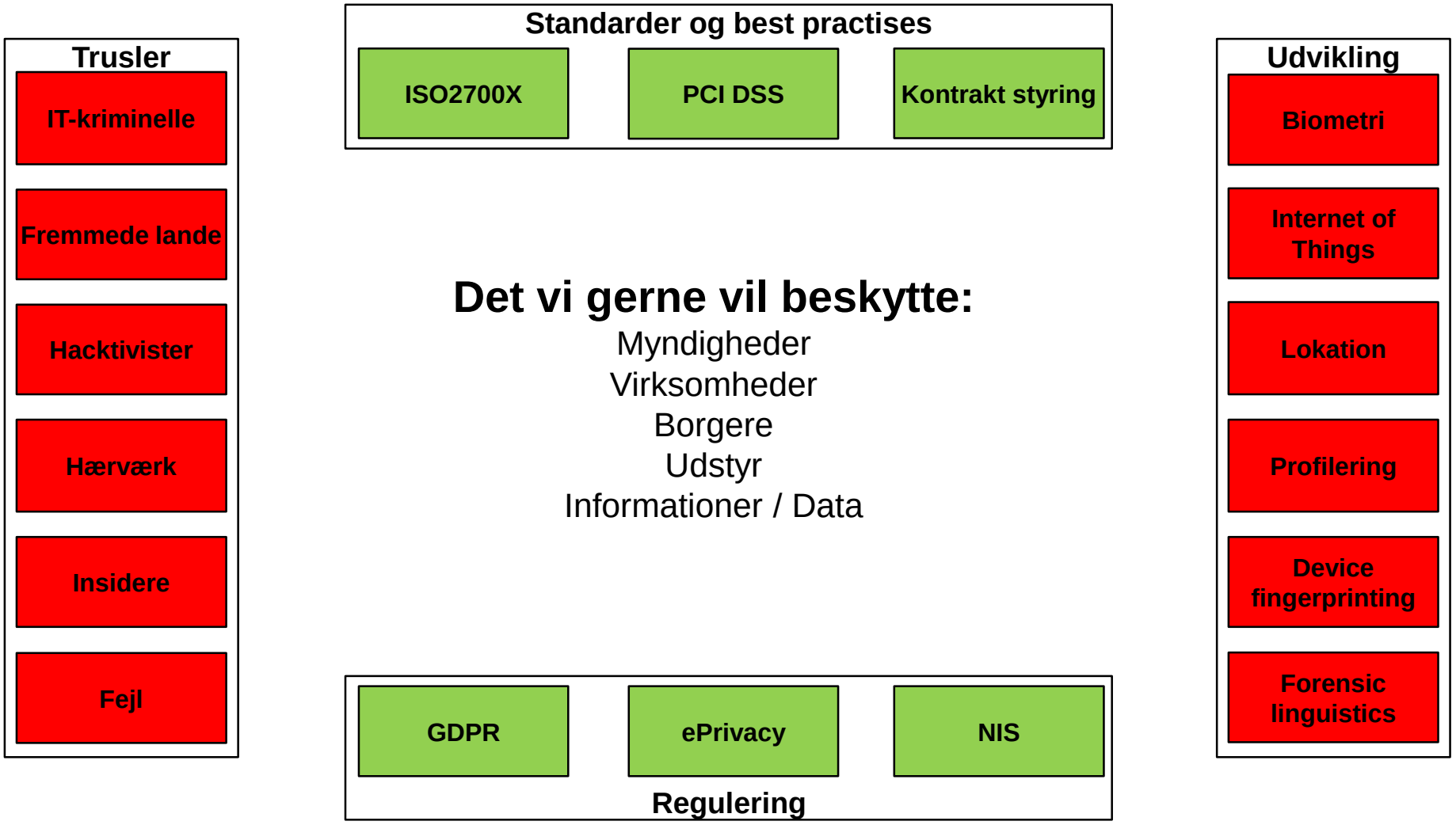
Implementering af persondataforordningen

- Med fokus på sikkerhed og design

Situationsbillede



Persondataforordningen

- Principper: Lovlig, rimelig, gennemsigtig, formål, minimeret, korrekte, lagringsbegrænsning, sikkert, dokumenteret
- Rettigheder: Oplysningspligt, indsigtsret, berigtige, slette, begrænse, underrette, portabilitet, indsigelse, profilering
- Pligter: DPbDx2, databehandlere, fortegnelse, sikkerhedsforanstaltninger, DBN, DPIA, DPO, overførsel

- I praksis er der
  - mange afvejninger
  - tvivl om fortolkninger – især i europæisk perspektiv
  - regler som er vanskelige (grænsende til umulige) at efterleve.

