspektiv

# Jesper Løffler Nielsen

---



## Profil

- Certificeret IT-advokat og associeret partner hos Focus Advokater P/S
- Rådgiver om GDPR, IT-kontrakter, cybersikkerhed samt juridiske aspekter ved nye teknologier

### Forskning og undervisning

- Erhvervs-PhD i IT-ret (2013 – 2016)
- Ekstern lektor i IT-ret, Persondataret mv. (2010 -)
- En række UfR-artikler inden for IT-ret og databeskyttelse + enkelte bøger

### Andet

- Ekstern DPO
- IDA Databeskyttelse
- Netværksleder for Technology Denmark's netværk: "Innovation & Compliance"
- Blog om Tech & Jura på [www.version2.dk](http://www.version2.dk)
- Grundlægger af [www.techjura.dk](http://www.techjura.dk)

# Henrik Mansfeldt Witt



## Profil

- IT-advokat og partner hos Aumento Advokatfirma (H)
- Rådgiver om GDPR, IT-kontrakter og andre løbende kontrakstyper, cybersikkerhed samt juridiske aspekter ved nye teknologier, samt selskabsret og M&S.
- Bestyrelsesformand og bestyrelsesmedlem i en række selskaber, herunder Tech selskaber.
- Underviser på ITU og KU (SODA) i GDPR (på engelsk for ikke jurister) i et modul på et semester.
- Underviser på CBS i IT-kontrakter på HA IT (helt kursus)
- Afholder regelmæssigt kurset ”Kommercielle kontrakter for ikke-jurister hos Teknologisk institut.

# INTRODUKTION



# Hvorfor interessant for bestyrelser?

Side 6

- Bestyrelsen er overordnet ansvarlig for styring af virksomhedens risici.
- Den digitale udvikling går stærkt – både teknisk og juridisk.
- Den digitale udvikling skaber potentielt nye (og måske ukendte) risici.
- Risikoen for cybercrime er kendt – men ofte ikke håndteret på det strategiske niveau.
- Med NIS2 reguleringen øges kravene til mange virksomheder særligt på bestyrelsesniveau.
- Brug af kunstig intelligens er pt. en i hovedsagen umoden teknologi.
- Brug af kunstig intelligens er et strategisk valg på samme måde som at automatisere produktionen, som bestyrelsen bør være involveret i.

# Hvorfor interessant for bestyrelser?

Side 7

- Indsigt, forståelse og viden er en forudsætning for at kunne sætte emnerne på bestyrelsesdagsordenen.
- Nødvendigt for at kunne på, at de nødvendige kompetencer er tilstede i bestyrelseslokalet.
- Alle typer af virksomheder vil blive påvirket – enten direkte eller indirekte.
- Trusselsbilledet i forhold til cybercrime har ikke været mere alvorligt.
- Man kan enten blive ramt direkte eller indirekte.
- Med mindre man er en ren dansk virksomhed, så fokus fra hele EU/verden.

# OVERBLIK OVER EU'S "DIGITAL DECADE"

---



# EU Digitale Decade (2019 - )

---

## Cybersikkerhed

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

## Data (adgang og deling)

- S: Data Strategy**
- F: Free Flow of Data
- D: Open Data
- F: Data Governance Act
- F: Data Act
- F: European Health Data Space
- ? : Vehicle Data

## 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: Machinery (revision)
- F: AI Act
- F: EUid framework
- D: Product Liability Directive (revision)
- 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



**GDPR:**

*“Taking into account the nature, scope, context and purposes of processing as well as the **risks of varying likelihood and severity** for the rights and freedoms of natural persons, the controller shall implement **appropriate technical and organisational** measures to ensure and to be able to **demonstrate** that processing is performed in accordance with this Regulation...”*

(+ specific requirements!)

**NIS2 (cybersecurity):**

*“...take **appropriate and proportionate technical, operational and organisational measures** to manage the risks posed to the security of network and information systems...”*

(+ specific requirements!)

**AI Act (still being negotiated):**

*“A **risk management system shall be established, implemented, documented and maintained** in relation to high-risk AI systems...”*

(+ specific requirements!)



