

Stigende fokus på "-by design" lovkrav

Syddansk Universitet, Odense,

28. November 2025

Om mig

- **Jakub Skórczynski**, Ph.d.-studerende, SDU Esbjerg
- **Forskningsområde:** Brugen af data og dataregulering i energisektoren
- **Interesseområder:** Regulering af digitale teknologier, A.I., dataregulering og cybersikkerhed.
- **Arbejdserfaring:**
 - Focus Advokater P/S, Odense
 - Trainee: 2022 - 2023
 - Jurist med speciale i digital regulering: 2023 - 2024
- **Undervisningserfaring**
 - Instruktor
 - International Private Law and International Trade Law (2021 – 2023) samt Folkeret (2021 – 2022)
 - Ekstern lektor:
 - Cybersikkerhed og Privacy, SDU, 2024
 - Master i IT, SDU, 2024
 - AI502: Etik og privathed, SDU, 2024
 - IT- og databeskyttelsesret for ingeniører, SDU 2024 -
 - Teknologi og Jura - Esbjerg og Odense, SDU, 2025 -
 - Business Law, SDU, Sønderborg, 2025



Agenda

1. Udvikling af ”Privacy by design”

- Tankegangen om ”-By design” og udvikling af privatlivsfremmende tankegang

2. ”Data protection by design and by default” og den generelle tendens om ”-by design”

- Lovkravet i GDPR
- Andre eksempler på ”-by design”

3. ”Data protection by design and by default” i praksis

- Hvordan arbejdes der med begrebet i praktisk henseende, samt et eksempel på tankegangen.

4. Samarbejde mellem forskellige faggrupper

1. Udvikling af ”Privacy by design”

Oprindelse af ”-by design”

- Det er svært at opstille en specifik ”startdate” for udviklingen af ”-by design” tankegang:

While the emergence of privacy by design as a concept can be traced back to the sixties where it was used in the building and architecture sectors to emphasise the growing importance of residential privacy, it only gained traction in the software engineering community some twenty years later to counterweight the rampant development of surveillance technologies, especially in the United States.

Data Protection by Design 101. Dissecting, applying and supporting Article 25(1) GDPR, Pierre Dewitte, s. 20

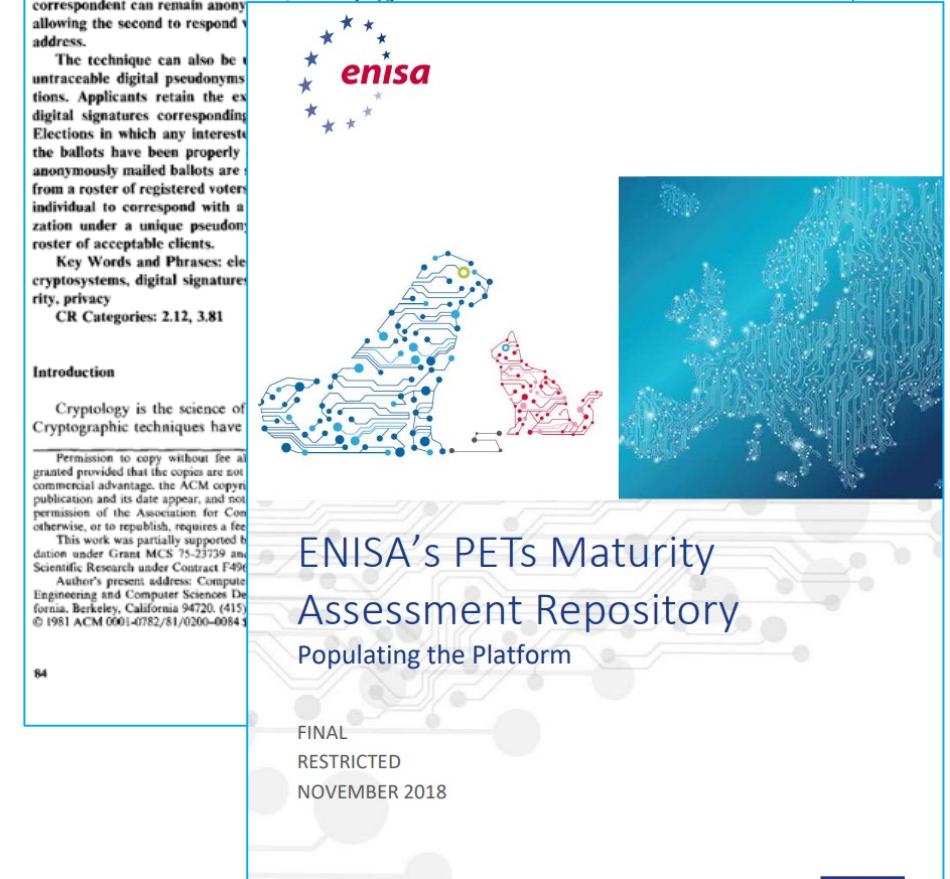
- Udgangspunkt: *Man ønsker at løse problematikker i designstadiet.*
- I 1980’erne begynder mange softwareingeniører at indse privatlivsmæssige udfordringer med de nye teknologier
- Men teknologien viser sig også at være en potentiel løsning...

