Digital

VEJLEDNING

DI's skabelon for Data Protection Impact Assessment

DI Digital
1787 København V.
3377 3377
itek.di.dk
itek@di.dk

DI Digital – et branchefællesskab i Dansk Industri for virksomheder inden for it, tele, elektronik og kommunikation

Udgivet af: DI Digital

Redaktion: Henning Mortensen

Afløser "DI's skabelon for Privacy Impact Assessment", oktober 2014, ISBN: 978-87-7144-040-9.

ISBN: 978-87-7144-089-8

0.07.16

Digital

INDHOLDSFORTEGNELSE

Baggrund

PIA Q&A

PIA-proces

PIA-analyse

Bilag A: Indledende afklaring af behov for DPIA

Bilag B: Juridiske principper

Bilag C: Dataflowanalyse

Bilag D: Datasubjektets risici

Bilag E: Korrigerende foranstaltninger

Bilag F: Information

Bilag G: Privatlivsfremmende teknologier

BAGGRUND

Privatlivets fred (privacy) har stor fokus i en tid, hvor nye teknologiske muligheder åbner sig hver dag, og hvor der i stigende grad behandles personoplysninger fra forskellige side om brugernes/borgernes adfærd på internettet. Ny lovgivning i form af persondataforordningen har også stor betydning for området, i og med at virksomheder og myndigheder skal til at beskytte personoplysninger på en helt ny måde, når forordningen får virkning i 2018. DI har haft stor fokus på området gennem mange år og har udgivet en række publikationer på området.

Denne publikation har til formål at være en let tilgængelig vejledning i, hvordan virksomheder kortlægger konsekvenser for beskyttelse af data ved digital behandling af personoplysninger og iværksætter tiltag til beskyttelse og kontrol af beskyttelse af personoplysninger. En sådan kortlægning kaldes en Data Protection Impact Assessment (DPIA) eller en Privacy Impact Assessment (PIA)[1].

Anvendelsen af personoplysninger kan skabe store fordele for virksomhederne og deres kunder. Generelt er anvendelsen af big data et af de digitale områder, hvor forretningen kan udvikle sig mest. For mange virksomheder er det nødvendigt at tage bl.a. disse teknologier til sig for at kunne klare sig i den globale konkurrence og for at leve op til kunders ønsker og forventninger. Det er dog samtidig vigtigt, at virksomhederne holder sig for øje, at nogle kunder ikke ønsker, at deres personoplysninger behandles, eller kun behandles i et meget begrænset omfang. For at imødekomme disse kunders tillid er det vigtigt, at virksomheder tænker over, om deres forretningsmodel kan forbedres for at imødekomme disse kunder.

Mange lande har lavet skabeloner for PIA'er. Dette dokument er inspireret af arbejde lavet af myndigheder i Canada[2], Australien[3], UK[4] og Danmark[5]. De nationale frameworks, som er kilderne for denne publikation, er ganske omfattende, og lovgivningen og kulturen i de forskellige lande varierer. Med persondataforordningen introduceres Data Protection Impact Assessment i europæisk ret. Vi har derfor også gennemgået disse regler, og præsenterer dem i et selvstændigt bilag. Denne publikation lægger sig dog ikke op af en bestemt lovgivning og søger således ikke at skabe compliance med en bestemt lovgivning, men skal ses som en vejledning, der søger at være generisk på tværs af regulatoriske regimer. Derfor vil der for hvert nationalt marked, virksomheden opererer på, fortsat være behov for en juridisk compliancevurdering. Eksistensen af en DPIA, og de overvejelser virksomheden

---

[1] Denne type analyser blev oprindeligt lavet med henblik på bredt at vurdere konsekvenserne for privatlivet ved et givent initiativ, Privacy Impact Assessment, PIA. I persondataforordningen bruges dog ordet Data Protection Impact Assessment, som må antages at have et mere indskrænket anvendelse end PIA, fordi der alene er fokus på data og ikke bredt fokuseres på privacy, som også omfatter f.eks. adgang til krop og bolig.
[2] http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12451&section=text#cha1.0.
[3] http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/privacy-impact-assessment-guide.
[4] http://www.ico.org.uk/pia_handbook_html_v2/html/0-advice.html.
[5] http://www.digst.dk/Arkitektur-og-standarder/Styring-af-informationssikkerhed-efter-ISO-27001/Konsekvensvurdering-for-privatlivet.aspx.

har gjort sig i denne forbindelse, vil alt andet lige gøre compliancevurderingen lettere.

Man skal være opmærksom på at der findes PIA'er, som er lavet til anvendelse af konkrete teknologier, der behandler personoplysninger, f.eks. på RFID-området[6]. Denne vejledning søger at være generisk på tværs af teknologier og er således teknologineutral.

DPIA Q&A

Hvad er en DPIA?

En DPIA er en vurdering af risici, set fra et individs synspunkt, ved at en aktør behandler individets personoplysninger.