# DEEP DIVE: REGULERING AF CYBERSIKKERHED

---

# Direkte og indirekte regulering

---

## Generelle krav

- **Databeskyttelsesreglerne**, inkl. en række sikkerhedsrelaterede krav

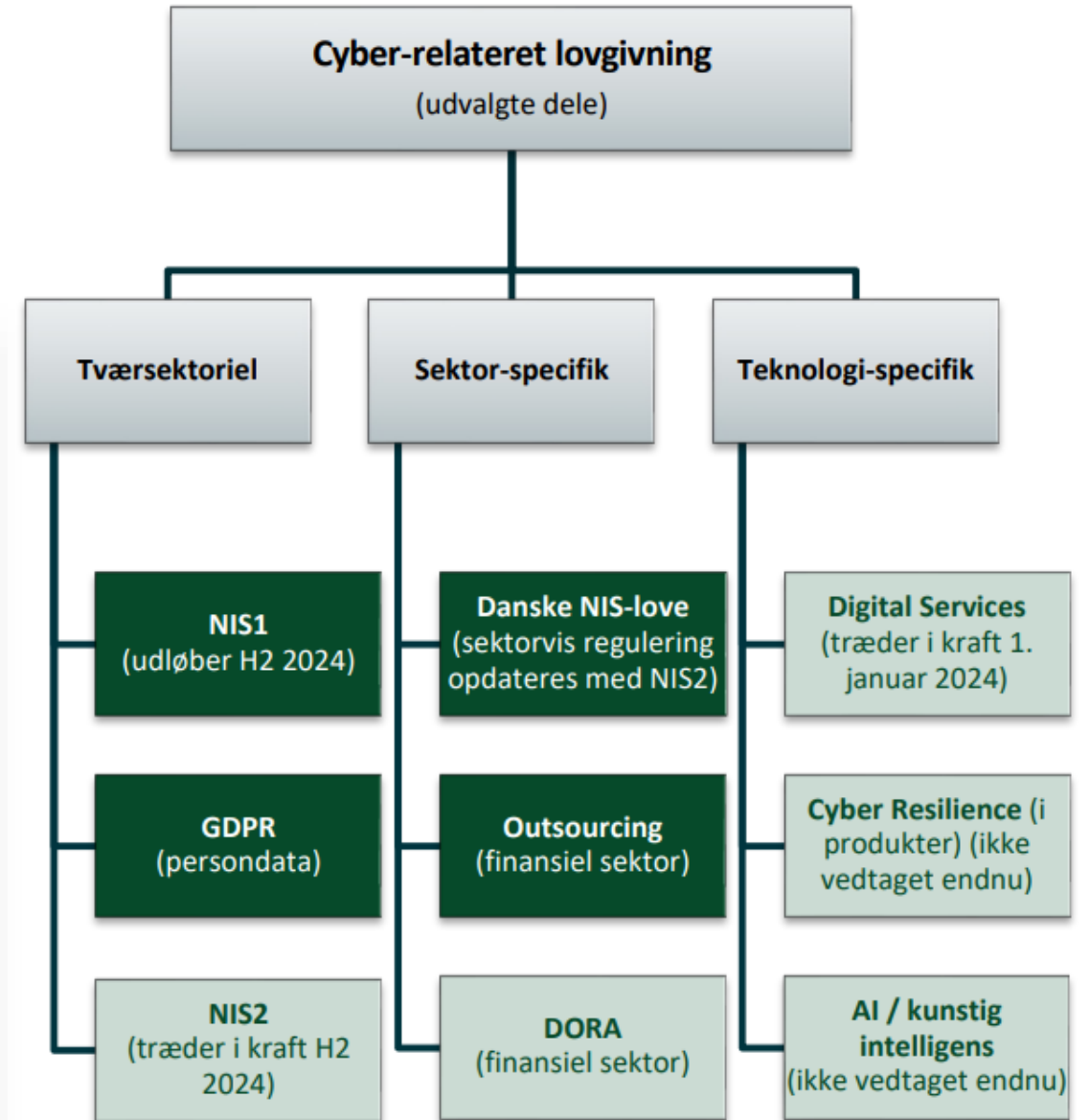
## Sektorspecifikke krav

- Krav om/anbefaling ift. **offentlige myndigheders** efterlevelse af informationssikkerhedsstandard 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 ledelsesansvar**, 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

# Regulering



# TIMELINE FOR CYBERSECURITY LEGISLATURE IN THE EU



## Cybersecurity Act

- Strengthening the role of The EU in regards to cybersecurity (ENISA, certifications, etc.)

April 2019  
(Adopted)

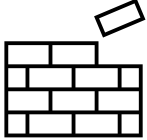
December 2022  
(Adopted)



## NIS2

- Requirements for **cyber security** in several sectors

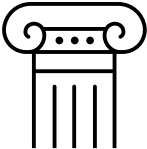
## Critical Entities Resilience (CER)



- Ensuring the **physical resilience** of critical entitites

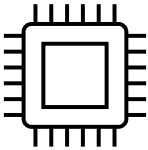
## DORA

- Requirements for **cyber security** in the financial sector



## Cybersecurity Regulation & Information Security Regulation

- Requirements for cyber security and information security in the EU institutions (Negotiations in progress)



## Cyber Resilience Act (CRA)

- Requirements for products/services with digital elements – "**Security by Design**" (Negotiations in progress)

# Om NIS2

## Primære formål

- ❖ Harmonisering
- ❖ Udvidelse af omfattede sektorer
- ❖ Flere krav
- ❖ Mere håndhævelse og bøder på GDPR-niveau
- ❖ I øvrigt begrebsmæssig ændring til "cybersikkerhed" (= bredere end blot systemer)

## Tidshorisont

- ❖ Den endelige NIS2 tekst blev offentliggjort i Den Europæiske Unions Tidende den 27. december 2022
- ❖ Medlemsstaterne har til den 17. oktober 2024 til at implementere NIS2 i national lovgivning, hvorefter den vil finde anvendelse

# NIS2

1	Artikel 1 – 2:	Genstand og anvendelsesområde
2	Artikel 3 – 4:	Omfattede sektorer og EU-retsakter
3	Artikel 5 – 6:	Definitioner og harmonisering
4	Artikel 7 – 13:	Krav til nationale cybersikkerhedsstrategier og lovgivningsmæssige rammer
5	Artikel 14 – 19:	Uddybning af samarbejdet på tværs af EU og internationalt
6	Artikel 20 – 25:	Krav til cyberrisici, foranstaltninger og underretning ved hændelser
7	Artikel 26 – 28:	Jurisdiktion og registrering af omfattede enheder
8	Artikel 29 – 30:	Krav til informationsdeling på tværs af medlemsstaterne
9	Artikel 31 – 37:	Tilsyn og håndhævelse
10	Artikel 38 – 46:	Gennemførelse og afsluttende bestemmelser



# Materielle krav

Artikel  
20

Krav til ledelsesforankring, governance og awareness

Artikel 21

Krav til risikostyring af cyberrisici (inklusive konkrete minimumskrav )

Artikel 23

Krav til underretning af tilsynsmyndighed ved sikkerhedshændelser x 3  
(24 timer → 72 timer → En måned)









# Risikostyring af cyberrisici

De i stk. 1 omhandlede foranstaltninger baseres på [...] og **mindst** omfatter følgende:

- a) *politikker for risikoanalyse og informationssystemsikkerhed*
- b) *håndtering af hændelser*
- c) *driftskontinuitet, såsom backup-styring og reetablering efter en katastrofe, og krisestyring*
- d) *forsyningskædesikkerhed, herunder sikkerhedsrelaterede aspekter vedrørende forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere*
- e) *sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder*
- f) *politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici*
- g) *grundlæggende cyberhygiejnepraksisser og cybersikkerhedsuddannelse*
- h) *politikker og procedurer vedrørende brug af kryptografi og, hvor det er relevant, kryptering*
- i) *personalesikkerhed, adgangskontrolpolitikker og forvaltning af aktiver*
- j) *brug af løsninger med multifaktorautentificering eller kontinuerlig autentificering, sikret tale-, video- og tekstkommunikation og sikrede nødkommunikationssystemer internt i enheden, hvor det er relevant.*

