Rådet for Digital Sikkerhed

13. november 2017

Rådet for Digital Sikkerheds vejledning om Databeskyttelse gennem Design

Databeskyttelse gennem Design

I denne vejledning gennemgår Rådet for Digital Sikkerhed, RfDS, begrebet Databeskyttelse gennem Design, som adresseres i persondataforordningen.

Konklusionen er, at Databeskyttelse gennem Design stiller krav om, at den dataansvarlige i hele livscyklen for en applikation, der behandler personoplysninger, understøtter alle de garantier, der stilles i forordningen. Den dataansvarlige skal dermed overveje, om applikationen kan designes på en sådan måde, at man med tekniske og organisatoriske foranstaltninger kan understøtte f.eks. databeskyttelsesprincipperne, fastlæggelsen af hjemmel til behandlingen, de registreredes rettigheder og de pligter, som påhviler dataansvarlige og databehandlere. Dermed rækker begrebet langt ud over blot at iværksætte tekniske og organisatoriske sikkerhedsforanstaltninger, jf. den oprindelige definition af begrebet som stammer fra Ann Cavoukian. I denne vejledning giver RfDS nogle eksempler på, hvad der i praksis kan ligge i begrebet.

Baggrund og disclaimer

Persondataforordningen, som adresserer hvordan personoplysninger må behandles fra maj 2018, kan være noget af en mundfuld for de fleste organisationer at gå i gang med. RfDS har derfor besluttet at komme med nogle få vejledninger på området, hvor vi forklarer forskellige dele af forordningen, som det i praksis kan være særlig vanskeligt at arbejde med.

Vejledningerne er fortrinsvist blevet til på baggrund af henvendelser fra organisationer, der har ønsket at få belyst et konkret problem. Vejledningerne er ikke autoritative i betydningen, at man kan støtte ret på dem. Vejledningerne har heller ikke et politisk eller kommercielt sigte. Endelig er der ikke et rådgiveransvar tilknyttet vejledningerne. I stedet skal vejledningerne ses som et praktisk anvendelige bud på, hvordan RfDS som en gruppe af professionelle eksperter anskuer et begreb eller en problemstilling. Vejledningerne kan aldrig erstattes af en konkret vurdering.

Historik

Databeskyttelse gennem Design stammer fra Ann Cavoukian, der siden 90'erne har spillet en væsentlig international rolle for at beskytte personoplysninger. Over tid nåede Cauvokian frem til den væsentlige konklusion, at databeskyttelse bedst kan opnås ved at designe sine løsninger på en sådan måde at databeskyttelsen er understøttet igennem selve designet af løsningen. Hun kondenserede sit arbejde ud i syv principper, der fremgår af nedenstående figur.

Rådet for Digital Sikkerhed
Vester Farimagsgade 37B, 1.th., 1606 København V
Telefon: +45 53 36 02 23 mail: info@digitalsikkerhed.dk web: www.digitalsikkerhed.dk

Ann Cauvokians privacy by design principper

1. ***Proaktiv, ikke reaktiv***
   Foranstaltninger skal altså iværksættes inden en risiko materialiserer sig.
2. ***Privacy som standardindstilling***
   Den registrerede skal ikke selv foretage sig noget for at beskytte sine oplysninger; beskyttelsen skal være slået til fra starten.
3. ***Privacy skal være indlejret i systemet***
   Foranstaltningerne skal designes ind i et systems arkitektur og ikke tilføjes efterfølgende.
4. ***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.
5. ***Beskyttelse i hele livscyklussen***
   Beskyttelsen skal indbygges i designfasen inden systemet sættes i drift og være aktiv i hele systemets levetid.
6. ***Transparens***
   Der skal være gennemsigtighed i forretningsmodeller og teknologier, og det der signaleres, skal kunne verificeres (af en uafhængig tredjepart).
7. ***Brugeren i centrum***
   De registreredes interesser skal være i fokus f.eks. gennem standardindstillinger, notifikation og empowerment af brugerne, så de er i kontrol.

Flere andre parter har siden arbejdet videre med dette begreb. ENISA har f.eks. i 2014 i rapporten ”Privacy and Data Protection by Design” plæderet for anvendelsen af designstrategier med design- eller arkitekturmønstre, ud fra hvilke man kan vælge i værktøjskassen af privatlivsfremmende teknologier, PETs. Artikel 29-gruppen ønskede i rapporten ”The Future of Privacy” fra 2009, at der blev etableret et nyt Privacy by Design Principle i europæisk ret.