DPIA'en består af en analyse og af en proces. Analysen sikrer, at de rette spørgsmål bliver stillet og besvaret. Processen sikrer, at spørgsmål stilles og svar gives på det rette tidspunkt i en teknologis livscyklus. DPIA'en foretages ikke af individet selv men istedet af den aktør, som behandler personoplysningerne.

Hvad er en personoplysning?

En personoplysning er enhver form for information om en identificeret eller identificerbar fysisk person.

Hvad er en behandling af personoplysninger?

En behandling af personoplysninger er enhver operation, som personoplysningerne gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.

Hvorfor skal virksomheder foretage en DPIA?

Der er mange gode grunde til at beskytte personoplysninger set fra individets synspunkt. Disse grunde en gennemgået grundigt i "De overvågede" af DI og Forbrugerrådet, kapitel 1 og 2. Grundlæggende skal virksomheden være opmærksom på, at når der behandles personoplysninger, opgiver individet (typisk i rollen som kunde eller medarbejder) egen kontrol med nogle af sine personoplysninger. Der er meget individuelle grænser for, i hvilket omfang det opleves som værende en god ide, og det har uomtvisteligt en række implikationer for det pågældende individ og vedkommendes tillid til virksomheden.

Set fra virksomhedens synspunkt er der også god grund til at værne om individernes personoplysninger og lave en DPIA. For det første vil signalet om, at der samles så få personoplysninger ind som muligt, at de behandles så lidt som muligt af så få som muligt og sikres bedst muligt, skabe tillid hos individerne og dermed flere kunder. For det andet skabes der med en DPIA mulighed for at tekniske løsninger, der beskytter privacy, designes ind i it-systemerne, hvilket er langt billigere end at

[6] http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf.

bygge dem på efterfølgende. De nye persondataforordning stiller krav om, at beskyttelse af personoplysninger designes ind i løsningerne i fremtiden. Det er dermed omkostningsminimerende at lave en DPIA. For det tredje kan man bedre styre risici for problemer med behandling af personoplysninger, når man har en DPIA. For det fjerde mindskes sandsynligheden for databrud og dermed for tab af trust og omdømme. For det femte er det lettere at sikre compliance med en given lovgivning.

Hvornår skal en DPIA gennemføres?

En DPIA skal gennemføres efter behov f.eks. ved etablering eller ved væsentlige ændringer af teknologier, som digitalt behandler personoplysninger, eller som på anden måde har konsekvenser for beskyttelsen af personoplysninger.

Teknologier skal forstås i bredeste forstand. Det mest typiske eksempel vil være databaser, der behandler oplysninger som navn, adresse, e-mail, cpr-nummer, osv. Men teknologier som f.eks. passive RFID-tags, der løbende afgiver et nummer til omgivelserne, vil i visse sammenhænge kunne henføres til et individ. Selv om der ikke foretages en egentlig databehandling, har teknologien altså implikationer for beskyttelsen af personoplysninger og bør derfor omfattes.

I persondataforordningen er der krav om, at der gennemføres DPIA'er "hvis en type behandling, navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang, sammenhæng og formål, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder", jf. artikel 35, stk. 1. I Artikel 35, stk. 3 uddybes det, at der især skal gennemføres DPIA'er, når der sker:

a) en systematisk og omfattende vurdering af personlige forhold vedrørende fysiske personer, der er baseret på automatisk behandling, herunder profilering, og som er grundlag for afgørelser, der har retsvirkning for den fysiske person eller på tilsvarende vis betydeligt påvirker den fysiske person
b) behandling i stort omfang af særlige kategorier af oplysninger, jf. artikel 9, stk. 1, eller af personoplysninger vedrørende straffedomme og lovovertrædelser, jf. artikel 10, eller
c) systematisk overvågning af et offentligt tilgængeligt område i stort omfang.

Desuden præciseres det i persondataforordningens artikel 35, stk. 4 og 5, at tilsynsyndighederne kan lave lister, som præciserer hvilke behandlingsaktiviteter, der kræver, at der skal gennemføres DPIA'er og hvilke behandlingsaktiviteter, der ikke kræver DPIA'er. Ifølge artikel 35, stk. 6, skal disse lister koordineres på europæiske plan, hvis de vedrører udbud eller påvirker områder, hvor der indgår registrerede fra flere medlemsstater.

Hvem skal gennemføre en DPIA?

DPIA'en skal efter behov gennemføres eller sikres gennemført af den aktør, der har ansvaret for behandling af personoplysninger.

Den, der har ansvaret, kaldes den dataansvarlige. Den, som behandler data, kaldes databehandleren (f.eks. en outsourcingpartner eller cloudleverandør). Det individ, som persondata omhandler, kaldes datasubjektet.