Sikkerhed versus DPbD, indhold

Direktiv 95/46/EF om sikkerhed, artikel 17

"...den registeransvarlige skal iværksætte de fornødne tekniske og organisatoriske foranstaltninger..."

"Disse foranstaltninger skal ... tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer..."

Forordning 2016/679 om sikkerhed, artikel 32

"...gennemfører den dataansvarlige og databehandleren passende tekniske og organisatoriske foranstaltninger..."

"...for at sikre et sikkerhedsniveau, der passer til ... risici" "for fysiske personers rettigheder og frihedsrettigheder"

Forordning 2016/679 om DPbD, artikel 25

"...gennemfører den dataansvarlige ... passende tekniske og organisatoriske foranstaltninger..."

"...med henblik på integrering af de fornødne garantier i behandlingen for at opfylde kravene i denne forordning og beskytte de registreredes rettigheder"

Summa sumarum

For både sikkerhed og DPbD er der tale om implementering af passende tekniske og organisatoriske foranstaltninger.

Men for sikkerhed har foranstaltningerne til formål at tilvejebringe et sikkerhedsniveau, der passer til risici.

Mens foranstaltningerne efter DPbD skal understøtte at kravene i forordningen og de registreredes rettigheder efterleves.

Fordi formålene med de to artikler er forskellige er de passende tekniske og organisatoriske foranstaltninger, som kan bruges til at understøtte disse formål også forskellige.

Eller sagt på en anden måde: DPbD handler ikke alene om at designe sikkerhedsforanstaltninger ind i it-systemerne (det er kun en delmængde af designkravene). Det handler om meget mere end det.

Sikkerhed versus DPbD, tidspunkt

Direktiv 95/46/EF om sikkerhed, præambel 46, som uddyber artikel 17

"...der træffes de fornødne tekniske og organisatoriske foranstaltninger både under selve udformningen og under iværksættelsen af en behandling..."

Forordning 2016/679 om sikkerhed, artikel 32

Ingen bemærkninger om tidspunkt hverken i artikel 32 eller i præambel 83

Forordning 2016/679 om DPbD, artikel 25

"...både på tidspunktet for fastlæggelse af midlerne til behandling og på tidspunktet for selve behandlingen..."

Summa sumarum

DPbD tidspunktet gælder også for sikkerhed, fordi sikkerhed er en delmængde af kravene i forordningen og de registreredes rettigheder.

Kravene om DPbD gælder dog ikke for legacysystemer – ud over på sikkerhedsområdet, hvor det også hidtil har skulle være på plads under selve udformningen.

Legacysystemer skal derfor kun rettes til, hvis der sker væsentlige ændringer/changes. Det kan overvejes om der kan introduceres kompenserende foranstaltninger.

Man kan sige, at artikel 17 i databeskyttelsesdirektivet, 95/46/EF, splittes op i flere dele, samtidig med at den udvides:

- forordningens artikel 32 om sikkerhed
- forordningens artikel 25 om databeskyttelse gennem design
- (og for den sags skyld også artikel 35 om konsekvensanalyse)
- med artikel 24 som overligger for de passende tekniske og organisatoriske foranstaltninger.

DPbD, materielt indhold 1

Meget sparsomt med oplysninger om materielt indhold

Artikel 25: Pseudonymisering.

Præambel 78: Minimering af behandling, pseudonymisering, gennemsigtighed, den registrerede skal kunne overvåge behandlingen, forbedre sikkerhedselementer.

Ingen praksis af betydning.

Begrebets baggrund

Ann Cavoukians syv privacy by design principper

Proaktiv, ikke reaktiv
Foranstaltninger skal altså iværksættes inden en risiko materialiserer sig.

Privacy som standardindstilling
Den registrerede skal ikke selv foretage sig noget for at beskytte sine oplysninger; beskyttelsen skal være slået til fra starten.

