God Privacy Praksis

- en guideline for IT-leverandører og kunder

Udgivet af: ITEK og Dansk Industri
Redaktion: Henning Mortensen
ISBN: xxx
0.11.06

Indholdsfortegnelse

Introduktion

I forlængelse af ITEK og Dansk Industris arbejde med informationssikkerhed har de to organisationer valgt at sætte fokus på privacy og invitere til samarbejde med en række andre interessenter om dette emne. Privacy er et emne, der får stigende betydning for anvendelsen af og tilliden til de elektroniske informationssystemer, vi anvender i dagligdagen. Især i lyset af at disse systemer anvendes i flere og flere sammenhænge og behandler information, der i stigende grad er følsom for den enkelte bruger i rollen, som borger, ansat eller virksomhed.

Formålet med dette notat er på et overordnet plan at give anbefalinger til, hvordan privacy, som udtrykt gennem en række principper, kan implementeres i elektroniske løsninger. I notatet vil de principper, der ligger til grund for privacy blive præsenteret, og der vil blive oplistet en række spørgsmål, som skal guide produktudviklere, serviceleverandører og professionelle kunder til at få privacy indarbejdet i deres it-løsninger. Det er hensigten, at spørgsmålene skal udgøre en "Praksis" for arbejdet med privacy.

Denne ”Praksis” er udarbejdet af ITEK og Dansk Industri i samarbejde med IT-sikkerhedspanelet under ministeriet for Videnskab, Teknologi og Udvikling, Finansrådet, Institut for Menneskerettigheder, Digital Rights, Forsvarets Forskningstjeneste, AIM Danmark, TDC A/S, Siemens A/S, Microsoft Danmark A/S, Nensome ApS, Zebranet ApS, IBM Danmark A/S, LOGISYS A/S, Parkegaard og Kristensen Sikkerhed ApS, RFIDsec ApS og CSIS A/S og med tilslutning fra Forbrugerrådet.

Baggrund

ITEK og Dansk Industri har i flere andre publikationer beskæftiget sig med privacy. I notatet: ”Principper for privacy”[1] forsøges privacy defineret og de forskellige principper for privacy, der findes i lovgivning og konventioner identificeres. I notatet ”Privacy fremmende teknologier” beskrives, hvad den enkelte bruger eller den lille virksomhed aktuelt kan gøre for at beskytte sin egen privacy. I dette notat vil vi se på hvordan man i praksis kan sikre at privacy er tilvejebragt i elektroniske løsninger.

Privacy er et begreb, som det er vanskeligt at definere. Ordet er blevet forsøgt defineret i mange forskellige sammenhænge. Dette viser på den ene side begrebets brede betydning og vigtighed, men det har også på den anden side bidraget til at udvande ordet.

Der sondres ofte mellem fire typer privacy[2]:

---

[1] ”Principper for privacy”, ISBN: 87-7353-602-4, kan findes på ITEKs hjemmeside. Notatet er udarbejdet af ITEK og Dansk Industri med støtte fra Forbrugerrådet, Finansrådet, Institut for Menneskerettigheder, Digital Rights, AIM Danmark, TDC A/S, Siemens A/S, Microsoft Danmark A/S, Nensome ApS, Zebranet ApS, LOGISYS A/S, Parkegaard og Kristensen Sikkerhed ApS, RFIDsec ApS og CSIS ApS.

[2] Privacy & Human Rights, udgivet af EPIC, 2003, p. 3. EPIC står for Electronic Privacy Information Center, og er formodentlig USA's mest indflydelsesrige privacyorganisation.

- Informationsprivacy, som vedrører indsamlingen og behandlingen af personlig information - også kaldet databeskyttelse
- Kropslig privacy, som vedrører retten til at beskytte sin fysiske krop mod f.eks. genetiske tests
- Kommunikationsprivacy, som vedrører sikkerhed og privacy i forhold til breve, mail, telefonopkald, internetanvendelse og lignende
- Territorial privacy, som vedrører grænsedragningen mellem det private miljø og andre miljøer f.eks. på arbejdspladsen og i det offentlige rum - herunder f.eks. videoovervågning og ID tjek.

Vi fokuserer i denne Praksis fortrinsvis på informations- og kommunikationsprivacy.

Vi kan imidlertid komme privacy begrebet lidt nærmere. Den ældste henvisning til privacy findes hos den senere amerikanske højesteretsdommer, Louis Brandeis, som i slutningen af 1800-tallet beskrev det som ”the right to be let alone”[3].

EPIC mener, at der som minimum er internationale konsensus om, at privacy vedrører retten til at indsamle, vedligeholde, anvende, videregive/transmittere og behandle personlig information[4].

Den engelske tænketank, DEMOS, som forsker i demokrati og demokratiske principper, har en definition, som inkluderer psykologiske aspekteraf privacy med fokus på risiko: "Privacy can best be understood as a protection against certain kinds of risks - risks of injustice through such things as unfair inference, risks of loss of control over personal information, and risks of indignity through exposure and embarrassment"[5].