# Omfattede enheder og sektorer

- Organisation som sådan bliver omfattet, men visse krav gælder kun for systemerne, der faktisk bruges til at levere den kritiske ydelse
- **Konkret vurdering:**
  - → **Artikel 3 og 4 + Annex I og II** samt henvisninger til anden EU-regulering, sektorrapporter, mv.
  - → **Bagatelgrænse** ("mikro"/"små")
  - → Yderligere kompleksitet for **internationale organisationer**
  - → Afgrænsning ift. **hvilke konkrete systemer**, der er omfattet
  - → Kommende **sektorspecifik regulering** (bekendtgørelser, vejledninger mv)
- ObS! Mange vil også blive "**indirekte**" **berørt** som leverandører til omfattede organisationer (sikring af værdikæden)

Essentielle enheder	Vigtige enheder
 <b>Energi</b> – forsyning, distribution, transmission og salg af energi	 <b>Post- og kurerservice</b> – postvæsen og kurertjenester
 <b>Transport</b> – sø- og luftfart, jernbane- og vejtransport	 <b>Affaldshåndtering</b>
 <b>Bank og finans</b> – bankvæsen, finansielle markedsinfrastrukturer, handel og børser	 <b>Kemiske produkter</b> – fremstilling, produktion og distribution
 <b>Sundhed</b> – forskning, produktion, udbydere og fremstillere af medicinske udstyr	 <b>Fødevarer</b> – produktion, forarbejdning og distribution
 <b>Drikkevand og spildevand</b> – primærleverandører og -distributører	 <b>Fremstilling/produktion</b> – medicinsk udstyr, computere, elektronik, optisk udstyr, elektrisk udstyr, maskineri, køretøjer, transportudstyr, mv.
 <b>Digital infrastruktur</b> – internetudvekslingspunkter, DNS-udbydere, TLD-navneregistre, cloudcomputing	 <b>Udbydere af online markedspladser</b> – online markedspladser, søgemaskiner og SoMe
 <b>Offentlig administration</b>	 <b>Forskning</b> – kommercielt
 <b>Rummet</b> – infrastruktur til rumtjenester	

# Sanktioner

## Eksempler på tilsynenes sanktionsbeføjelser

- **Bøder** (op til 10.000.000 EUR eller 2% af den samlede globale omsætning)
- **”On-site”-inspektioner**, herunder stikprøvekontrol
- Regelmæssige og målrettede **sikkerhedsaudits** udført af et uafhængigt organ eller myndighed
- **Ad hoc-revisioner**, herunder navnlig ved væsentlige hændelser
- **Sikkerhedscanninger** pba. risikovurderinger
- Anmodning om informationer for at **vurdere de implementerede cybersikkerhedsforanstaltninger**, herunder politikker
- Anmodning om **adgang til data**, dokumenter, mv. for at udføre tilsynets opgaver
- Anmodninger om **beviser for implementering af cybersikkerhedspolitikker** pba. af sikkerhedsaudits
- **Midlertidig suspendering af certificering eller godkendelse** til levering af tjenester
- **NB! Midlertidigt forbyde enhver med ledelsesansvar på direktionniveau eller juridisk repræsentant at udøve ledelsesfunktioner** i den pågældende enhed

# DEEP DIVE: REGULERING AF AI

---

# Artificial Intelligence APIs Landscape - January 2023

VISION

- clarifai KAIROS Base64.ai Matroid AWS FaceX VISUA folio3 Cloudmersive. ayoniX Yandex Microsoft Azure ModerateContent MODIFACE [VISIONIFY]  
 PICPURIFY muse.ai Hugging Face imagga SmartClick Meta AI eyedea Baidu sightcorp HUAWEI alwaysAI PimEyes VALOSSA kakao developers DeepAffects  
 Q4Q api4ai chooch OpenAI WebPurify LUXAND SENTISIGHT.AI image labeling and recognition Width.ai Alibaba Cloud HIVE sightengine CloudSight™ ximilar IBM Watson Repustate. data in sight

SPEECH

- Speech-To-Text** DEEPGRAM AssemblyAI syml.ai Yandex SONIX Google Cloud HUAWEI HIVE Apptek  
 VOCI Neural Space Hugging Face Cloudmersive. Microsoft Azure kakao developers rev.ai  
 Speechly Meta AI VOCAPIA ONEAI AWS OpenAI Alibaba Cloud SPEECHMATICS IBM Watson
- Text-to-Speech** Hugging Face Speech. kakao developers Apptek HUAWEI Alibaba Cloud  
 VOICEGAIN IBM Watson Cloudmersive. acapela group AWS Google Cloud  
 ReadSpeaker Yandex Microsoft Azure Speechki RESEMBLE.AI

TRANSLATION

- Hugging Face Unbabel Alibaba Cloud IBM Watson modernMT Apptek TILDE 科大讯飞 IFLYTEK DeepL Rosetta.ai SYSTRAN beyond language AWS HIVE verbit Yandex LingvaNex LILT  
 Meta AI Google Cloud 川村インターナショナル Kawamura International kakao developers elhuyar Microsoft Azure Neural Space Lesan YarakuZen Translate.com pangeanic Globalese Tencent 腾讯

TEXT / NLP

- OpenAI Neural Space lettria Hugging Face text2data api TextRazor. Alibaba Cloud textgain CELM LANGUAGE TECHNOLOGY ONEAI IBM Watson Apptek Intellexer with the AI  
 connexun emvista Gavagai. allganize ParallelDots cortical.io twinw.rd Repustate. data in sight bytesview ALPH ALPHA TEKLIA meaning cloud KLANGOO. AWS [VISIONIFY]  
 MonkeyLearn clarifai Meta AI Cloudmersive. Google Cloud HIVE DeepAffects Microsoft Azure TISANE LABS dandelion Neticle MODERATION API