Privacy skal være indlejret i systemet
Foranstaltningerne skal designes ind i et systems arkitektur og ikke tilføjes efterfølgende.

Der skal være fuld funktionalitet
Der skal være både fuld funktionalitet og fuld sikkerhed, og der må således ikke være en modstrid mellem sikkerhed og databeskyttelse.

Beskyttelse i hele livscyklussen
Beskyttelsen skal indbygges i designfasen inden systemet sættes i drift og være aktiv i hele systemets levetid.

Transparens
Der skal være gennemsigtighed i forretningsmodeller og teknologier, og det der signaleres, skal kunne verificeres (af en uafhængig tredjepart).

Brugeren i centrum
De registreredes interesser skal være i fokus f.eks. gennem standardindstillinger, notifikation og empowerment af brugerne, så de er i kontrol.

DPbD, materielt indhold 2

ENISA

Designstrategier med design- eller arkitekturmønstre

Eksempel: En designstrategi er f.eks. ”Demonstrate”. Hovedelementet i denne strategi er, at man kan demonstrere, at man efterlever reglerne (Cavoukians 6. princip). Denne strategi gør f.eks. brug af designmønstrene, privacy management systems, logning og auditering.

John Borking

Privacy Enhancing Technologies, hvor man med bestemte teknologier, som f.eks. kryptering, pseudonymisering og anonymisering understøtter kravene i forordningen og de registreredes rettigheder.

DI

Tre-trins-raket: Data Protection Impact Assessment, Data Protection by Design og Privacy Enhancing Technologies.

Revision og Regnskab

Artikel i december 2017.

Rådet for Digital Sikkerhed

Case tilgang.

DPbD, cases

Fritekstfelt versus dropdown

Styring af muligheder for input.

Data Discovery og Data Loss Prevention

Find personoplysninger og undgå tab af fortrolighed ved fejl.

Indsigtsknap

Lav et setup, hvor alle personoplysninger i alle systemer hentes frem ved klik på en knap.

Automatiseret sletning ved ophævelse af samtykke

Når et samtykke eventuelt trækkes tilbage skal behandlingen straks ophøre (med mindre der er anden hjemmel). I en række tilfælde kan man derfor lige så godt slette personoplysningerne.

Udløbsdatoer

Sæt udløbsdatoer på data når de skabes, således at de automatisk slettes eller anonymiseres, når formålet er opfyldt.

Biometri i den registreredes varetægt fremfor i en central database

Lad den registrerede beholde sin biometri på et lokalt smartcard fremfor i en central database.

Pseudonymer

Langt de fleste behandlinger kan ske uden at den registrerede er identificeret.

Privacy credentials / partielle pseudonymer

Identiteten er hemmelig, men autorisation kan ske alligevel ud fra de relevante kriterier, f.eks. gyldigt kørekort, mand / kvinde eller myndig.

Sikkerhed, materielt indhold 1

Meget sparsomt med oplysninger om materielt indhold

Artikel 32: Pseudonymisering, kryptering; fortrolighed, integritet, tilgængelighed og robusthed; genoprette tilgængelighed; regelmæssig afprøvning.

Præambel 83: Vurdere risici; en række forskellige typer at trusler nævnes.

Desuden: masser af praksis!!! (og en sikkerhedsbekendtgørelse, som dog ikke gælder efter 25. maj).

Sikkerhedsbekendtgørelsen, Alle data

- Der skal fastlægges interne bestemmelser og instrukser
  - Organisation
  - Fysisk sikring
  - Adgangskontrol
  - Autorisation og kontrol hermed
  - Ansvar for behandling og destruction af ind- og uddata
  - Anvendelse af EDB-udstyr
  - Tilsyn med overholdelse af sikkerhedsforanstaltningerne
  - Årlig revision
- Instruktion til medarbejderne
- Databehandleraftaler
- Samme sikkerhed på hjemmearbejdspladser
- Forhindre uvedkommendes fysiske adgang
- Reperation og service samt salg og kassation af medier
- Autorisation
  - Autorisation må kun gives til opfyldelse af formål med behandling
  - Revision samt Drift- og systemtekniske opgaver kan også opnå adgang
  - Kun autoriserede brugere skal have adgang og kun til det som autorisationen dækker