De personer, som hos den dataansvarlige har ansvaret for det it-system, som skal behandle personoplysningerne, bør gennemføre DPIA'en. Typisk vil der være tale om en it-projektgruppe. Hvis den dataansvarlige har en it-sikkerhedschef, en it-sikkerhedsansvarlig og/eller en jurist til rådighed, bør vedkommende tilknyttes arbejdet med DPIA'en. I henhold til persondataforordningens artikel 35, stk. 2, bør der også tilknyttes en databeskyttelsesrådgiver (DPO), hvis virksomheden har udpeget en sådan i medfør af persondataforordningens artikel 37.

DPIA-proces og DPIA-analyse

En DPIA-proces skal sikre, at konsekvenser for beskyttelse af personoplysninger kortlægges på det optimale tidspunkt i it-projekter. En DPIA-analyse skal sikre, at de rette afklarende spørgsmål til it-projektet bliver stillet.

DPIA-PROCES

Der er lige så mange modeller for DPIA-processen, som der er DPIA'er. Hvis der findes en it-projekt model (eller som vi kalder det i denne forbindelse, en teknologiprojektmodel) i virksomhedens organisation, bør DPIA'en knyttes an til denne. I denne vejledning har vi valgt en meget simpel model, der ser ud som følger:

I "idefasen" skal det afklares, om der er behov for en DPIA, og virksomheden bør desuden skabe sig et overblik over de juridiske regler for behandling af personoplysninger i de lande, hvor it-løsningen skal fungere.

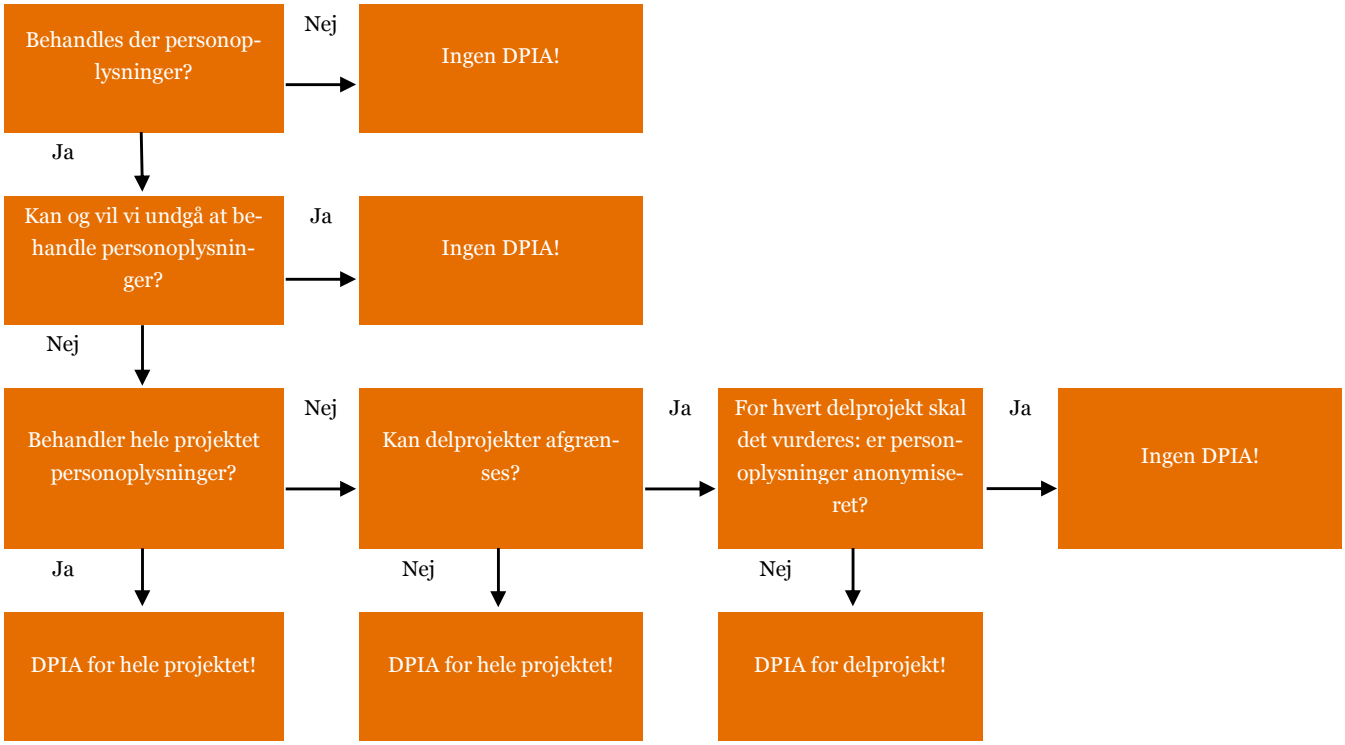
Indledende afklaring af behov for DPIA

Det er projektlederens ansvar at sikre, at der undervejs igennem teknologiprojektets faser foretages en vurdering af, om der skal gennemføres en DPIA, og i givet fald om den skal dække hele eller dele af projektet. I den forbindelse indhentes informationer fra projektgruppens deltagere eller fra data- og systemejere rundt omkring i organisationen. Det er vigtigt at sikre sig, at man har alle relevante parter med omkring bordet. Jo tidligere i forløbet i ovenstående figur man får gjort sig overvejelser om beskyttelse af personoplysninger, jo billigere bliver det at lave den rette løsning. Undervejs i forløbet vil man foretage justeringer af projektet. Det er vigtigt, at man ved sådanne justeringer også vurderer, om DPIA'en skal justeres, således at DPIA'en udvikler sig sammen med projektet. Hvis de teknologier, som tages i anvendelse i projektet, har meget store konsekvenser, kan det overvejes, om man vil konsultere et udvalg af de individer, hvis data skal behandles med teknologien.