Med persondataforordningen har begrebet fået sin egen artikel. I artikel 25, stk. 1 hedder det således, at den dataansvarlige skal gennemføre ”passende tekniske og organisatoriske foranstaltninger,…, som er designet med henblik på effektiv implementering af databeskyttelsesprincipper,…, og med henblik på integrering af de fornødne garantier i behandlingen for at opfylde kravene i denne forordning og beskytte de registreredes rettigheder.” Foranstaltningerne skal gennemføres ”på tidspunktet for fastlæggelse af midlerne til behandling og på tidspunktet for selve behandlingen”. Dette må fortolkes således, at efterlevelsen af forordningens bestemmelser skal designes ind på så tidligt et stadie i et it-projekt som

muligt og vedblive at understøtte forordningen indtil den sidste behandling af personoplysningerne, som vil være en sletning eller anonymisering; altså i hele it-systemets lifecycle. Allerede designede systemer berøres altså ikke af bestemmelsen - med mindre de re-designes eller ikke lever op til eksisterende lovgivning.

Mere end sikkerhed

Der har fra forskellig side været en udlægning af Databeskyttelse som Design som om det alene handlede om at implementere foranstaltninger, der understøttede it-sikkerhed. It-sikkerhed er bestemt et af de formål, som er omfattet af bestemmelsen. Men som det fremgår af ovenstående, er begrebet langt bredere og det er altså nødvendigt, men ikke tilstrækkeligt at kigge ned i sikkerhedsværktøjskassen, når der skal vælges design. Tværtimod er man nødt til at kigge på det bredest mulige spektrum af organisatoriske og teknologiske muligheder, når man skal fastlægge et design, der understøtter hele forordningen.

Den dataansvarlige har altså en pligt til at overveje sine muligheder i bred forstand, men man kan ikke pege på bestemte tiltag, som skal implementeres efter artikel 25. Det må forventes, at vi over de kommende år gennem praksis vil få fastslået, hvad der konkret som minimum skal overvejes at implementere.

Databeskyttelse gennem Design – cases

For at forstå bredden i begrebet er det relevant at se på nogle eksempler.

1. **Fritekstfelt versus dropdown**
   I mange systemer med strukturerede data er der lavet fritekstfelter, hvor der kan tilføjes oplysninger efter konkret behov. Man kunne f.eks. forestille sig, at der i tilknytning til håndtering af betalinger i et økonomiprogram kunne tilføjes noter til betalingsfrister. Tanken kunne være at en regnskabsmedarbejder kunne tilføje, at der er givet kredit i 14 dage grundet kortvarige likviditetsproblemer hos en kunde. Men når nu feltet er lavet som et fritekstfelt kunne regnskabsmedarbejdere også skrive andre ting som f.eks. at der er givet kredit i 14 dage grundet at kunden ikke kan komme til computeren som følge af kemobehandling på hospital. Feltet kunne i øvrigt også bruges til subjektive og usaglige vurderinger af kunden. Når der i designet anvendes fritekstfelter mister den dataansvarlige kontrollen med, om de registreringer, der foretages i systemet, er saglige og lovlige. Systemet kunne måske re-designes således, at fritekstfeltet blev erstattet med en dropdownmenu med prædefinerede og saglige valgmuligheder.

2. **Tab af personoplysningers fortrolighed**
   Der sker med jævne mellemrum, at personoplysninger ved menneskelige fejl bliver offentliggjort på en hjemmeside. Typisk er der tale om sagsakter eller lister af personer med tilknyttet personnummer. Man kunne designe sit CMS-system således, at der automatisk blev foretaget skanning efter personoplysninger i det materiale, som uploades til hjemmesiden. Denne disciplin kaldes data discovery. Programmet søger så f.eks. på en syntaks på seks_cifre-fire_cifre. Hvis programmet finder en sådan syntaks, spørger det brugeren om der er tale om CPR-numre og i bekræftende fald blokeres upload til hjemmesiden.

3. **Automatiseret oplysning og indsigt**
   Den registrerede skal oplyses forinden behandling foretages og har desuden ret til at få indsigt i hvilke personoplysninger der behandles til hvilke formål. Disse processer kan automatiseres. Oplysningen kan indbygges automatisk i flowet af data, der går umiddelbart forud for indhentningen af personoplysninger. Indsigtsretten kan designes ved at lave en knap, som brugeren

af et system kan klikke på og dermed få indsigt i hvilke personoplysninger organisationen er i besiddelse af – f.eks. navn, adresse, forsendelsesadresse, kundenummer, købshistorik og historik for anvendelse af hjemmeside.