PET's

- ”Privacy enhancing technologies” (PETs)
- En disciplin der har været under markant udvikling siden 1980’erne
 - Har sin oprindelse i anonym kommunikation og anonyme transaktioner
 - Det oprindelige fokus knyttede sig til risici for systemejerne
 - Dette fokus ændrede sig til at omfatte risici slutbrugerne og det var det næste skridt i retningen mod PET's
- I væsentlig omfang kryptografi, anonymiseringsteknikker og andre privatlivsfremmende tiltag

of message content for thousands of years [3]. Recently, some new solutions to the “key distribution problem” (the problem of providing each communicant with a secret key) have been suggested [2, 4], under the name of public key cryptography. Another cryptographic problem, “the traffic analysis problem” (the problem of keeping confidential who converses with whom, and when they converse), will become increasingly important with the growth of electronic mail. This paper presents a solution to the traffic analysis problem that is based on public key cryptography. Baran has solved the traffic analysis problem for networks [1], but requires each participant to trust a common authority. In contrast, systems based on the solution advanced here can be compromised only by subversion or conspiracy of all of a set of authorities. Ideally, each participant is an authority.

The following two sections introduce the notation and assumptions. Then the basic concepts are introduced for some special cases involving a series of one or more authorities. The final section covers general purpose mail networks.



ENISA's PETs Maturity Assessment Repository Populating the Platform

FINAL
RESTRICTED
NOVEMBER 2018

enisa

Introduction

Cryptography is the science of Cryptographic techniques have

Permission to copy without fee is granted provided that the copies are not for commercial advantage, the ACM copy publication and its date appear, and no permission of the Association for Computing Machinery is required. This work was partially funded by the National Science Foundation under Grant MCS-75-23739 and by the Defense Advanced Research Projects Agency under Contract F49620-85-C-0001. Author's present address: Computer Engineering and Computer Sciences Department, University of California, Berkeley, California 94720. (415) 642-5575. © 1981 ACM 0001-0782/81/0200-0004\$01.00

64

Privacy by design udvikler sig som et koncept

- I løbet af 90'erne populariseres tankegangen '**Privacy by design**' , og det begynder at blive anvendt i juridiske sammenhænge...
- I 1998 bliver **begrebet 'Privacy by Design'** udtænkt af Canadieren Peter-Hope Tindall, der anvendte begrebet i konteksten af: "*the process of architecting privacy protection into a system*"
- Begrebet levede en relativt stille tilværelse i nogle år, men det blev **i stigende grad anvendt i juridiske sammenhænge** i løbet af 00'erne
- Der skete et stort gennembrud i 2009, da Ann Cavoukian, som var daværende 'Information and Privacy Commissioner of Ontario' populariserede begrebet.
 - **Seven Foundational Principles**



SEVEN FOUNDATIONAL PRINCIPLES

The Privacy by Design framework is based on seven foundational principles:

1. **Proactive not Reactive; Preventative not Remedial**
Anticipate, identify and prevent privacy invasive events before they occur.
2. **Privacy as the Default Setting**
Build in the maximum degree of privacy into the default settings for any system or business practice. Doing so will keep a user's privacy intact, even if they choose to do nothing.
3. **Privacy Embedded into Design**
Embed privacy settings into the design and architecture of information technology systems and business practices instead of implementing them after the fact as an add-on.
4. **Full Functionality – Positive-Sum, not Zero-Sum**
Accommodate all legitimate interests and objectives in a positive-sum manner to create a balance between privacy and security because it is possible to have both.



Privacy by Design – Seven foundational principles af Ann Cavoukian

1. Proactive not Reactive; Preventative not Remedial

- Anticipate, identify and prevent privacy invasive events before they occur.

2. Privacy as the Default Setting

- Build in the maximum degree of privacy into the default settings for any system or business practice. Doing so will keep a user's privacy intact, even if they choose to do nothing.

3. Privacy Embedded into Design

- Embed privacy settings into the design and architecture of information technology systems and business practices instead of implementing them after the fact as an add-on.

4. Full Functionality — Positive-Sum, not Zero-Sum

- Accommodate all legitimate interests and objectives in a positive-sum manner to create a balance between privacy and security because it is possible to have both

5. End-to-End Security — Full Lifecycle Protection

- Embed strong security measures to the complete lifecycle of data to ensure secure management of the information from beginning to end.

6. Visibility and Transparency — Keep it Open

- Assure stakeholders that privacy standards are open, transparent and subject to independent verification.

7. Respect for User Privacy — Keep it User-Centric

- Protect the interests of users by offering strong privacy defaults, appropriate notice, and empowering user-friendly options.

Spørgsmål til jer

Praktisk eksempel: SDU skal udvikle et nyt system, der skal erstatte "ItsLearning". I bliver i den forbindelse udpeget til at hjælpe med en opgave.

Med udgangspunkt i " *Seven foundational principles* " skal i give bud på tiltag der kan være relevante at inddrage. Nævn venligst eksempler på praktiske løsninger der kan være relevante. F.eks. med de erfaringer i har ved at anvende *ItsLearning*.

Vi gennemgår emnet i fællesskab

Privacy by design

(...) Privacy by design is neither just a list of principles nor can it be reduced to the implementation of specific technologies. In fact, it is a process involving various technological and organizational components, which implement privacy and data protection principles by properly and timely deploying technical and organization measures that include also PETS.

Data Protection Engineering: From Theory to Practice, ENISA, Januar 2022, s. 6

- *Privacy by Design* og ”Seven foundational principles” af Ann Cavoukian er samtidigt ikke retligt bindende, men er blot reningslinjer
 - De får dog en væsentlig betydning i de efterfølgende år...

