BILAG 3: PRIVATLIVSFREMMENDE TEKNOLOGIER

Beskyttelsen af personoplysninger kan forbedres ved at designe sin teknologi således, at den reducerer graden af indgriben i de registreredes privatliv. Dette kaldes Privacy by Design (PbD) - eller i forordningen: data protection by design. Som en del af dette design kan man supplere med teknologier, som er privatlivsfremmende. Disse teknologier kaldes Privacy Enhancing Technologies (PET). Beslutninger om hvilket design og hvilke teknologier der skal vælges kan baseres på en konsekvensanalyse (Data Protection Impact Assessment, DPIA og Privacy Impact Assessment, PIA).

Det skal bemærkes, at der ikke findes globalt accepterede definitioner af disse tre begreber.

I forordningens præambel 78 nævnes dog at databeskyttelse gennem design bl.a. henviser til "minimering af behandlingen af personoplysninger" og "pseudonymisering af personoplysninger så hurtigt som muligt". Det nævnes også i præambel 83 at kryptering kan begrænse risici, og i præambel 28 at pseudonymisering kan mindske risikoen, ligesom pseudonymisering og kryptering eksplicit fremhæves i artikel 32. Det er dog tanken at pseudonymisering og kryptering skal suppleres af andre databeskyttelsesforanstaltninger, jf. præambel 28. Det eneste ord, som er eksplicit defineret i forordningen, er pseudonymisering, hvor det i artikel 4, nr. 5 hedder: " behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, forudsat at sådanne supplerende oplysninger opbevares separat og er underlagt tekniske og organisatoriske foranstaltninger for at sikre, at personoplysningerne ikke henføres til en identificeret eller identificerbar fysisk person".

PbD og PET må anvendes ud fra en konkret vurdering. I dette bilag skitseres et par muligheder overordnet.

Data protection by design

Der er tale om data protection by design, når man designer sin teknologi således, at den reducerer graden af indgriben i de registreredes privatliv. Et banalt eksempel er, når et it-system designes således, at adgangen til indsamlede personoplysninger teknisk begrænses til kun at omfatte ansatte med en given rolle i en virksomhed istedet for alle virksomhedens medarbejdere. Jo færre, der har adgang til data, jo mindre er risikoen for, at data kan blive brugt til et formål, der er uforeneligt med de registreredes interesser, og jo bedre er adgangsbegrænsningen set fra den pågældende registreredes synspunkt.

Det vigtigste designprincip er, hvor det er muligt, at designe løsningen således, at den slet ikke behandler personoplysninger. Dette kan f.eks. ske ved at anonymisere jvf. nedenfor.

Et andet centralt designprincip er at overveje at overdrage retten til at skabe sammenhæng mellem de registrerede personoplysninger og identiteten til den registrerede. Hermed afskærer virksomheden sig selv fra at identificere det den registrerede, som personoplysningerne vedrører, men den registrerede kan skabe sammenhængen, når den registrerede skønner, at det er i vedkommendes egen interesse.

Man kan lade sig inspirere til designprincipper ved at følge DI's skabelon til konsekvensanalyser[3] eller ved at besvare nogle af de spørgsmål der er i Tjeklisten til nærværende vejledning.

Et designprincip, som har fået særskilt plads i forordningen, er Data Protection by Default, hvor alle de gode databeskyttelsestiltag, man har indbygget i en applikation og vil give mulighed for at de registrerede kan gøre brug af, slås til som standard, og ikke overlades til den registrerede selv at slå til.

Privacy Enhancing Technologies

De privatlivsfremmende teknologier dækker principielt over alle teknologier, som giver forbedringer af privatlivsbeskyttelsen i et it-system. Således vil f.eks. rollebaseret adgangskontrol, hvor adgang til personoplysninger begrænses til alene at være den gruppe medarbejdere, der har en given rolle, kunne anskues som en privatlivsfremmende teknologi. Rigtig mange teknologier ville derfor kunne falde i denne kategori og bør anvendes for at skabe sikkerhed og for at komme i compliance med forordningen. Overordnet kan man tal om bl.a. nedenstående grupper af teknologier:

Data Loss Prevention
Kan forhindre e-mails med specifikke data eller syntakser i at forlade virksomheden, som f.eks. CPR-numre, kontonumre eller lignende.

Data Discovery
Giver mulighed for at afdække persondata på virksomhedens netværk der ikke er ligger på de rette systemer.

Identity and Access Governance
Kan give overblik over brugerroller og deres adgange til systemer og data og omfatter bl.a. "Priviledged Account Management" som skal forhindre it-folk i at have for brede beføjelser og "Role Mining", der kan afdække om der er nogle ukendte mønstre i fordelingen af roller og rettigheder.