4. **Automatiseret sletning når samtykke trækkes tilbage**
   I en række tilfælde har den dataansvarlige lov til at behandle personoplysninger fordi den registrerede har givet sin tilladelse - hvilket kaldes samtykke. Hvis den registrerede af personlige grunde fortryder, at han har givet samtykke kan han trække dette tilbage igen, hvorefter databehandleren ikke har lov til at behandle personoplysningerne (med mindre den dataansvarlige kan finde en anden hjemmel). I sådanne tilfælde kunne systemet designes således at alle personoplysninger, der blev behandlet med hjemmel i samtykke automatisk blev slettet i det øjeblik samtykket blev trukket tilbage.

5. **Udløbsdatoer**
   I en række tilfælde kan den dataansvarlige designe sine systemer således, at der tilknyttes en sletningsdato til personoplysninger allerede på det tidspunkt, hvor de fødes ind i et system. Det kan f.eks. være, at man designer sit økonomisystem således, at alle bogførte data slettes eller anonymiseres, når der er gået fem år efter registreringen (og dermed ikke er hjemmel til at behandle oplysningerne efter bogføringsloven). Et andet eksempel er, at man kan fastlægge en politik for sit e-mail-system således, at e-mails automatisk slettes senest et år efter at de er modtaget. E-mails, som der er et formål med at behandle ud over eet år, kan så overflyttes til et ESDH-system eller et fildrev indenfor det pågældende år.

6. **Biometriske identifikatorer**
   Biometriske identifikatorer er typisk en beregnet talværdi, der siger noget om et biologisk kendetegn ved en registreret. Det kan f.eks. være en talværdi beregnet for et fingeraftryk, hvor flere observationspunkter ved fingeren vægtes sammen af en algoritme, som så udregner et tal. Når beregningen foretages flere gange på den samme finger bliver talværdien altid den samme. Hvis en anden fingers observationspunkter vægtes sammen findes en anden talværdi. Fingeraftryk står ikke til at ændre, og derfor er det ganske indgribende at miste kontrollen med talværdien for sin finger. Derfor er det allerede en del af praksis at fingeraftryk kun i særlige tilfælde opsamles i centrale systemer, hvor den registrerede mister kontrollen med anvendelsen. I stedet kan man designe en løsning, hvor den registrerede tildeles et smartcard, hvor den registrerede selv udregner talværdien for sit fingeraftryk og på den baggrund giver en PIN-kode, der kan bruges til at identificere den registrerede.

7. **Pseudonymer**
   I en række tilfælde er det ikke relevant at dem, som behandler personoplysninger kan identificere den registrerede, mens de behandler oplysningerne. Man kan derfor adskille indholdsoplysninger fra identificerende oplysninger. En patient (den registrerede) kunne f.eks. få taget en blodprøve hos sin læge. Lægen kunne så tildele blodprøven et løbenummer, når den sendes til analyse på et laboratorium. Laboratoriet kender ikke den registrerede, men kan sagtens analysere blodprøven alligevel. Laboratoriet sender diagnosen tilbage til lægen sammen med løbenummeret. Lægen genskaber så forbindelsen mellem løbenummeret og diagnosen og kan fastslå, hvilken diagnose patienten (den registrerede) har. Dette kaldes pseudonymisering.

8. **Privacy credentials / partielle identiteter**
   I stedet for at bede brugere (de registrerede) om at afsløre deres identitet kunne man bede om noget andet, som afslører det man har brug for at vide. F.eks. er det tilstrækkeligt i en række sammenhænge at vide om den registrerede har et gyldigt kørekort, er mand eller kvinde, er myndig eller er medlem af en forening og har betalt kontingent. Fordelen er, at den registrerede er i langt højere kontrol med sine oplysninger, når de ikke har identificeret sig, men det alene er autentificeret, at de opfylder et bestemt relevant kriterium for at blive autoriseret til et eller andet.

Konklusion

Eksemplerne ovenfor illustrerer, hvordan forordningens hensigter kan understøttes gennem et godt design, der tager udgangspunkt i at beskytte de registrerede i forhold til mange af de garantier, der findes i forordningen. Det er næsten kun kreativiteten, der stiller grænser for, hvad der kan tænkes at ligge i begrebet. Men der er en pligt til at vælge et godt design. Ann Cavokians designprincipper og ENISAs designstrategier med design- eller arkitekturmønstre er gode inspirationskilder til, hvordan man kan tænke sit design på en måde, der understøtter forordningen. Som tiden går og vi får mere praksis at forholde sig til, vil vi blive klogere på det konkrete materielle indhold, som ligger i artikel 25, og som hele tiden vil udvikle sig og til stadighed give mulighed for bedre beskyttelse af de registrerede.