Det er centralt, at man i alle dele af projektet overvejer fordele og ulemper ved at behandle personoplysninger, herunder om man helt kan undgå at behandle personoplysninger. Hvis man kan undgå at behandle personoplysninger, udsætter man individet for den mindst mulige risiko, man opnår den bedste beskyttelse af

privacy og måske kan dette påvirke datasubjektets tillid positivt. Hvis man kan undgå at behandle personoplysninger, falder man også helt uden for kravene i persondataforordningen. Der findes forskellige teknologier og metoder til at begrænse behandlingen af personoplysninger. Et udvalg af disse er gennemgået i bilag G. Det er vigtigt at få inspiration til, hvordan man i nogle sammenhænge kan designe sig ud af brugen af personoplysninger. Hvis man når frem til, at det alligevel er nødvendigt at behandle personoplysninger, skal man finde ud af, om det er i alle projektets dele, at der behandles personoplysninger, eller om det kun er i dele af projektet.

Beslutningen, af om der skal foretages en DPIA, og hvilken del af projektet en sådan i givet fald skal dække, afhænger af en række forhold, der kan skitseres som følger:



På baggrund af ovenstående kan man konkludere, om der skal gennemføres en total DPIA, en DPIA for delprojektet eller ingen DPIA.

I bilag A kan findes en skabelon for den indledende afklaring af, om der skal gennemføres en DPIA, og hvilket omfang den skal have.

Hvis man har besluttet sig for at lave en DPIA-proces, laver man en lille DPIA-projektbeskrivelse tilknyttet it-projektet, sikrer sig at alle relevante aktører giver input, får analyseret hvilke risici der kan opstå for datasubjekterne og hvilke korrigerende tiltag for beskyttelse af personoplysninger, der skal tilbydes i systemet, får dokumenteret arbejdet og slutteligt kontrolleret og revideret indsatsen.

Hvis man gennemfører sin DPIA i medfør af persondataforordningen, præciseres det i artikel 35, stk. 7 at den mindst skal omfatte:

a) en systematisk beskrivelse af de planlagte behandlingsaktiviteter og formålene med behandlingen, herunder i givet fald de legitime interesser, der forfølges af den dataansvarlige
b) en vurdering af, om behandlingsaktiviteterne er nødvendige og står i rimeligt forhold til formålene
c) en vurdering af risiciene for de registreredes rettigheder og frihedsrettigheder som omhandlet i stk. 1, og
d) de foranstaltninger, der påtænkes for at imødegå disse risici, herunder garantier, sikkerhedsforanstaltninger og mekanismer, som kan sikre beskyttelse af personoplysninger og påvise overholdelse af denne forordning, under hensyntagen til de registreredes og andre berørte personers rettigheder og legitime interesser.

Compliance

Virksomhederne skal være opmærksomme på, at behandling af personoplysninger er reguleret i persondataforordningens artikel 35 og som hovedregel skal man sikre sig at man er i compliance hermed[7]. Foruden dette er området reguleret i national lovgivning over en god del af verden. Man skal sætte sig ind i lovgivningen i de lande, man opererer i, og man bør få lavet en gennemgang af, om den måde man behandler personoplysninger på, er i overensstemmelse med lokal lovgivning. DPIA i denne vejledning sikrer ikke compliance med alverdens lovgivning! På tværs af lovgivning i forskellige lande kan man opstille en liste over principper for beskyttelse af personoplysninger, som går igen i mange landes lovgivning, og som det derfor kan være meget nyttigt at være opmærksom på på forhånd. Disse principper er gennemgået i bilag B. Overholdelse af principperne er omfattet af de spørgsmål, der stilles i de øvrige bilag til denne DPIA.

DPIA-ANALYSE

Når det er afklaret, at der er behov for at gennemføre en DPIA, tillige med hvilke dele af projektet den skal gennemføres for, skal man igang med selve analysen.

Planlægning og arkitektur

I it-projektets fase "planlægning og arkitektur" bør man lave en datalowanalyse, kortlægge datasubjektets risici og planlægge implementering af korrigerende foranstaltninger.