2. ”Data protection by design and by default”
og den generelle tendens om ”-by design”

Data Protection by Design – Et lovkrav i EU

Privacy by Design (PbD)

- Rødder tilbage til midt-90'erne, herunder en række principper udviklet af direktøren for det canadiske datatilsyn (Ann Cavoukian)
- Frivilligt: Handler om et mindset
- Ikke fast defineret indhold

Data Protection by Design (DPbDD)

- Gældende fra 25. maj 2018 i hele EU (+ UK efter Brexit)
- Lovkrav i EU, jf. GDPR artikel 25
- = Overholdelse af GDPR's krav ifbm. design af digitale løsninger, og det skal kunne dokumenteres

”-By design” som en generel tendens

”The sleeping giant” of GDPR

» *I en stadig mere digital verden har overholdelse af kravene til databeskyttelse gennem design og databeskyttelse gennem standardindstillinger en vigtig rolle med hensyn til at fremme privatlivets fred og databeskyttelse i samfundet.«*

EDPB, Retningslinjer 4/2019 om artikel 25 Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger
(v. 2 oktober 2020)

Teksten i GDPR

Artikel 25

Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger

1. Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, som behandlingen indebærer, gennemfører den dataansvarlige både på tidspunktet for fastlæggelse af midlerne til behandling og på tidspunktet for selve behandlingen passende tekniske og organisatoriske foranstaltninger, såsom pseudonymisering, som er designet med henblik på effektiv implementering af databeskyttelsesprincipper, såsom dataminimering, og med henblik på integrering af de fornødne garantier i behandlingen for at opfylde kravene i denne forordning og beskytte de registreredes rettigheder.
2. Den dataansvarlige gennemfører passende tekniske og organisatoriske foranstaltninger med henblik på gennem standardindstillinger at sikre, at kun personoplysninger, der er nødvendige til hvert specifikt formål med behandlingen, behandles. Denne forpligtelse gælder den mængde personoplysninger, der indsamles, og omfanget af deres behandling samt deres opbevaringsperiode og tilgængelighed. Sådanne foranstaltninger skal navnlig gennem standardindstillinger sikre, at personoplysninger ikke uden den pågældende fysiske persons indgriben stilles til rådighed for et ubegrænset antal fysiske personer.
3. En godkendt certificeringsmekanisme i medfør af artikel 42 kan blive brugt som et element til at påvise overholdelse af kravene i nærværende artikels stk. 1 og 2.

Teksten i GDPR

Artikel 25

Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger

1. Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, som behandlingen indebærer, gennemfører den dataansvarlige både på tidspunktet for fastlæggelse af midlerne til behandling og på tidspunktet for selve behandlingen passende tekniske og organisatoriske foranstaltninger, såsom pseudonymisering, som er designet med henblik på effektiv implementering af databeskyttelsesprincipper, såsom dataminimering, og med henblik på integrering af de fornødne garantier i behandlingen for at opfylde kravene i denne forordning og beskytte de registreredes rettigheder.
2. Den dataansvarlige gennemfører passende tekniske og organisatoriske foranstaltninger med henblik på gennem standardindstillinger at sikre, at kun personoplysninger, der er nødvendige til hvert specifikt formål med behandlingen, behandles. Denne forpligtelse gælder den mængde personoplysninger, der indsamles, og omfanget af deres behandling samt deres opbevaringsperiode og tilgængelighed. Sådanne foranstaltninger skal navnlig gennem standardindstillinger sikre, at personoplysninger ikke uden den pågældende fysiske persons indgriben stilles til rådighed for et ubegrænset antal fysiske personer.
3. En godkendt certificeringsmekanisme i medfør af artikel 42 kan blive brugt som et element til at påvise overholdelse af kravene i nærværende artikels stk. 1 og 2.

DPbDD skal kunne dokumenteres

Artikel 5

Principper for behandling af personoplysninger

1. Personoplysninger skal:
 - a) behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede (»**lovlighed, rimelighed og gennemsigtighed**«)
 - b) indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål; viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, skal ikke anses for at være uforenelig med de oprindelige formål (»**formålsbegrænsning**«)
 - c) være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles (»**dataminimering**«)
 - d) være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges (»**rigtighed**«)
 - e) opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles; personoplysninger kan opbevares i længere tidsrum, hvis personoplysningerne alene behandles til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, under forudsætning af, at der implementeres passende tekniske og organisatoriske foranstaltninger, som denne forordning kræver for at sikre den registreredes rettigheder og frihedsrettigheder (»**opbevaringsbegrænsning**«)
 - f) behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger (»**integritet og fortrolighed**«).

2. Den dataansvarlige er ansvarlig for og skal kunne påvise, at stk. 1 overholdes (»ansvarlighed**«).**

DPbDD skal kunne dokumenteres

Artikel 5

Principper for behandling af personoplysninger

1. Personoplysninger skal:
 - a) behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede (»**lovlighed, rimelighed og gennemsigtighed**«)

b) indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål; viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 80 stk. 1 skal ikke anses for at være uforenelig mod de oprindelige formål (»**formålschæmmen**«)

Artikel 24

Den dataansvarliges ansvar

1. Under hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder **gennemfører den dataansvarlige passende tekniske og organisatoriske foranstaltninger** for at sikre og for at være i stand til at påvise, at behandling er i overensstemmelse med denne forordning. Disse foranstaltninger skal om nødvendigt revideres og ajourføres.

(...)

- f) behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger (»**integritet og fortrolighed**«).

