Retsudvalgets høring om it-tekniske tiltag til sikring af følsomme personoplysninger

Christiansborg onsdag d. 12. november

Grit Munk, chefkonsulent, Ingeniørforeningen IDA

Privacy By Design

Udviklet af den canadiske Information & Privacy Commissioner Ann Cavoukian

Privacy handler ikke om at skjule oplysninger, men om retten til at kunne kontrollere informationer om os selv. At skabe empowerment ifht vores personlige oplysninger

PbD er en teknisk løsning til at holde sig på forkant med den teknologiske udvikling. Lovgivning skal medvirke til at hensynet til privatlivet tages med i opbygningen af systemet.

PbD er som teknologi udviklet og kan implementeres f.eks. gennem offentlige it-udbud som et krav til leverandører af offentlig it- og digitaliseringsløsninger.

PbD og privacy by default er essentielle principper i EU kommissionens forslag til forordning

Big data gør privacy vigtigere en nogensinde

Big data er kendetegnet ved:

Volume (mængde): Større mængder af data end normale systemer kan håndtere.

Velocity (hastighed): Højt tempo i datatilstrømning.

Variety (mangfoldighed): Mange forskellige datatyper og kilder.

Big data technologies:

Persondata er det nye olie – Big data er maskinen, der skal pumpe det op:

En ny generation af teknologier og arkitekturer, designet til at udtrække værdi fra meget store mængder data, ved i højt tempo at opsamle, opdage og eller analysere data.

Kilde: Wikipedia, 29.01.2014 og Ann Cavoukian & Jeff Jonas.

Big data udfordrer privacy på 3 niveauer:

Datahøst: indsamling af data sker i langt større stil og det langt fra altid, at de enkelte borgere aktivt har givet tilsagn om. at deres private data må opsamles og hvad de må bruges til. Og ofte er folk slet ikke klar over, hvad der registreres.

Data mining: Her renses data og analyseres i forhold til andre data med det formål at skabe sammenhæng mellem aktuelle forhold og dermed give os ny viden. Det kan være i forskningssammenhænge, men det kan også være til rent kommercielle forhold.

Applikationsfasen: Datamining resulterer i en algoritme, der er en generaliseret form af den nye viden. Værdien af den ligger i koblingen til den virkelige verden, f.eks. et datasæt af skoleelever eller kunder. Afhængig af algoritmen kan man herved for eksempel forudsige handlinger eller præferencer. Et kendt eksempel er "Dem, der lånte denne bog, kunne også lide xxx".

Det kræver en dynamisk teknologi, der følger med udviklingen i databrug!

7 fundamentale principper:

1. Proaktiv beskyttelse – det handler om at forebygge
2. **Privacy by default**, dvs. automatisk beskyttelse som standardindstilling. Hvis man ikke gør noget er personsikkerheden intakt.
3. Privacy er indbygget i it-design, arkitektur og forretningspraksis og ikke noget man vælger til.
4. Beskyttelse ses som plussum og ikke som et trade off – man vil gerne have mulighederne og fordelene.
5. Fuld livscyklus beskyttelse, hvor data bliver sikkert opbevaret og sikkert destrueret,
6. Uanset hvilken praksis der bruges, skal det være åbent og verificerbart for alle og
7. Brugercentreret, dvs. brugervenligt og med fokus på brugerens privatliv.

I praksis:

- Det skal være klart, hvad de tilsigtede *og utilsigtede* konsekvenser kan blive.
- Det skal være klart, hvor data er kritiske data – i sig selv eller i *forbundethed.*
- Undgå unødig transport af data – eller anonymiser dem (som ved forskning)
- Offentliggør kravsspecifikationerne, så beskyttelsesniveauet bliver officielt

- Borgerne skal let kunne se, hvad egne data har været anvendt til. (Transparens log)
- Borgerne skal kunne vælge, hvem der ser hvilke af borgerens egne data
- En myndighedsperson må kun få adgang til den delmænge af en borgers data, der er absolut nødvendig til myndigheds udøvelsen

Udviklingen peger på, at Skyen bliver vores personlige datalager

- Der udvikles p.t. apps, der kan hjælpe os til at kontrollere vores skyer: Hvem der må få adgang til vores data og præcist hvilke.