DOC PARSING

- General OCR** ScanDocFlow Microsoft Azure klippa Cloudmersive. ABBYY asprise  
 Base64.ai OCRSpace Google Cloud Alibaba Cloud ROSSUM  
 AWS NATIF AI clarifai HUAWEI Nanonets HIVE
- Resume** daXtra affinda. HireAbility  
 sovren hireEZ HrFlow.ai  
 textkernel Chill SuperParser
- Invoice/Receipt/ID** Syphr NATIF AI klippa mindee tabscanner AWS IDfy affinda. Google Cloud  
 ROSSUM Microsoft Azure FormX.ai Cloudmersive. Dataleon ScanDocFlow asprise  
 Nanonets HUAWEI Xtracta your data engine Base64.ai TAGGUN parsel ABBYY VERYFI

GENERATIVE AI

- inworld LT GitHub Copilot D-ID mem COMPOSE AI Ultimate. viable Typewise ada copysmith Hour One. Colossyan runway neuroflash {lyne} Movio PhotoRoom  
 WRITER Quickchat hume Facet CODACY stability.ai OpenAI Magnifi WOMBO.AI soul machines frase genei plask craftly.ai [PERSADO] S Rytr  
 Writersonic KAEDIM letterdrop cohere YEPIC.AI elai. mavenoid anyword Mitty AI21 labs Let's Enhance.io Rephrase.ai synthesia Mintlify Hypotenuse AI Linguix XOXKind

# STATUS på EU's arbejde med AI (ikke-udtømmende!)

- **April 2021:**
  - EU-Kommissionens udkast til forordning om AI (AI Act – uddybes senere)
  - EU-Kommissionens udkast til forordning om "Machinery"
  - Opdatering af koordineringsplanen mellem medlemslande
- **Juni 2022:**
  - udkast - Parlamentets foreløbige indstilling til AI ACT offentliggjort (meget omfattende ændringer)
- **December 2022:**
  - Rådets indstilling til AI Act offentliggjort (meget omfattende ændringer)
- **April 2023:**
  - Enighed mellem Parlamentet og Rådet om teksten til Machinery Regulation (afløser Maskin direktivet) og indeholder en regulering af embedded software eller related software inklusiv AI.

# Hvad betyder "AI" egentlig?

---

## AI Act (udkast fra april 2021)

"'artificial intelligence system' (AI system) means **software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with**

...

### Annex I

- (a) **Machine learning approaches**, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;
- (b) **Logic- and knowledge-based approaches**, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;
- (c) **Statistical approaches**, Bayesian estimation, search and optimization methods."



# Hvad betyder "AI" egentlig?

---

## Den sandsynlige kommende definition i forordningens artikel 3 (rådets indstilling side 71)

- artificial intelligence system' (AI system) means a system that is designed to operate *with elements of autonomy* and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of objectives using **machine learning and/or logic- and knowledge based approaches**, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, **influencing the environments with which the AI system interacts**;

# Hvad betyder "AI" egentlig?

---

## Fra den nye Machinery forordning:

*Provisions related to the third-party conformity assessment of software ensuring safety functions set out in this Regulation **should only apply to systems with a fully or partially self-evolving behaviour using machine learning approaches ensuring safety functions**. On the contrary, those provisions should not apply to software incapable of learning or evolving, and programmed only to execute certain automated functions of machinery or related products.*

## *Fra Rådets udtalelse om udkast til AI ACT: (side 52)*

*“The [Machinery Regulation] applies the same definition of AI system as this Regulation. With regard to high-risk AI systems related to products covered by Regulations 745/2017 and 746/2017 on medical devices, the applicability of the requirements of this Regulation should be without prejudice and take into account the risk management logic and benefit-risk assessment performed under the medical device framework. “*

# AI Act (udkast )

De fire niveauer	Hvilke løsninger?	Krav
Niveau 1 – Ingen (ekstra) krav	Alle, der ikke er nævnt i niveau 2-4	(Gældende regler, fx GDPR, krav til cybersikkerhed, produktsikkerhed mv)
Niveau 2 – Krav om gennemsigtighed (TITLE IV)	<b>Chatbots, emotion-detection, deep fakes</b> mv	Skal oplyse, at der er tale om AI
Niveau 3 – Skærpede krav til "høj risiko" (TITLE III + Annex II og III)	<b>AI indarbejdet i udstyr, som er underlagt anden EU-sikkerhedslovgivning</b> (køretøjer, jernbaner, maskiner, droner, radioudstyr/IoT, medicinsk udstyr mv)  <b>Øvrige konkrete "usecases" i Annex III</b> , herunder ifbm. kritisk infrastruktur, eksamensbedømmelse, jobansøgninger, kreditvurderinger, retshåndhævelse mv	En lang række krav,, herunder <i>Risk management system (test), Technical documentation, Data Governance, Transparency and provision of information to users, Accuracy, Robustness and Cybersecurity, Human oversight , Record keeping mv. Registrering af systemet i en EU database Overensstemmelsesvurdering og erklæring CE mærkninger med tilhørende dokumentation inklusiv brugervejledning</i>
Niveau 4 – Forbudt (TITLE II)	<b>Skadelig manipulation, udnyttelse af svagheder, social scoring "a la Kina" + visse former for real-time ansigtsgenkendelse</b> mv.	Forbudt – med mindre de enkelte lande vedtager ved lov i det omfang forordningen tillader det.

# AI ACT = klassisk produktregulering

---

- 1. Hovedforpligtelserne påhviler producenten af high risk AI systemer, men**
- 2. husk at hele markedovervågningsregulering gælder, så er man importør, distributør eller forhandler af high risk AI systemer, så husk at overholde de forpligtelser man bliver overholdt (ikke set før med rene software produkter)**
- 3. Så hvis man er ansvarlig for import, distribution eller anvendelse af et high risk AI system, så vær opmærksom på de udvidede forpligtelser hvis:**
  - Man sælger whitelabel versioner af High Risk AI systemer
  - Man har adgang til at ændre det tilsigtede formål med high risk AI systemer, der allerede er på markedet/i anvendelse.
  - Man laver betydelige ændringer til et high risk AI System,
- 4. CE mærkning af alle high risk AI systemer.**