- 2. Den dataansvarlige er ansvarlig for og skal kunne påvise, at stk. 1 overholdes (»ansvarlighed«).**

GDPR artikel 25 – Dissekeret

- ”*passende tekniske og organisatoriske foranstaltninger*” + ”*designet med henblik på effektiv implementering af databeskyttelsesprincipper*” → **Digitale løsninger skal tænke GDPR’s krav ind fra starten**
- ”*behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor*” → **Baseret på en risikovurdering**
- ”*Under hensyntagen til det aktuelle tekniske niveau*” + ”*implementeringsomkostningerne*” → **Valg af de rigtige løsninger ud fra en samlet vurdering af tilgængelige teknologier og heraf følgende omkostninger**
- + ansvarlighedsprincippet, jf. art. 5(2) og 24 → **Overvejelser og valgte løsninger skal dokumenteres**

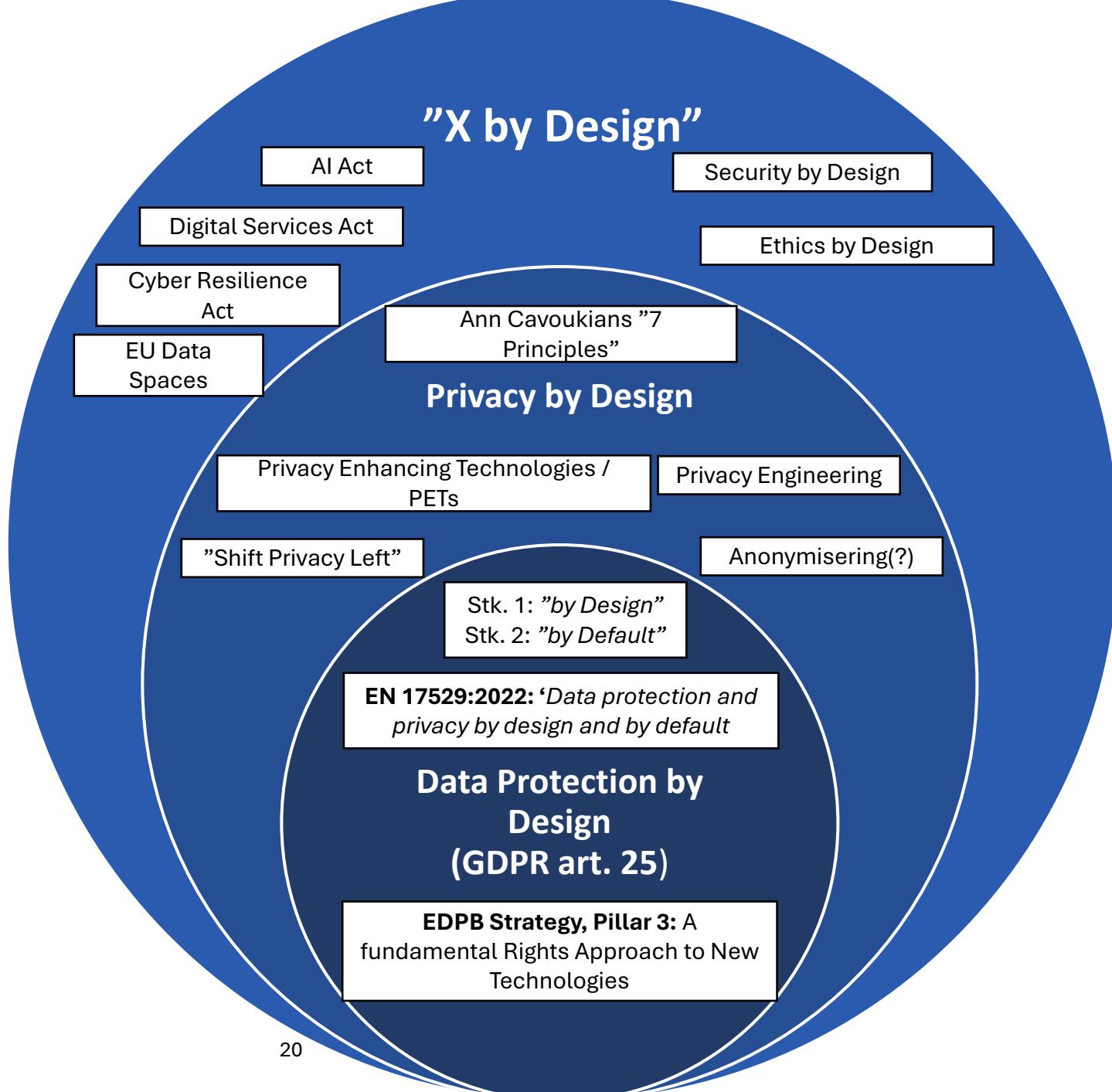
Stigende tendens til lovkrav, som forudsætter at compliance tænkes ind i udviklingsfasen

Eksempler på lovkrav

- GDPR art. 25 → Data Protection by Design
- NIS2-direktivet, Cyber Resilience Act m.fl. → Security by Design
- Nye regler i årsregnskabsloven → Ethics by Design
- Nyere praksis fra Folketingets Ombudsmand → Forvaltningsret by Design
- AI Act → Trustworthy AI by Design

Man ser ”-by design” tankegang i flere regelsæt, og det illustreres bedst på næste slide.

Oversigten over "-by Design"



Spørgsmål til jer

Hvilke typer af ”-By design” krav kan være relevante for AI løsninger?