Log management
Gør det muligt at redegøre for, hvem der har haft adgang til hvilke data hvornår.

Backup
Backup sikrer at data kan genskabes – f.eks. efter man har været udsat for en sikkerhedshændelse. Retten til at blive glemt som omtalt i forordningen kan dog være en udfordring, da det kan være vanskeligt at slette specifikke data fra backup systemet.

Shadow-it discovery
Virksomhedens ansvar dækker også over informationer der placeres på systemer udenfor it-afdelingens kontrol. Denne type services kan afdække den totale mængde af it-services der anvendes i organisationen.

---

[3] http://di.dk/Virksomhed/Produktion/IT/itsikkerhed/personoplysninger/Pages/DIsskabelonforPrivacyImpactAssessment.aspx.

Information Lifecycle Management
Sletning af data der ikke skal anvendes mere er en væsentlig praktisk udfordring. Med denne type software kan man sætte regler op for datas "udløbsdato".

Pseudonymization
Identificerende data erstattes af koder i kombination med en nøgle, således at data ikke kan henføres til en person uden anvendelse af nøglen, hvilket som nævnt i forordningen bidrager til at reducere risiko.

Encryption
Kodning af data således at data kun kan læses af den, som er besiddelse af nøglen.

Anonymization
Konvertering af dele af data således at de data som kan henføres til en person slettes eller gøres permanent ulæsbare; f.eks. gennem kryptering, hvor dekrypteringsnøglen slettes.

Virtual or partial identities
En identitet, som ikke kan tilknyttes en konkret fysisk person. Der kan eventuelt på samme it-system laves en kombination af flere virtuelle identiteter uden linkability. I en række sammenhænge kan den dataansvarlige nøjes med at kende bestemte karakteristika ved en fysisk person - f.eks. over 18 år, gyldigt adgangskort eller studerende/pensionist. En række identitetsudbydere kan sikre dette for den registrerede. Identitetsudbyderen skal kende til den registreredes rigtige identitet.

Et par af teknologierne fortjener en uddybelse på grund af den særlige rolle de spiller i forordningen.

Anonymisering

Anonymisering er en meget vidtgående PET. Det betyder, at personoplysninger endegyldigt fraknyttes den registreredes identitet således, at der ikke igen på nogen måde kan etableres forbindelse. I dette tilfælde vil der således typisk ikke længere være tale om personoplysninger i lovens forstand, men altså blot om data. De pågældende data falder derfor udenfor lovens anvendelsesområde.

Det faktum, at der ikke kan genetableres en forbindelse mellem data og identitet, kan være en udfordring - f.eks. hvis der opstår mistanke om, at data kan tilknyttes et kriminelt forhold eller hvis en registreret ikke kan forfølge sine rettigheder. Det vil ikke være muligt at opklare, hvilken registreret der står bag kriminalitet eller har krav på at få opfyldt en rettighed, når data er anonymiseret. Omvendt giver anonymisering den bedst tænkelige beskyttelse af privatlivets fred.

Anonymisering kan være ganske udfordrende at etablere i praksis. Hvis de umiddelbart identificerende oplysninger som f.eks. navn og adresse fjernes fra et datasæt, kan der sagtens blandt de resterende oplysninger være mulighed for at identificere en registreret, f.eks. ved at isolere nogle data, ved at koble data på tværs af datasæt eller ved at finde en stor sandsynlighed for at to sæt data hører sammen. Anonymisering foregår ud fra to grundlæggende teknikker. Den ene mulighed er at randomizere data f.eks. ved at tilføje uægte data til ægte data for en registreret eller ved at bytte om på data således, at et gennemsnit over det samlede datasæt fastholdes. Den anden mulighed er at generalisere, f.eks. således at visse data ikke bliver præcist gengivet, men falder i intervaller.

Anonymisering brugt i forbindelse med kommunikation kaldes kommunikationsanonymisering. Det betyder, at et it-system ikke registrerer oplysning som f.eks. IP-adresse, MAC-adresse, e-mailadresse og cookie-ID. På den måde kan den registrerede øge sin sandsynlighed for, at virksomheden ikke ved, hvilken part der har indgået i kommunikationen. It-systemet kan tilbyde dette. Den registrerede kan dog også selv foretage tiltag, som anonymiserer vedkommendes egne data i kommunikationsflowet.