Dataflowanalyse

Det første, man skal give sig i kast med, er en dataflowanalyse. Dataflowanalyse er normalt en videnskabelig disciplin, der beskæftiger sig med, hvordan data flyder igennem og imellem funktioner i en applikation, med det formål at optimere applikationens performance. I denne sammenhæng har dataflowanalyse til formål at

[7] For generelt at komme i compliance med persondataforordningen kan henvises til DI's vejledning: "Persondataforordning – Implementering i danske virksomheder", http://digital.di.dk/SiteCollectionDocuments/Vejledninger/Persondataforordningen/Vejledning%20om%20persondataforordningen%20med%20bilag.pdf.

kortlægge, hvilke personoplysninger, som kommer ind i organisationen, hvordan, hvorfor, hvilken behandling der finder sted, og hvem der har adgang til personoplysningerne.

Centralt i denne forbindelse er det at tage stilling til, i hvilket omfang individet er identificeret, og graden hvormed andre faktorer kan påvirke, om individet kan identificeres. Samlet set får man følgende forhold at forholde sig til:

1. Graden af identificerbarhed (Hvordan er personoplysningerne tilknyttet identiteten?)
    a. Identificerbar
    b. Indirekte identificerbar
    c. Reversibelt pseudonym
    d. Irreversibelt pseudonym
    e. Anonym
2. Linkbarhed (Kan personoplysningerne linkes til andre oplysninger, som kan afsløre identiteten?, f.eks. en anden virtuel identitet)
3. Observerbar (Kan der observeres forhold som afslører identiteten?, f.eks. lokation og tid)

Man kan tilknytte talværdier til de tre punkter og på den måde afspejle den risiko, som man udsætter de registrerede individer for ved at behandle deres personoplysninger. Dette er især anvendeligt, hvis it-systemet kan designes på forskellig måde, hvor der kan tilknyttes forskellige værdier til designalternativerne.

Herefter skal man lave selve dataflowanalysen som bl.a. omfatter:

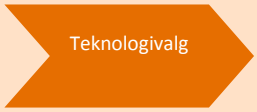
1. Hvilke personoplysninger, der indsamles
2. Hvilke kilder der er til personoplysningerne
3. Hvilket formål man har med at behandle personoplysningerne
4. Kortlægge hvilken behandling der finder sted
5. Bestemme hvem der har adgang til personoplysninger
6. Bestemme hvem der er ansvarlig for datas sikkerhed
7. Kortlægge dataflowet efter indsamlingen og i resten af datas levetid

I bilag C er listet en række spørgsmål, som følger den ovenstående proces. Det vil være en fordel, hvis man kan visualisere dataflowet.

Risici og korrigerende foranstaltninger

Behandlingen af personoplysninger kan ud fra datasubjekternes synspunkt være risikabel, fordi de kan få afsløret forhold, som de ikke ønsker at få afsløret. Man skal bemærke, at det er meget individuelt, hvilken risiko datasubjekterne tillægger behandling af personoplysninger. Køb af en roman kan være ok, men køb af koranen eller bibelen kan betragtes som risikabelt. Køb af en tv-serie kan være ok, men køb af en pornofilm kan være risikabelt. Afgivelse af personoplysninger kan være ok i en sammenhæng, men hvis de sammenstilles med personoplysninger fra en anden sammenhæng, kan det være risikabelt. I bilag D findes en oversigt over forskellige risici, set fra datasubjekternes synsvinkel.

Man kan iværksætte korrigerende foranstaltninger for at beskytte personoplysninger. For det første kan man forsøge at sikre, at informationer ikke kan henføres til en person og altså være personoplysninger, jf. nogle af eksemplerne fra bilag G. I de tilfælde, hvor det ikke er en mulighed, må man sørge for at sikre personoplysningerne bedst muligt. Bilag E giver en meget overordnet indføring i beskyttelse af personoplysninger. Som udgangspunkt anbefales det at beskytte personoplysninger under anvendelse af en sikkerhedsstandard.



I it-projektets fase "teknologivalg" bør man lave en vurdering af, om man kan beskytte nogle af personoplysninger med forskellige teknologier, således at de enten ikke længere er at definere som personoplysninger, eller således at de er maskeret. For at få inspiration til dette henvises til bilag G.

I it-projektets fase "implementering og test" skal man sikre sig, at man giver brugerne de rette informationer. Desuden skal man sikre sig, at man anonymiserer eller sletter de data, man ikke længere har brug for.

Information

Det skal overvejes i hvilket omfang datasubjekterne skal gøres opmærksom på, at virksomheden behandler personoplysninger. Herunder skal det også overvejes at sikre, at datasubjekterne har adgang til at ændre data og trække deres samtykke tilbage. I bilag F er der listet en række spørgsmål, som virksomheden bør tage stilling til.

Sletning

Virksomheden må kun behandle personoplysningerne i det omfang, de har brug for det i henhold til formålet. Virksomheden skal herefter slette data eller anonymisere dem.

Kontroller og eksternt vurdering

I it-projektets fase "drift og ændringer" skal virksomheden følge op på DPIA-analysen og indføre kontroller.