# Standarder kommer til at spille en central rolle

---

- **AI Acts krav til "high risk"-løsninger kommer i praksis til at blive udfyldt/konkretiseret i tekniske standarder (bestilt af Kommissionen):**
  - *"To advance the technical harmonisation in the field of trustworthy artificial intelligence and prepare the necessary technical ground for the implementation of the future AI Act, once applicable, it is necessary to draft European standards or European standardisation deliverables in order to support the key technical areas covered by the proposed AI Act. These include the requirements for design and development of AI systems defined as high-risk in the proposed AI Act, the AI providers' quality management system, conformity assessment and auditing of AI systems."* (EU Kommissionen, december 2022)
- **Pt. arbejder CEN/CENLEC (inkl. Dansk Standard) med standarder til følgende emner:**
  - *Risk Management*
  - *Data Governance and Data Quality*
  - *Record Keeping*
  - *Transparency*
  - *Human Oversight*
  - *Accuracy and Robustness*
  - *Cybersecurity*
  - *Quality Management*
  - *Conformity Assessment*

Obs! GDPR gælder jo altså stadig..

**Datatilsynet: Ledige må ikke profileres med algoritmer bare fordi de samtykker**

Privacy

**Italy orders ChatGPT blocked citing data protection concerns**

MIT  
Technology  
Review

SIGN IN

SUBSCRIBE

ARTIFICIAL INTELLIGENCE

**A Cambridge Analytica-style scandal for AI is coming**

Can you imagine a car company putting a new vehicle on the market without built-in safety features?

# Opsamling: Regulering af AI nu og i fremtiden

---

## 1. Omfattet af gældende regler - men med nye udfordringer

- Særligt menneskerettigheder, GDPR, forvaltningsloven og regler om informationssikkerhed (NIS)

## 2. Gældende regler bliver justeret for tage højde for nye teknologier

- Færdselsloven → Særregler for selvkørende enheder
- GDPR art. 22 om profilering og automatiserede afgørelse
- Kommende revision af "Maskindirektivet" → Særlig fokus på AI-styrede robotter/enheder
- Kommende revision af produktansvarsregler

## 3. Der indføres helt nye regler specifikt for at regulere nye teknologier

- Fx AI Act

*Lovkrav*

Produktsikkerheds-  
krav

Tekniske standarder

*Andre "krav"/faldgruber*

AI Act (Udkast)

Forvaltningsregler

D-mærket

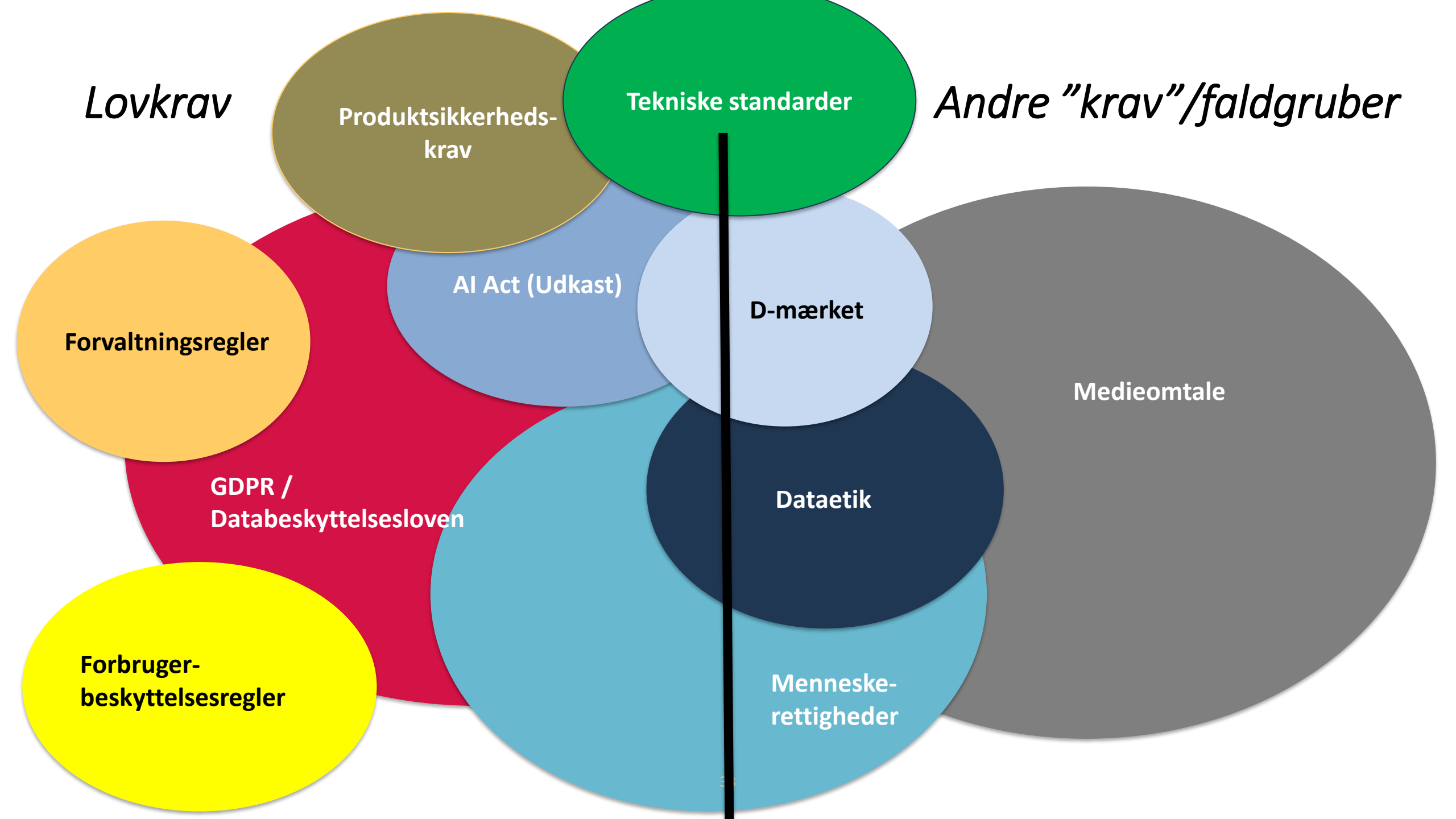
GDPR /  
Databeskyttelsesloven

Medieomtale

Dataetik

Forbruger-  
beskyttelsesregler

Menneske-  
rettigheder





# DET LEDELSESMÆSSIGE/KONTRAKTMÆSSIGE PERSPEKTIV

---

# Det handler ikke kun om jura

---

Cybersikkerhed kastes ud af bestyrelseslokalet og tørres af på it-afdelingen: “Det kan hurtigt blive meget langhåret”