ENISA: DATA PROTECTION ENGINEERING – From Theory to Practice (January 2022)

Data Protection by Design

“Nowadays, it is regarded as a multifaceted concept: in legal documents on one hand, it is generally described in very broad terms as a general principle; by researchers and engineers on the other hand it is often equated with the use of specific Privacy Enhancing Technologies (PETS). However, privacy by design is neither just a list of principles nor can it be reduced to the implementation of specific technologies. **In fact, it is a process involving various technological and organizational components, which implement privacy and data protection principles by properly and timely deploying technical and organization measures that include also PETS.**”

Data Protection Engineering

“Engineering those principles relates not only to choices made with regards to designing the processing operation but also selecting, deploying, configuring and maintaining appropriate technological measures and techniques. These techniques would support the fulfilment of the data protection principles and offer a level of protection adequate to the level of risk the personal data are exposed to. **Data Protection Engineering can be perceived as part of data protection by Design and by Default. It aims to support the selection, deployment and configuration of appropriate technical and organizational measures in order to satisfy specific data protection principles.** Undeniably it depends on the measure, the context and the application and eventually it contributes to the protection of data subjects’ rights and freedoms”

Privacy Enhancing Technologies (PETs)

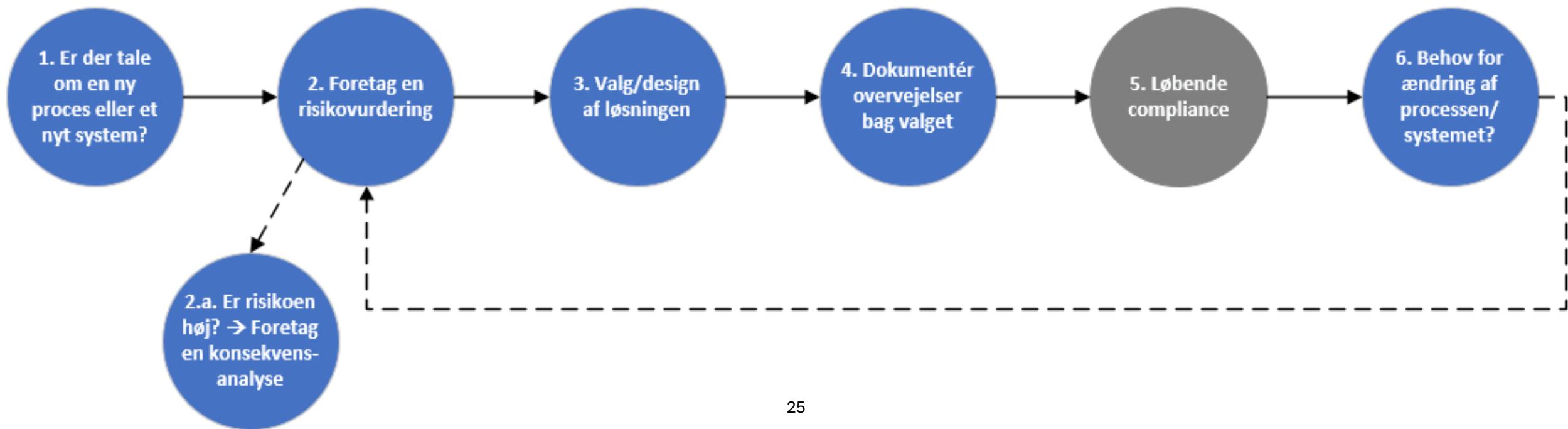
“Privacy Enhancing Technologies (PETs) cover the **broader range of technologies that are designed to support implementation of data** protection principles at a systemic and fundamental level”

3. ”Data protection by design and by default” i praksis

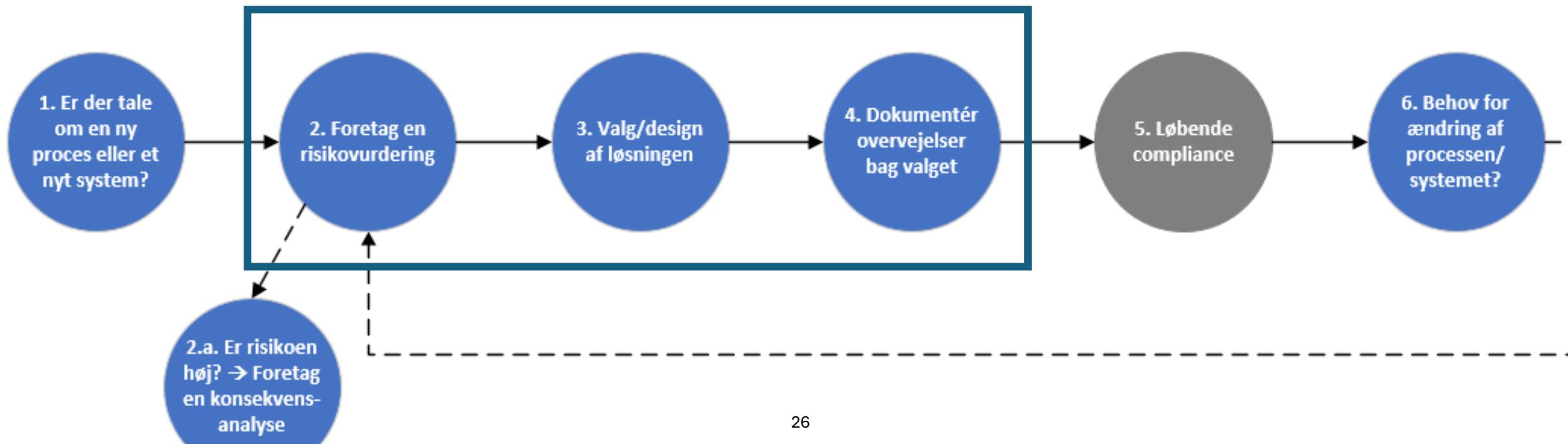
Overblik over kravene

Krav	Uddybning	Data Protection by Design (art. 25)
Ansvarlighed	Overblik, ledelsesforankring og dokumentation	
Generelle principper	Hvilke, hvorfor, hvordan og hvor længe?	
Behandlingsgrundlag	Vi må behandle de her oplysninger, fordi...	
Oplysningspligt	Privatlivspolitik, velkomstbreve, personalehåndbog mv.	
Henvendelser fra registrerede	Indsigt, berigtigelse, begrænsning, sletning mv.	<i>Alle GDPR's krav og principper skal, så vidt muligt, og under hensyntagen til økonomi og "state-of-the-art", tænkes ind ifbm. design og/eller indkøb af nye IT-systemer og digitale løsninger.</i>
Databehandlere og fælles dataansvar	Kontrakter: Hvem har ansvaret for hvad?	
Fortegnelser	Overblikket til Datatilsynet	
Sikkerhed	Riskobaseret sikkerhed (digitalt og fysisk)	
Databrud	Logning + evt. anmeldelse/orientering af registrerede	
Konsekvensanalyse/DPIA	Dybdegående (forudgående!) analyse ved <i>høj risiko</i>	
Dabeskyttelsesrådgiver/DPO	Kun krav for enkelte virksomheder	
3. lands overførsl	Særlige krav, hvis data opbevares i eller tilgås fra et land udenfor EU	