I it-projektets fase "drift og ændringer", skal virksomheden sikre sig, at der tages stilling til de tiltag, som DPIA-analysen anbefaler, bliver sat i værk. Hvis der er forhold, som virksomheden ikke ønsker at iværksætte, skal der være ledelsesopbakning til dette. De tiltag, som iværksættes, kan oplistes som kontroller, og dermed kan virksomheden løbende holde øje med, at den vedtagne beskyttelse af personoplysninger opretholdes. Tilsvarende kan virksomheden bruge kontrollerne til at vurdere, om der skal ske justeringer af beskyttelsen af personoplysninger. Kontrollerne

kan også vurderes af eksterne konsulenter, således at virksomheden kan få en uafhængig vurdering af beskyttelsen af personoplysninger. Endelig skal virksomhederne være opmærksomme på, om lovgivning ændrer sig.

BILAG A: INDLEDENDE AFKLARING AF BEHOV FOR DPIA

Organisationens navn:

_____

Projektets navn:

_____

Kort projektbeskrivelse:

_____

Projektleder:

_____

Ansvarlig for personoplysninger:

_____

Besvar nedenstående spørgsmål:

1. Behandles der personoplysninger? (Ja/Nej)
2. Kan og vil vi undgå at behandle personoplysninger? (Ja/Nej)
3. Behandler hele projektet personoplysninger? (Ja/Nej)
4. Kan der afgrænses delprojekter, som behandler personoplysninger? (Ja/Nej)
5. Er personoplysningerne anonyme i en del af projektet? (Ja/Nej)

Der skal laves en fuld DPIA, hvis der er svaret ja til spørgsmål 3 eller nej til spørgsmål 4. Hvis der er svaret nej til spørgsmål 5 kan man nøjes med en DPIA for delprojektet.

I det tilfælde, at der skal laves en DPIA, bør følgende spørgsmål kortfattet besvares/begrundes:

1. Beskriv overordnet, hvilke data der indsamles:

_____

_____

2. Beskriv overordnet, hvorfor de indsamles (formål):

_____

_____

3. Beskriv overordnet, hvem der kan få adgang til dem:

_____

_____

4. Beskriv overordnet, hvorfor det giver værdi for virksomheden at indsamle personoplysninger:

_____

_____

Dato:

_____

Udfyldt af:

_____

_____

Godkendt af projektleder (projektleders underskrift)

BILAG B: JURIDISKE PRINCIPPER

En række elementer går igen, når man læser forskellige former for regulering af behandling af personoplysninger blandt EU landene, OECD, Europarådet og APEC. Når man sammenstiller disse guidelines og love, kan man uddrage nogle principper, som det er fornuftigt at gå frem efter. Det er ikke det samme som compliance med et regelsæt! Hvis man søger at indrette sig efter disse principper, kommer man imidlertid tæt på regelsættene.

1. Man skal altid afklare om virksomheden er omfattet af den pågældende lovgivning for beskyttelse af personoplysninger
2. Man skal altid afklare, om de data virksomheden behandler, er at betragte som personoplysninger i juridisk forstand
3. Der skal altid være en juridisk person, som er ansvarlig for behandlingen, også desuagtet at selve behandlingen er outsourcet. Det skal afklares, hvem der juridisk anses for at være dataansvarlig og/eller databehandler, når man behandler personoplysninger
4. Der skal specificeres et formål med behandlingen af personoplysninger
5. Når personoplysninger er indsamlet til eet formål, må de ikke automatisk bruges til andre formål
6. Der skal altid være et retligt grundlag til at behandle personoplysninger. Som hovedregel indhentes samtykke til behandlingen af personoplysninger fra datasubjektet, om end der også i visse sammenhænge kan behandles personoplysninger uden samtykke (f.eks. som led i en kontrakt eller ud fra en interesseafvejning)
7. Behandlingen skal være nødvendig (proportional)
8. Man må kun indsamle de personoplysninger, man har brug for for at opfylde formålet (minimering)
9. Personoplysningerne skal til enhver tid være præcise
10. Der skal være åbenhed omkring indsamlingen, så datasubjektet er informeret og let kan få adgang til oplysninger og rette i oplysninger eller få opfyldt andre rettigheder
11. Der kan være særlige kategorier af data, som man som udgangspunkt ikke må behandle, f.eks. race, religion og politiske, seksuelle samt filosofiske tilhørsforhold
12. Personoplysningerne skal beskyttes efter god sikkerhedspraksis, f.eks. en sikkerhedsstandard
13. Der er som udgangspunkt skærpede krav, hvis man ønsker at videregive data til andre eller overføre dem til et andet land
14. Når data ikke længere skal anvendes i forhold til det formål, de er indsamlet, skal data anonymiseres eller slettes
15. Der skal evt. ske anmeldelse til myndigheder om behandling af personoplysninger.

For en gennemgang af reglerne i persondataforordningen henvises der til DI's vejledning: "Persondataforordningen – Implementering i danske virksomheder"[8].