En anden afart kaldes transaktionsanonymisering. Ideen er at to parter skal kunne indgå en transaktion uden at den registreredes identitet er kendt. Begrebet har været anvendt i forbindelse med anonyme online betalinger. En registreret kan i sin bank få udstedt en virtuel pengeseddel, som er anonym ligesom fysiske trykte pengesedler. Pengesedlen kan den registrerede bruge i en onlinebutik. Onlinebutikken kan af banken få verifikation for, om pengesedlen er ægte, og ikke er brugt tidligere, og kan herefter gennemføre transaktionen med den registrerede uden at kende den registreredes identitet. Når dette kan gennemføres skyldes det en avanceret krypteringsmekanisme baseret på zero-knowledge-proof, som vi ikke vil komme nærmere ind på her.

Pseudonymisering

Pseudonymisering betyder, at personoplysninger fraknyttes den registreredes identitet, men istedet tilknyttes en nøgle, som så kan tilknyttes en identitet. Fordelen er, at personoplysningerne ikke umiddelbart kan tilknyttes den registrerede. Alene den, der kontrollerer nøglerne, kan identificere den registrerede. Det fjerner en række risici og gør databehandlingen mere sikker set fra den registreredes synspunkt.

F.eks. kunne man forestille sig, at en registreret går til sin praktiserende læge for at blive undersøgt for en sygdom, hvis diagnose skal stilles på baggrund af en blodprøve. Den registrerede identificerer sig overfor lægen, som autentificerer den registrerede. Herefter tages blodprøven, som tilknyttes en nøgle af lægen. Blodprøven kan så sendes hvorsomhelst hen, uden at nogen ved hvem den tilhører - herunder til et vilkårligt laboratorium, der skal analysere prøven. Resultatet af blodprøveundersøgelsen kommer tilbage til lægen, der på baggrund af nøglen tilknytter prøvens resultat til den registrerede og stiller diagnosen. Fordelen for den registrerede er, at alene den praktiserende læge ved, hvad hans diagnose er; laboratoriets ansatte ved det ikke og har ikke mulighed for at finde ud af det.

I et mere ekstremt tilfælde kunne man forestille sig, at den registrerede selv fik nøglen, således at det kun var den registrerede selv, der kunne se sin diagnose. I de tilfælde, hvor den registrerede selv administrerer nøglen, kunne der måske være mulighed for, at den registrerede selv var dataansvarlig i lovens forstand, og dermed vil en række forhold blive lettere for virksomheden.

Pseudonymisering rummer rigtig mange muligheder for at forbedre databeskyttelsen set fra den registreredes synspunkt, herunder muligheden for at give den registrerede selv kontrol over sine egne personoplysninger.

Kryptering

Kryptering er en byggesten, der bruges i flere af ovenstående løsninger. Kryptering er en proces, som omdanner oprindelig information til information, der er ulæselig

for tredjepart. Dette foregår som regel ved at bruge en offentlig og privat nøgle. Hvis Alice vil sende en fortrolig besked til Bob, bruger hun Bobs offentlige nøgle til at kryptere den med. Der er alene Bob, der har kontrol med sin private nøgle, og dermed er det alene Bob, der kan læse beskeden.

Kryptering er uendelig meget mere kompliceret og kan bruges i langt flere sammenhænge end skitseret ovenfor. Noget af det, som er særligt lovende, er, at man under særlige forudsætninger kan foretage databehandling på krypterede data uden at disse dekrypteres, og dermed uden at en registrerets identitet afsløres. Det vil være alt for omfattende i denne sammenhæng at komme igennem krypteringens muligheder. Men hovedbudskabet er, at hvis man kerer sig om at beskytte personoplysninger, er det en rigtig god ide at se på, om kryptering kan bringes i anvendelse på en eller anden måde.

Et par bemærkninger om lovgivning

Det er værd at notere sig, at pseudonymisering aldrig og anonymisering ikke altid betyder, at data i juridisk forstand ikke er personoplysninger. Det er f.eks. ikke nok alene at fjerne direkte identificerbar information som navn og adresse fra et datasæt. Der skal mere til, f.eks. en proces for generalisering (altså fjernelse af de enkelte records) med kontrol af at man ikke f.eks. indirekte kan slutte sig frem til de registreredes identitet, for at opnå det resultat at man ikke længere behandler personoplysninger. Psedonymisering og anonymisering skal derfor ses som metoder til at forbedre de registreredes sikkerhed. Har man anonymiseret korrekt, falder de anonymiserede data imidlertid udenfor forordningens anvendelsesområde.

Kilder

Der findes to vigtige kilder til det videre arbejde med privatlivsfremmende teknologier:

- Artikel 29-gruppens ”Opinion 05/2014 on Anonymisation Techniques”, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.
- IT- og Telestyrelsens “Nye digitale sikkerhedsmodeller”, http://digitaliser.dk/resource/781482.