Sikkerhed, materielt indhold 2

Sikkerhedsbekendtgørelsen, Alle data, fortsat

- Inddatamateriale
  - Adgangsbegrænsning til dem der er autoriseret
  - Sletning når det ikke er relevant for formål
  - Fornødne sikkerhedstiltag ved sletning
- Uddatamateriale
  - Ditto som inddatamateriale
  - Revison og personer med drift- og systemtekniske opgaver må få adgang
  - Opbevares så uvedkommende ikke kan få adgang
- Eksterne kommunikationsforbindelser skal sikres

Sikkerhedsbekendtgørelsen, Data med anmeldelsespligt

- Autorisationer skal redegøre for R, WE, D
- Kontrol af de tildelte autorisationer hvert halve år
- Kontrol med afviste adgangsforsøg og evt. blokering
- Logning af alle anvendelser af personoplysninger
  - Tidspunkt
  - BrugerID
  - Anvendelse
  - Den registrerede
  - Anvendt søgekriterium
  - 6 mdr., dog op til 5 år.

I praksis: ISO27002

- Informationssikkerhedspolitikker og retningslinjer
- Organisering (rolle, funktionsadskillelse, mobilt udstyr, fjernarbejdspladser)
- HR-sikkerhed (før, under og efter ansættelsen)
- Styring af aktiver (ansvar, klassifikation, mediehåndtering)
- Adgangsstyring (politik, brugeradgang, brugeransvar, system og app-adgang)
- Kryptering
- Fysisk sikring (områder, udstyr)
- Driftssikkerhed (procedurer og ansvar, skadelig kode, backup, logning, installation, sårbarheder, audit)
- Kommunikationssikkerhed (netværk og segmentering, overførsel af information)
- Anskaffelse, udvikling og vedligehold
- Leverandørforhold (krav til og styring af)
- Styring af brud
- Beredskab (kontinuitet og retablering)
- Compliance (love, standarder, best practises og kontrakter)

Sikkerhedsteknologier

- Antivirus
- Patchning
- Firewall
- Backup
- Netværkssegmentering
- Identity and access governance
- Asset management
- Logging (Siem)
- Shadow IT discovery
- Penetrationstests
- Kryptering
- Secure DNS
- Klassifikation
- Automatiseret compliance

Sikkerhedscompliance

- IT-sikkerhedspolitik
- ISMS
- Regelsæt
- Procedurer
- Beredskab
- Awareness
- Risikovurdering

- Mapping af GDPR og ISO27002
- Excel-fil til dokumentationskrav

Risici

- Artikel 25 (design): “Under hensyntagen til … risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder”
- Artikel 32 (sikkerhed): ditto
- Der er mange andre steder i forordningen, hvor et konkret tiltag afhænger af en risikovurdering:
  - Forordningen er mere fleksibel end direktiv 95/46/EF
  - Der Introduceres mere usikker for de dataansvarlige: er vores skøn det samme som Datatilsynets?
- Artikel 35 (konsekvensanalyse): Hvis der er bl.a. høj risiko skal der foretages en konsekvensanalyse.
- Igen en smuk sammenhæng mellem artiklerne 24 (dataansvarligs ansvar), 25 (design), 32 (sikkerhed) og 35 (konsekvensanalyse)

Risikovurdering

Konsekvensvurdering

- Identificer aktiver
- For hvert aktiv, hvad er så **konsekvensen** (stor, medium, lav) ved tab af fortrolighed, tilgængelighed og integritet

Trusselsvurdering

- Identificer trusler og fastlæg **sandsynlighed** (stor, medium lav)

Sårbarhedsvurdering

- Hvilke korrigerende tiltag har vi således at vi kan reducere sandsynligheden til en given restsandsynlighed

Beskrivelse af risikobilledet

- Sammenvejning af risici, forslag til ekstra korrigerende foranstaltninger og ledelsesmæssig accept af restrisiko

Afstikker: risikobilledet

Konsekvens / Sandsynlighed	Lav	Mellem	Høj
Lav			
Mellem			
Høj			

Spørgsmål

LinkedIn

https://www.linkedin.com/in/henning-mortensen-343b0/

IT-Universitetet

https://www.itu.dk/efteruddannelser/itu-professional-courses/kurser/persondataforordningen