[8] http://digital.di.dk/SiteCollectionDocuments/Vejledninger/Persondataforordningen/Vejledning%20om%20persondataforordningen%20med%20bilag.pdf.

BILAG C: DATAFLOWANALYSE

Organisationens navn:

_____

Projektets navn:

_____

Projektleder:

_____

Ansvarlig for personoplysninger:

_____

Besvar nedenstående spørgsmål:
(der bør ved svarene tages hensyn til graden af individernes identificerbarhed (f.eks. identificere et individ på baggrund af særlige data), linkbarhed (f.eks. linke to data sammen til den samme identitet) eller observerbarhed (f.eks. deducere sig frem til en identitet på baggrund af alle de øvrige data)

1. Hvilke personoplysninger vil blive behandlet?
   (f.eks. navn, adresse, e-mail, telefonnummer, IP-adresse, metadata, adfærd, køb eller lokation)
   _____
   _____

2. Hvilke typer af teknologier anvendes?
   (f.eks. databaser, webportaler, sociale medier, biometri, RFID eller TV-overvågning)
   _____
   _____

3. Hvordan foregår indsamlingen af personoplysninger?
   (f.eks. egne eksisterende data, data fra individ, tracking data eller data fra tredjepart)
   _____
   _____

4. Til hvilket formål behandles personoplysningerne?
   (f.eks. kreditering, udsendelse af nyhedsbrev, fremsendelse af varer eller profilering)
   _____
   _____

5. Sikres det, at der ikke indsamles flere data end formålet tilsiger?
   (begrundelse)
   _____
   _____

6. Sikres det, at data ikke anvendes til andre formål?
   (begrundelse)
   _____

_____

7. På hvilket retligt grundlag foretages databehandlingen (f.eks. samtykke)?
(beskrivelse og begrundelse)

_____

_____

8. Hvilken behandling finder sted?
(f.eks. indsamling, læsning, redigering, beregning, sammenstilling, videregivelse, opbevaring eller sletning)

_____

_____

9. Hvem har adgang til data?
(f.eks. hvilke personalegrupper, hvilke outsourcingpartnere eller individerne selv)

_____

_____

10. Hvem har ansvaret for personoplysningernes sikkerhed?
(f.eks. data- og systemejer)

_____

_____

11. Hvordan ser dataflowet ud efter personoplysninger er indsamlet?
(f.eks. kan man tegne et flowdiagram over, hvor personoplysninger lagres, hvem der kan tilgå personoplysningerne og hvordan, hvordan det sikres, at de ikke bruges til andre formål (og hvis de gør, efter hvilken procedure det så sker) og hvornår de slettes; en livscyklusbetragtning for data)

_____

_____

12. Hvordan organiseres personoplysningerne?
(f.eks. kundenummer eller nummer relateret til et andet it-system (f.eks. CPR-nummer))

_____

_____

13. Videregives data til andre?
(f.eks. andre interne systemer, eksterne it-leverandører, eksterne samarbejdspartnere eller offentliggørelse)

_____

_____

Dato:

_____

Udfyldt af:

_____

Digital

_____

Godkendt af projektleder (projektleders underskrift)

BILAG D: DATASUBJEKTETS RISICI

Organisationens navn:

_____

Projektets navn:

_____

Projektleder:

_____

Ansvarlig for personoplysninger:

_____

Besvar nedenstående spørgsmål:

1. Vedrører den behandling af personoplysninger der sker forhold, som datasubjektet kan betragte som følsomme?
   (f.eks. politik, religion, helbred, relationer, arbejdssituation, sex, økonomi, medlemskab eller lokation) (begrundelse)
   _____
   _____

2. Indgår der behandling af kreditkortoplysninger?
   (beskrivelse og begrundelse)
   _____
   _____

3. Fremtræder behandlingen af personoplysninger troværdig?
   (f.eks. virker transaktionen sikker, virker efterfølgende opbevaring af personoplysninger sikker) (beskrivelse og begrundelse)
   _____
   _____

4. Kan datasubjektet få indsigt i informationer om behandlingen af personoplysninger?
   (f.eks. formål, ret til klage, ret til at tilbagetrække samtykke) (beskrivelse og begrundelse)
   _____
   _____

5. Er der risiko for at personoplysninger spredes til en for datasubjektet kreds af uvedkommende?
   (f.eks. hacking eller tyveri fra ansatte med adgang til data) (begrundelse)
   _____
   _____

6. Er der risiko for at data bruges til andre formål end dem, de er indsamlet til?
   (begrundelse)

   _____

   _____

7. Kobles der personoplysninger fra flere kanaler om datasubjektet uden datasubjektets viden?
   (f.eks. flere selskaber i samme koncern eller data købt fra tredjeparter) (beskrivelse og begrundelse)

   _____

   _____

8. Kan der ske nogen skade på eller for datasubjektet, hvis personoplysningerne kommer til uvedkommendes kendskab?
   (f.eks. økonomiske konsekvenser, forfølgelse, stigmatisering eller indskrænket handlefrihed) (beskrivelse)