Også forskellige standarder beskæftiger sig med privacy. I Common Criteria, som er en standard til at vurdere om et stykke software opfylder en række sikkerhedskrav, hedder det: Privacy ”requirements provide a user protection against discovery and misuse of identity by other users”[6].

De ovenstående eksempler viser, at privacy er mange ting og kan forstås på mange måder, og vi vil ikke lave en entydig definition. Blot vil vi konkludere, at privacy vedrører det mulige tab af personlig integritet og de deraf følgende konsekvenser. For en yderligere uddybelse henvises der til ”Principper for privacy”.

Fordi begrebet privacy ikke er præcist defineret, kan man tale om flere grader af privacy. Disse nuancer fremgår af nedenstående figur 1.

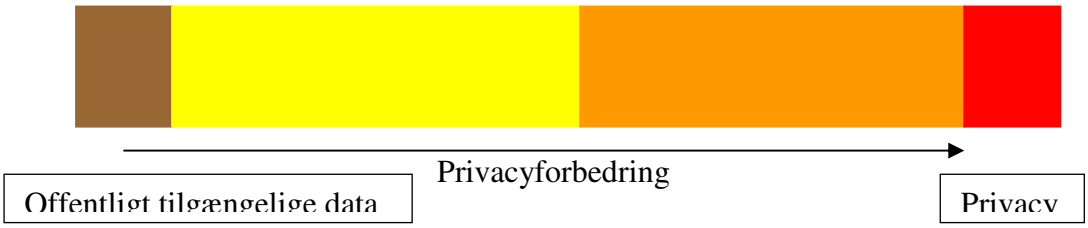
---

[3] Samuel Warren and Louis Bradeis, The Right to privacy, 4 Harvard Law review, 193-220 (1890), http://www.louisville.edu/library/law/brandeis/privacy.html.

[4] http://www.epic.org/reports/dmfprivacy.html.

[5] http://www.demos.co.uk/catalogue/thefutureofprivacyvolume1.

[6] Common Criteria er en ISO-standard ved navn: ISO/IEC 15408:2005, og den kan i sin fulde længde findes på http://www.commoncriteriaportal.org. Privacy-kravene fremføres i standardens 2. del: ”Security functional requirements”, http://www.commoncriteriaportal.org/public/files/ccpart2v2.3.pdf.



Figur 1: En model for de forskellige nuancer af privacy.

I figurens to ekstrema har vi henholdsvis at gøre med offentligt tilgængelige data (venstre side) kontra den situation, hvor kun brugeren har adgang til egne personhenførbare data (højre side). I det mellemliggende område vil data være tilgængelige for en snævrere og snævrere kreds, efterhånden som vi bevæger os fra venstre mod højre. Den manglende enighed om en definition på privacy betyder i forhold til figuren at der ikke er enighed om hvorvidt privacy skal betragtes alene som et ekstremum eller placeres længere til venstre i figuren. I den konkrete sammenhæng vælger vi derfor at tale om priacyforbedringer efterhånden som vi bevæger os fra venstre mod højre i figuren uden at forholde os til om privacy rent definitorisk eventuelt måtte opnås inden vi når det højre ekstremum.

Der vil være en hel række metoder man kan opnå privacyforbedringer med - f.eks. lovgivning, tekniske foranstaltninger og personlig adfærd. Gennem hvert enkelt privacyforbedring bevæger man sig mod højre i figuren. Hvor man vil eller kan placere sig i en given situation er også afhængig af en række faktorer - f.eks. hvad man må eller skal lovgivningsmæssigt, hvilke præferencer man har, hvilken situation man er i, og hvad man har af tekniske muligheder. Det skal dog bemærkes, at har man først bevæget sig langt til venstre i figuren og selv eller af andre fået offentliggjort data om sig selv, kan det ikke omgøres.

I det brune område er alle data offentligt tilgængelige. Tilblivelsen af dette scenario kan ske ved at området ikke er omfattet af regulering eller at loven specificerer at alle data altid skal være tilgængelige. Et eksempel, hvor dette finder sted, er i Sverige, hvor oplysninger om indkomst og betaling af skat ikke anses som et privat anliggende og disse oplysninger er dermed offentligt tilgængelige.

I det gule område har brugeren ikke kontrol med sin identitet og sine data i betydningen at databehandleren kan bruge disse inden for lovgivningens rammer og måske inden for visse tekniske foranstaltninger. Brugeren er nødt til at afgive data, der er personhenførbare. Det kan f.eks. være, at brugeren er nødt til at angive sit navn, adresse, IP-adresse, mailadresse eller andet for at få adgang til det, han gerne vil. Afgivelse af disse oplysninger betyder ikke nødvendigvis, at brugeren er identificeret. Men ved at kombinere flere af denne type informationer kan man ret hurtigt finde ud af, hvem brugeren er. For at forbedre privacy for brugeren opstiller loven visse rammer for anvendelsen af data og desuden kan visse teknologier stille brugeren bedre ved at reducere sandsynligheden for at der finder misbrug sted. I det gule område har vi således lovgivningen og visse tekniske foranstaltninger som privacyforbedrende midler. Vi vil beskæftige os med det gule område i afsnittet: ”Praksis”.