**Ny analyse: Hackerangreb vælter ind over danske virksomheder**

Danmarkidag

Torsdag 8. september 2022 kl. 07:00

Debat | Alt for mange virksomheder kan ikke dæmme op for cyberangreb – Danmark har brug for flere specialister

---

## Hovedvurdering

- Truslen fra cyberspionage mod den danske sundhedssektor er **MEGET HØJ**. Fremmede stater har blandt andet interesse i at stjæle forskningsdata og intellektuel ejendom fra sektoren.
- Truslen fra cyberkriminalitet er **MEGET HØJ**. Der er muligt, at cyberkriminelle angreb kan forstyrre patientbehandlingen.

Truslen fra cyberaktivisme som DDoS-angreb stiger

---

# Det handler ikke kun om jura

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 offentlige 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.**

# Ledelsesforankring af cybersikkerhed



Link til [Bestyrelsesforeningens vejledning om cybersikkerhed for bestyrelser og direktion, vers. 4.0](#)

# ANBEFALINGER OG TJEKLISTE

*Til styrkelse af strategiske  
cyberkompetencer i danske bestyrelser*

## 1. Risikovurdering

- værdier og trusler

### Det anbefales, at

- bestyrelsen mindst to gange om året modtager og forholder sig til en opdateret risikovurdering på cyberområdet baseret på virksomhedens vigtigste værdier, it-infrastruktur, forretningsmodel, primære sårbarheder, sandsynlige trusler, mulige tab ved angreb samt mulige konkurrencemæssige vurderinger.

## 3. Politikker, processer og beredskab

- delegering og operationalisering

### Det anbefales, at

- bestyrelsen fører kontrol med, at cybersikkerhedsstrategien er operationaliseret i politikker, processer og forretningsgange.
- bestyrelsen fører kontrol med, at virksomheden har implementeret passende cyberhygiejne, herunder en relevant backup, der løbende er testet,
- bestyrelsen fører kontrol med, at virksomheden har testede beredskabs- og kommunikations-planer i tilfælde af alt fra hackerangreb til strømnedbrud.

## 5. Kultur

- mennesker og træning

### Det anbefales, at

- medlemmer af bestyrelse og direktion regelmæssigt følger specifikke kurser for at

## 2. Risikoappetit

- risikoafvejning og risikovillighed

### Det anbefales, at

- bestyrelsen så ofte som relevant og mindst én gang om året fastsætter virksomhedens cybersikkerhedsstrategi, herunder risikoappetit, baseret på en afvejning af virksomhedens generelle forretningsstrategi, forretningsmål, it-infrastruktur, generelle risikoappetit, sikkerhedsbudget og investeringsvilje m.v.

## 4. Rapportering

- kontrol og tilsyn

### Det anbefales, at

- bestyrelsen implementerer cybersikkerhed som en fast del af sit årshjul og, på linje med øvrige væsentlige risici,
- bestyrelsen har cybersikkerhed på agendaen på hvert møde, og modtager relevant rapportering forud for mødet med bl.a. aktuelt trusselsbillede, sikkerhedshændelser, resultater af sikkerhedstest, awareness aktiviteter og revisionsgennemgange, samt evt. forslag til supplerende tiltag.

## 6. Governance

- kompetencer og organisering

### Det anbefales, at

- bestyrelsen forholder sig til, om den har tilstrækkelige kompetencer og erfaring med

# Ledelsesansvar

Fra Bestyrelsesforeningens vejledning, s. 57-58

## Ansvar for cybersikkerhed

- Ledelsens ansvar for cybersikkerhed er baseret på et **civilretligt ansvar**
  - Fx selskabslovens § 115, nr. 2 om *"fornødne procedurer for risikostyring og interne kontroller"*.
- **Ansvarsnorm**
  - Culpa
  - "Forsvarlig adfærd"
- **"Business Judgment Rule"**
  - Forretningsmæssigt skøn
  - Forudsætter forsvarligt beslutningsgrundlag
  - Domstole generelt tilbageholdende med at tilsidesætte skøn

**Bemærk!** Overholdelse af minimumskrav i lovgivning **ikke** underlagt skøn (se næste slide)

# Ledelsesansvar

Fra Bestyrelsesforeningens vejledning, s. 57-58

## Eksempler

- Ikke forretningsmæssigt skøn
  - *Om* der skal udarbejdes cybersikkerhedsstrategi
  - *Om* der skal udarbejdes risikovurderinger
  - *Om* der skal fastsættes risikoappetit indenfor cybersikkerhed
  - *Om* ledelsen skal godkende sikkerhedsforanstaltninger
  - *Om* foranstaltningerne skal opfylde minimumskravene i den relevante lov
  - *Om* ledelsen løbende skal føre tilsyn med strategiens gennemførelse
  
- Forretningsmæssigt skøn
  - *Hvordan* strategien skal udarbejdes
  - *Hvordan* og *hvor* omfattende risikovurderinger skal være
  - Virksomhedens *konkrete* risikoappetit
  - *Hvordan* risikostyringsarbejdet skal tilrettelægges
  - *Hvilke* kontroller der skal måles på