Databeskyttelse gennem Design – En step-by-step guide



Databeskyttelse gennem Design – En step-by-step guide



Step 2: Risikovurderinger og konsekvensanalyser

Risikovurdering:

"En kortlægning af alle de risici behandlingen medfører og en kategorisering (scoring, sandsynlighed og alvorlighed) heraf. En vurdering af hvad der er passende tekniske og organisatoriske foranstaltninger, til at sørge for at forordningen overholdes og dette kan dokumenteres." (Datatilsynet.dk)

Konsekvensanalyse/DPIA:

- En mere omfattende, formbunden vurdering af risici og konsekvenser (+ evt. høring hos Datatilsynet)
- Alene påkrævet ved (nye) behandlinger med en *høj risiko* (reguleret i art. 35 og 36)

Eksempel: Kritik af gymnasiums brug af eksamensovervågningssoftware

- Datatilsynet indledte en sag af egen drift for at undersøge en række gymnasier med henblik på eksamensovervågningssoftware
→ Roskilde Katedralskole
 - Behandlingsgrundlag, proportionalitetsprincippet og opbevaringsbegrænsning undersøgt.
- Eksamener gennemført på private computere
- ExamCookie
 - Behandler en række personoplysninger → Navn, CPR-nummer, skærmbilleder, aktive URL-adresser m.v.

Eksempel: Kritik af gymnasiums brug af eksamensovervågningsssoftware

- Behandlingsgrundlag 
 - Behandling af data **nødvendig af hensyn til gymnasiets udførelse af sine myndighedsopgaver**
- Proportionalitetsvurdering 
 - Opfyldt, bl.a. i lyset af **nødvendighed i forhold til formålet om at opdage og forebygge snyd.**
 - En række indstillinger blev slået fra
- Opbevaringsbegrænsning 
 - Opfyldt, **inden for 30 dage.**
- Oplysningspligt 
 - Opfyldt → Datatilsynet havde bl.a. lagt vægt på at om det var **letforståelig kommunikeret** taget i betragtning at der var tale om gymnaselever i aldergruppen 16-20 år
- **Det var hvad Datatilsynet som udgangspunkt undersøgte.**

Eksempel: Kritik af gymnasiums brug af eksamensovervågningsssoftware

- Dabeskyttelse gennem design: 
 - Handler om at træffe passende tekniske og organisatoriske foranstaltninger.



Henset til bestemmelsens risikobaserede tilgang skal den dataansvarlige således foretage en risikovurdering og i den forbindelse identificere eventuelle risici for de registreredes rettigheder, og fastlægge deres sandsynlighed og alvor med henblik på at gennemføre foranstaltninger til effektivt at afbøde de identificerede risici.

- **Roskilde Katedalskole:** Risikoen var lav og acceptabel + Programmet indrette til at sikre DPbDD
- **Datatilsynet:** Roskilde Katedalskole har identificeret enkelte risici....
 - Utilsigtet indsamling af data i udklipsholderen
 - Hvis eleven tilgår sine helbredsoplysninger under prøven

Eksempel: Kritik af gymnasiums brug af eksamensovervågningsssoftware

- ... Men Roskilde Katedralskole havde ikke ”*identificeret og vurderet alle de specifikke risici for elevernes rettigheder og frihedsrettigheder, der er forbundet med brugen af eksamensovervågning, og at visse risici, som gymnasiet har identificeret, ikke er håndteret fyldestgørende.*”
- Ved behandling af skærmbilleder sker der f.eks. Indsamling af information fra elevernes skærme
 - F.eks. Elevernes private bogmærker, adresselinjen kan indeholde søge- og browserhistorik m.v.
- Elever med ordblindhed aflægger prøven med særlige hjælpemidler
 - F.eks. Oplæsning af tekst, ordforslag m.v.
 - Behandling af helbredsoplysninger, og derfor potentelt i strid med Art. 9
- Filer og mapper på computerne kan indeholde private data
 - Metadata eller navne
- Fejlkonfiguration med forkert eksamensstarttidspunkt
 - ”Den flittige studerende” - Der indsamles oplysninger inden eksamensstart.
- Utilstrækkelig risikovurdering førte til **kritik**

Step 3: Valg/design af løsning

”Privacy Enhancing Technologies” / PET’s

- Designet af løsninger og de komponenter der vælges, skal understøtte privatlivsbeskyttelse.
- Eksempler fra Datatilsynet:
 - Anonymisering (Obs! Den juridiske definition sætter baren meget højt)
 - Pseudonymisering
 - Dataminimeringsforanstaltninger
 - Adgangskontrol i form af access management + auditsporing
 - Kryptering
 - Inputvalidering, sikkerhedsmønstre, kodemønstre, sikre netværks topografier mv.
 - Systemmæssig håndhævelse af databeskyttelse (= tving brugeren)

ENISA: DATA PROTECTION ENGINEERING – From Theory to Practice (January 2022)