   _____

   _____

9. Kan der ske utilsigtet ændring eller tilintetgørelse af personoplysningerne?
   (begrundelse)

   _____

   _____

10. Hvor stor er den gruppe af datasubjekter, som kan blive berørt?
    (beskrivelse)

    _____

    _____

Dato:

_____

Udfyldt af:

_____

_____

Godkendt af projektleder (projektleders underskrift)

BILAG E: KORRIGERENDE FORANSTALTNINGER

Organisationens navn:

_____

Projektets navn:

_____

Projektleder:

_____

Ansvarlig for personoplysninger:

_____

Besvar nedenstående spørgsmål:
(der bør ved svarene tages højde for interne trusler, eksterne trusler (herunder leverandører) og trusler uden for virksomhedens kontrol)

1. Er der en sikkerhedsorganisation, som har til opgave at sikre personoplysningernes fortrolighed, integritet og tilgængelighed?
   (kort beskrivelse)
   _____
   _____

2. Er det obligatorisk for virksomheden at udpege en databeskyttelsesrådgiver (DPO)?
   (hvem er det i givet fald)
   _____
   _____

3. Følges en sikkerhedsstandard, som sikrer, at sikkerhedsvurderingerne kommer hele vejen rundt om organisationen?
   (f.eks. ISO27000 eller ISF) (kort beskrivelse)
   _____
   _____

4. Tager vurderingen af sikkerheden udgangspunkt i en risikovurdering?
   (kort beskrivelse)
   _____
   _____

5. Er der fysisk adgangskontrol?
   (beskrivelse)
   _____
   _____

6. Er der styring af brugeres rettigheder og adgang?
(beskrivelse)

_____

_____

7. Foretages der sikkerhedsopdateringer af styresystemer, databaser, m.v.?
(beskrivelse)

_____

_____

8. Logges adgang til personoplysninger?
(beskrivelse)

_____

_____

9. Er der adgang til personoplysninger fra bærbart udstyr?
(beskrivelse)

_____

_____

10. Kan der implementeres teknologier, som pseudonymiserer eller anonymiserer personoplysninger?
(beskrivelse og begrundelse)

_____

_____

11. Slettes eller anonymiseres data, når der ikke længere er brug for dem i henhold til formålet?
(beskrivelse)

_____

_____

12. Er der behov for at foretage anmeldelse af databehandlingen til myndighederne?
(begrundelse og evt. dokumentation)

_____

_____

Dato:

_____

Udfyldt af:

_____

_____

Godkendt af projektleder (projektleders underskrift)

BILAG F: INFORMATION

Organisationens navn:

_____

Projektets navn:

_____

Projektleder:

_____

Ansvarlig for personoplysninger:

_____

Besvar nedenstående spørgsmål:

1. Var datasubjektet orienteret før indsamlingen af personoplysninger fandt sted?
   (beskrivelse og begrundelse)
   _____
   _____

2. Er datasubjektet orienteret om formålet med behandlingen?
   (beskrivelse og begrundelse)
   _____
   _____

3. Har datasubjektet mulighed for at samtykke til eller at afvise, at data behandles?
   (beskrivelse og begrundelse)
   _____
   _____

4. Hvordan informeres datasubjekterne?
   (f.eks. e-mail, hjemmeside eller EULA) (beskrivelse)
   _____
   _____

5. Har datasubjekterne nogen grad af direkte kontrol med personoplysningerne?
   (f.eks. mulighed for at se og rette data via webadgang) (beskrivelse og begrundelse)
   _____
   _____

6. Har datasubjekterne et kontaktpunkt, som de kan henvende sig til, hvis de har spørgsmål til behandlingen af personoplysninger?
   (beskrivelse)

_____
_____

7. Er der en procedure for at datasubjekterne kan trække samtykke for behandling af personoplysninger tilbage?
(beskrivelse)
_____
_____

8. Er der en procedure for at vurdere om datasubjekterne skal orienteres, hvis deres data fortabes?
(f.eks. hvis data stjæles af en hacker) (beskrivelse)
_____
_____

9. Orienteres datasubjekterne og formål og videregivelse af personoplysninger?
(beskrivelse og begrundelse)
_____
_____

10. Orienteres datasubjektet om hvor længe personoplysninger behandles?
(beskrivelse og begrundelse)
_____
_____

11. Orienteres datasubjektet om muligheden for at klage over behandlingen?
(beskrivelse og begrundelse)
_____
_____

Dato:

_____

Udfyldt af:

_____

_____

Godkendt af projektleder (projektleders underskrift)

BILAG G: 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[9] 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

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

udenfor it-afdelingens kontrol. Denne type services kan afdække den totale mængde af it-services der anvendes i organisationen.

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 kaldet 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 i persondataforordningen ikke er personoplysninger. Det er f.eks. ikke nok alene at fjerne direkte identificerbar information som navn og adresse fra et data-sæt. 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.