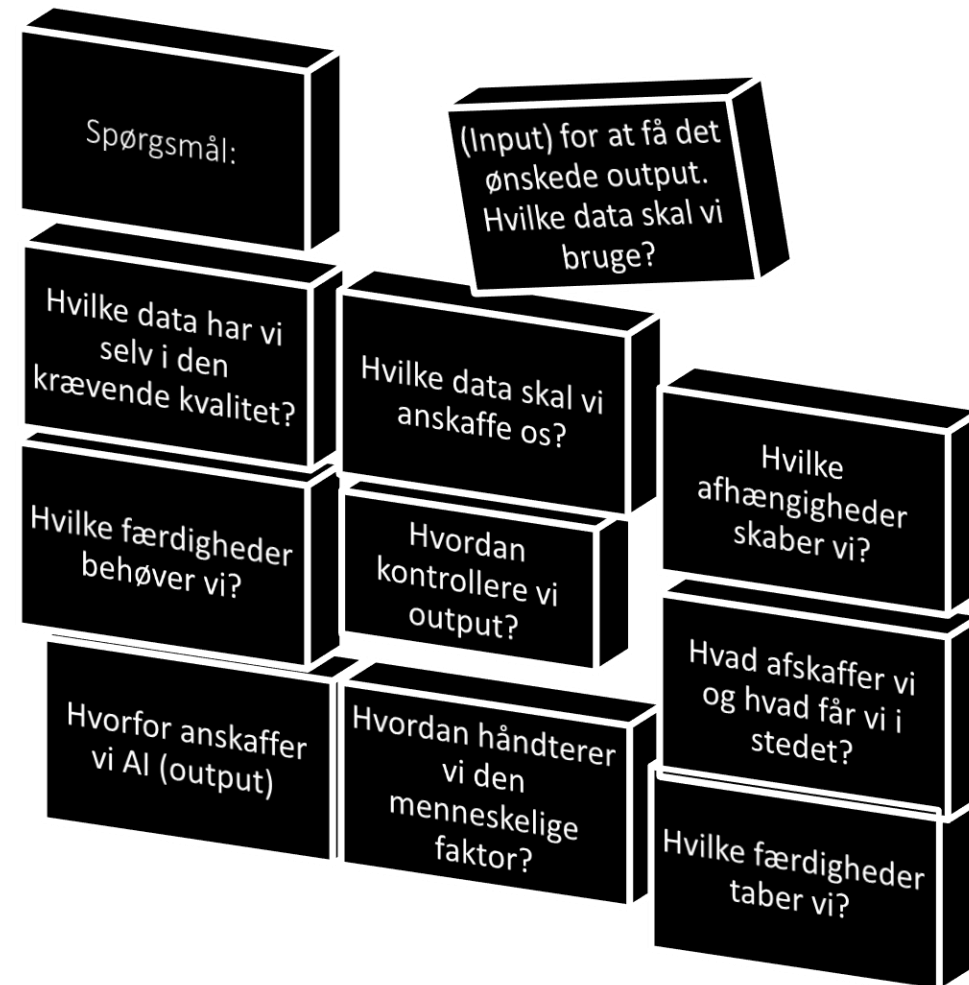
# Konkret eksempel: NIS2

- Ledelsens forpligtelser og ansvar **udtrykkeligt reguleret** (artikel 20)
  - *”ledelsesorganer **godkender** de foranstaltninger til styring af cybersikkerhedsrisici”*
  - *”**fører tilsyn** med [foranstaltninger til styring af cybersikkerhedsrisici] og kan **gøres ansvarlige**”*
  - *”ledelsesorganer er **forpligtet til at følge kurser**, således at de opnår tilstrækkelige kundskaber og færdigheder til at kunne identificere risici og **vurdere metoderne til styring af cybersikkerhedsrisici og deres indvirkning på de tjenester, der leveres af enheden.**”*
- **Sanktioner** ved overtrædelse
  - Bøder på op til € 10 millioner eller 2% af årlig global omsætning
  - + Mulighed for at myndighed kan udstede midlertidigt forbud for enhver med ledelsesansvar på direktionsniveau eller juridisk repræsentant at udøve ledelsesfunktioner i den pågældende enhed



# AI kræver også ledelsesforankring

- Hvis den planlagte brug af AI er af væsentlig betydning for virksomheden bør bestyrelsen få følgende spørgsmål besvaret af organisationen inden implementering, så man har et tilstrækkeligt besluthningsgrundlag for at vurdere de risici, der er forbundet med anskaffelsen og brug af AI.
- Hertil kommer, at man skal vurdere lovligheden/den kommende lovlighed af brugen af AI.



# Det kontraktmæssige perspektiv

**Nogle** af de hovedudfordringer, der skal håndteres i kontrakten:

- Pas på **leverandørens standardkontrakt** eller standard terms. De vil typisk stille dig dårligt som kunde.
- Få styr på, hvad det **præcis er, man køber**. (Software, en service eller.....)
- Få styr på, hvad det er, man får **rettigheder** til (typisk brugsrettigheder, men er det nok?)
  - Obs, husk rettigheder til træningsdata! (i bred og snæver forstand)
- **Garantier** fra leverandøren omkring performance (herunder bias) samt overholdelse af lovkrav (hvilke, løbende/ved indgåelse og hvor).
- Husk eventuelt **ansvar, hvis du er forhandler, distributør/importør af AI**, da dette ansvar kommer til at følge produktansvarsreglerne jf. Lov om produkter og markedsovervågning eller.....
- Ansvar herunder, produktansvar, ansvar for lovovertrædelse/rettighedskrænkelser i bred forstand → **Ansvarsbegrænsninger/fraskrivelser/friholdelse!**

# Det kontraktmæssige perspektiv (fortsat)

- **Håndhævelse/beføjelser** overfor leverandøren. Ophævelse er måske ikke relevant her.
  - Der skal tænkes i alternativer - da mangler kan resultere i nye typer af tab, herunder tab af goodwill.
  - Overvej derfor alternative misligholdelsesbeføjelser: f.eks. - ret først – afgør senere princip – kompensation – beredskab -
- Adgang til **løbende uddannelse/efteruddannelse af ens brugere**.
- Adgang til **indsigt/dokumentation/support/transparens**, herunder det der kræves efter AI ACT
- **Prisstruktur** og adgang til prisjusteringer (måske forbrugsafhængig prismodel)
- **Opsigelsesmuligheder** fra begge parter.
- Reel mulighed for at **skifte leverandøren** (teknisk og forretningsmæssigt)
  - Obs! Også nye regler på vej her, jf. Data Act
- **Lovvalg og værneting** har måske aldrig været vigtige – herunder brug af fast track løsninger.