Overordnet emnet	Konkrete PET's
3. Anonymisation and pseudonymisation	k-ANONYMITY Differential privacy Selecting the anonymization scheme
4. Data masking and privacy-preserving computations	Homomorphic encryption Secure multiparty computation Trusted execution environments Private information retrieval Synthetic data
5. Access, communication and storage	Communication channels Privacy preserving storage Privacy-enhancing access control, authorization and authentication
6. Transparency, intervenability and user control tools	Privacy policies Privacy icons Sticky policies Privacy preference signals Privacy dashboard Consent management Consent gathering Consent management systems Exercising right of access Exercising right to erasure, right to rectification

Andre eksempler på PET's

EDPS & AEPD: Joint paper on 10 misunderstandings related to anonymization (Apr. 2021)

Misunderstanding	Fact
<i>"Pseudonymisation is the same as anonymisation"</i>	Pseudonymisation is not the same as anonymisation
<i>"Encryption is anonymisation"</i>	Encryption is not an anonymisation technique, but it can be a powerful pseudonymisation tool.
<i>"Anonymisation of data is always possible"</i>	It is not always possible to lower the re-identification risk below a previously defined threshold whilst retaining a useful dataset for a specific processing
<i>"Anonymisation is forever"</i>	There is a risk that some anonymisation processes could be reverted in the future. Circumstances might change over time and new technical developments and the availability of additional information might compromise previous anonymisation processes.
<i>"Anonymisation always reduces the probability of re-identification of a dataset to zero"</i>	The anonymisation process and the way it is implemented will have a direct influence on the likelihood of re-identification risks .
<i>"Anonymisation is a binary concept that cannot be measured"</i>	It is possible to analyse and measure the degree of anonymization.
<i>"Anonymisation can be fully automated"</i>	Automated tools can be used during the anonymisation process, however, given the importance of the context in the overall process assessment, human expert intervention is needed .
<i>"Anonymisation makes the data useless"</i>	A proper anonymisation process keeps the data functional for a given purpose
<i>"Following an anonymisation process that others used successfully will lead our organisation to equivalent results"</i>	Anonymisation processes need to be tailored to 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.
<i>"There is no risk and no interest in finding out to whom the data belongs"</i>	Personal data has a value in itself, for the individuals themselves and for third parties. Re-identification of personal data can be achieved by combining datasets or by linking them to other datasets .

Step 4: Dokumentation

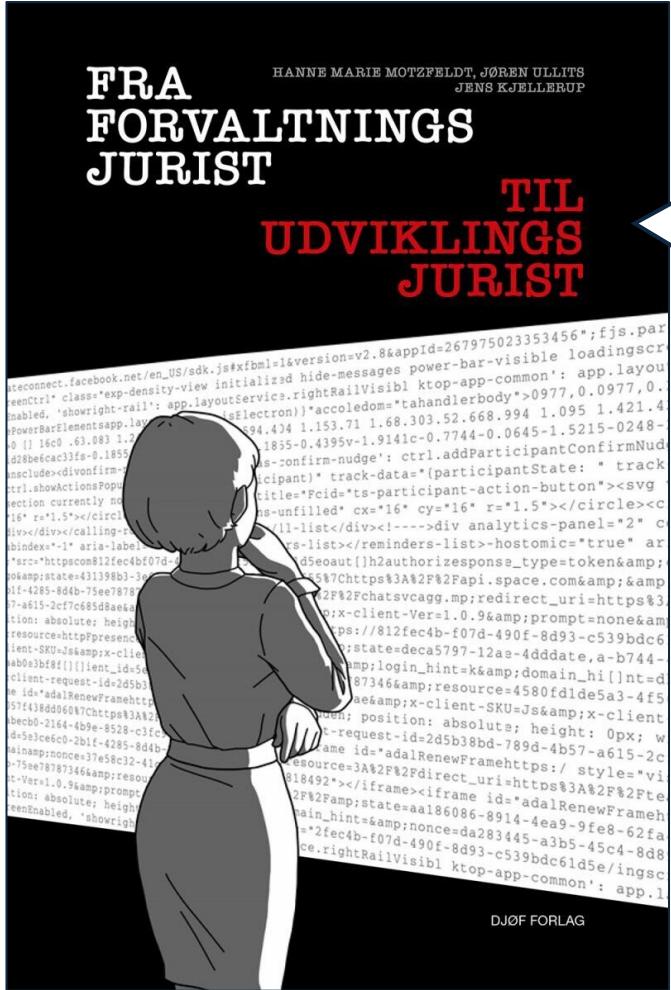
- **Artikel 25 er, ligesom alle andre krav i GDPR, underlagt et krav om dokumentation**
- Elementer fra artikel 25, som evt. bør dokumenteres:
 - Risikovurdering
 - Valg af privatlivsfremmende teknologier (f.eks. Anvendt til pseudonymisering af persondata)
 - Omkostningsovervejelser og trade-offs (fx sikkerhed vs. brugervenlighed)
 - Hvis dataansvarlige er kunde, der vælger en standardløsning → Dokumenter gerne overvejelser ifbm. valg af løsning
- **Der er ingen facilitliste eller formkrav**
 - Den dataansvarlige skal blot være i stand til at påvise de overvejelser, der er blevet gjort og de valg der blev truffet

Opsumming

- Bestemmelsen er et godt eksempel på at GDPR er *teknologineutral* og *risikobaseret*
- GDPR skal overholdes ved udvikling og drift af digitale løsninger → Det gælder også for AI
- Artikel 25's primære bidrag:
 - Understrege at GDPR skal **tænkes ind fra starten** baseret på en risikovurdering ("by *Design*")
 - **Standardindstillingen** skal være den der giver mest muligt databeskyttelse ("by *Default*")
 - Der efterlades rum til at tage **hensyn til omkostningsniveau** – men det må forudsætte, at overvejelser herom kan dokumenteres!

4. Samarbejde mellem forskellige faggrupper

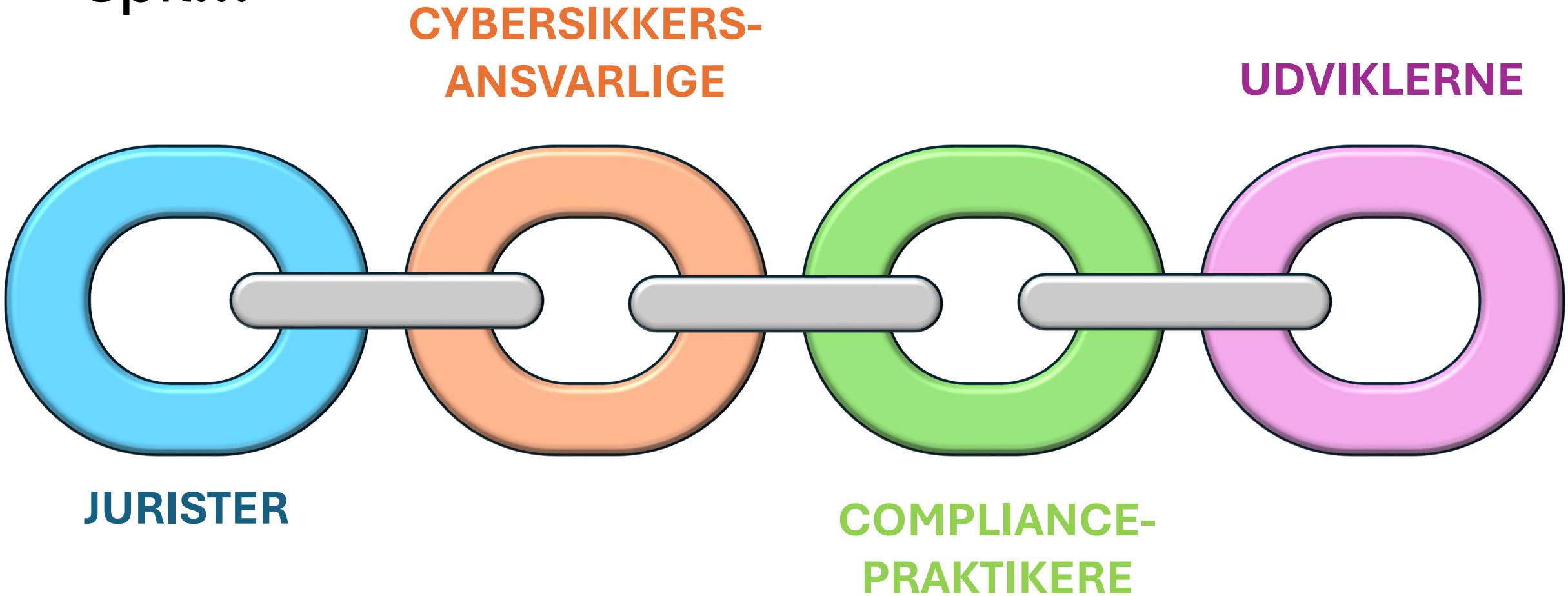
Jurister skal have teknologiforståelse og blive medspillere i udviklingsprocessen



"En udviklings- og driftsjurist bør ikke kun have juridiske kompetencer, **men også indsigt i den rolle, som de juridiske kompetencer spiller (eller burde spille) under offentlige digitaliseringsprocesser og kompetencer til at udfylde rollen.**"

Fra forvaltningsjurist til udviklings- og driftsjurist, Motzfeldt, Ullits, Loiborg og Kjellerup, 2. udgave, 2024, s. 18

Et samarbejde mellem faggrupper kommer i spil...



Vejledninger mv. med fokus på det praktiske perspektiv

- **Rådet for Digital Sikkerhed:** [Vejledning om privatlivsfremmende teknologier](#) (2020)
- **Fransk datatilsyn (CNIL):** [GDPR Developer Guide](#) (2020) – Obs! Tilgængelig på [GitHub](#)
- **ENISA:** [DATA PROTECTION ENGINEERING – From Theory to Practice](#) (Januar 2022)
- **DS/EN 17529:2022:** [Data protection and privacy by design and by default](#) (maj 2022)
- **ICO (UK):** [Privacy-enhancing technologies \(PETs\)](#) (Senest opdateret, juni 2023)

OPGAVE

- Sammen med jeres sidemand er i ansvarlige for projektstyringen i en virksomhed der udvikler mobilapplikationer. Jeres underordnede team af udviklere, skal designe en ny mobilapplikation til en sundhedsplatform. Applikationen skal kunne indsamle og behandle følsomme personoplysninger, herunder helbredsoplysninger. Applikationen skal gøre det muligt at kunne tilmelde sig til de regionale lægehuse. Patienterne skal have muligheden for tidsbestilling og have muligheden for at skrive til lægen vedrørende symptomer på sygdomme og bestilling af recepter.
- I har desværre et begrænset budget og i må derfor prioritere hvilke opgaver/tiltag i kan gennemføre. I skal prioritere 5 tiltag som applikationen skal kunne for at sikre at i overholder principperne for 'Data Protection by Design'.
- **Hvordan vil I sikre, at applikationen overholder principperne om 'Data Protection by Design'?** Brug venligst 7-8 minutter på opgaven, og derefter samler vi op i fællesskab.