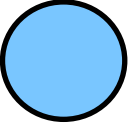
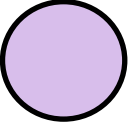
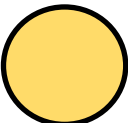
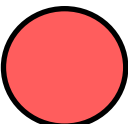
# Det kontraktmæssige perspektiv fra ChatGPT.....

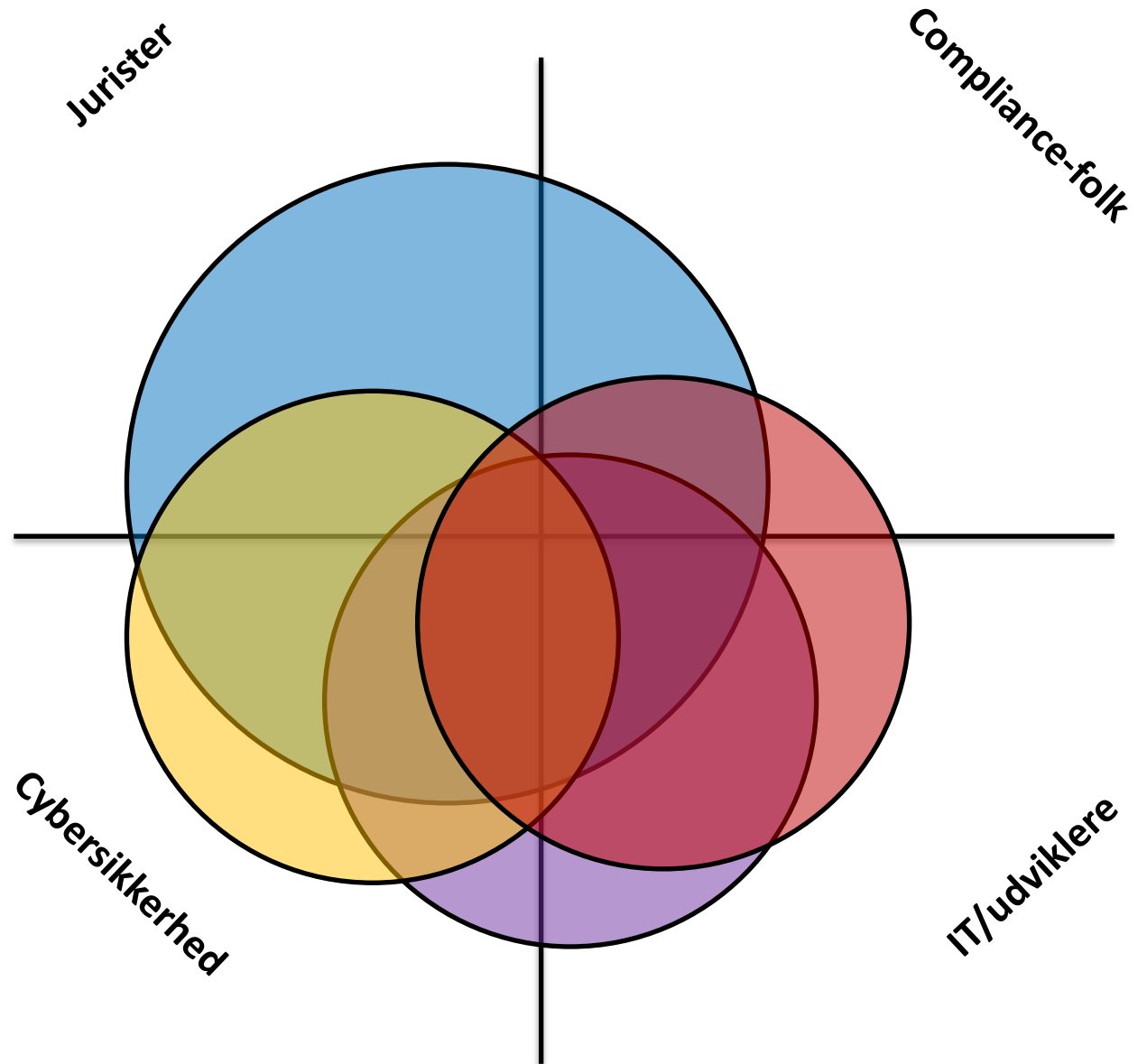
*”Indkøb af AI indebærer visse kontraktmæssige udfordringer, herunder:*

- 1. Dataejerskab: For at træne AI-modeller er store mængder data ofte nødvendige. Derfor er det vigtigt at fastlægge, hvem der ejer dataene, og hvem der har ret til at bruge dem efter købet af AI. Dette kan blive en udfordring, hvis dataene, der bruges i AI-modellen, er fortrolige eller følsomme.*
- 2. Ansvarsfordeling: Hvis AI-modellen fører til fejl eller skade, er det vigtigt at fastlægge, hvem der har ansvaret. Der kan også være spørgsmål omkring, hvem der skal betale for eventuelle skader eller tab, der opstår som følge af AI's handlinger.*
- 3. Intellektuelle ejendomsrettigheder: AI-modeller er ofte beskyttet af intellektuelle ejendomsrettigheder såsom patenter, ophavsret og varemærker. Det er vigtigt at klarlægge, hvem der ejer disse rettigheder, og om køberen har ret til at bruge AI-modellen på en bestemt måde.*
- 4. Adfærdsregler: AI-modeller kan have en stor påvirkning på samfundet og mennesker. Derfor er det vigtigt at klarlægge, om AI-modellen overholder bestemte adfærdsregler, etiske retningslinjer og lovgivning.*
- 5. Leveringstid: Implementering af AI-modeller kan tage tid og kræve tilpasninger og test. Det er vigtigt at klargøre, hvad der skal leveres, og hvornår det skal leveres.*

***Det er vigtigt at have en klar og omfattende kontrakt for at undgå potentielle udfordringer i forbindelse med indkøb af AI.”***

# Digital regulering og behovet for forskellige kompetencer

-  **GDPR**
-  **Cyber Resilience Act**
-  **NIS2**
-  **AI Act**



SPØRGSMÅL?

---