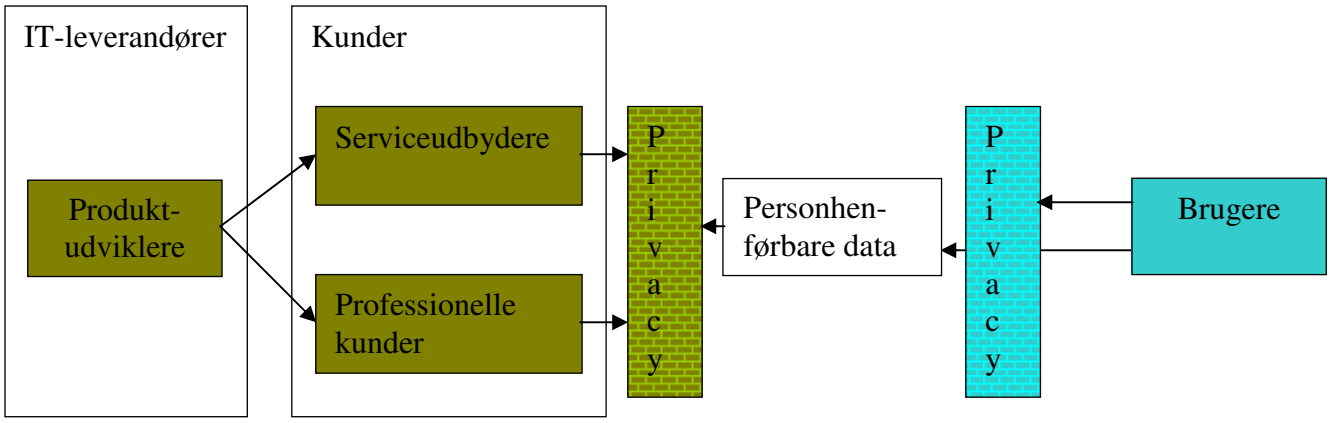
I det orange område kan man gennem en række bestemte teknologier sikre, at brugeren kan agere som unikt individ og afgive profildata uden at identificerende eller personhenførbare data bliver tilgængelige for andre end brugeren. Det betyder, at brugeren har kontrol med sin identitet og selv kan styre hvem, der får adgang til hvilke oplysninger, hvornår og hvor længe. Brugeren bestemmer dermed selv om han vil identificere sig (og dermed gøre sine oplysninger personhenførbare) eller ej

(og anvende et pseudonym). F.eks. kan brugeren købe en vare, uden at sælgeren ved, hvem brugeren er. Brugeren kan også få adgang til en offentlig service, uden at det offentlige ved, hvem det er, der har benyttet sig af den. Dette sker ved at brugeren hos en serviceudbyder (eller gennem en serie af serviceudbydere) laver en formålsspecifik nøgle eller et pseudonym. Sælgeren eller det offentlige får så kendskab til pseudonymet, men får ikke kendskab til identiteten bag pseudonymet.Sælgeren kan dermed dele alle data og samarbejde med underleverandører og partnere uden risiko for misbrug eller kriminalitet. Såfremt sælgeren eller det offentlige får mistanke om, at brugeren har begået noget kriminelt, eller noget der i øvrigt ikke er ønskværdigt, kan de dog med loven i hånden under på forhånd fastlagte vilkår skaffe sig adgang til brugerens identitet ved at pseudonymet eller serien af pseudonymer gennemløbes. Borgeren er altså ansvarlig for handlinger men har alligevel under normale forhold relativ stærk privacy inkl. muligheden for at opretholde kontrol med historiske data. Vi vil beskæftige os med det orange område i afsnittet ”Brugernes kontrol med egne identiteter”.

De teknologier, som giver privacyforbedringer i det orange område kalder vi med en fælles betegnelse for Privacy Enhancing Technologies, PET, eller Trust Enhancing Technologies, fordi risikoen reduceres for alle parter. Teknologier, der giver privacy forbedringer i det gule område kaldes Privacy Friendly Technologies eller Compliance Technologies. Det er meget vigtigt at pointere at de teknologier, der anvendes i de to områder er væsentligt forskellige. I det orange område giver teknologierne brugeren mulighed for, at han kan kontrollere sin identitet og sine data. I det gule område reducerer teknologierne alene muligheden for at data kan misbruges af databehandleren.

I det røde område har man absolut privacy i den betydning, at hver enkelt bruger har anonymitet. Det betyder, at brugeren kan være fuldstændig sikker på, at ingen af de oplysninger han eventuelt måtte afgive, på nogen måde vil kunne gøre, at han kan identificeres. Det indebærer at han er helt uden risiko for misbrug fra andre men også at han vil kunne holde sig helt skjult og udføre de handlinger han har lyst til uden ansvar overfor andre.

Som nævnt vil vi i denne "Praksis" give anbefalinger til, hvordan man kan forbedre privacy og især den del af privacy, der ligger i det gule område i figur 1. Der er altså en "Praksis" i at komme på højde med de principper for privacy, som er almindeligt anerkendt. At forbedre privacy kræver en samspil mellem en række aktører, som skitseret nedenfor i figur 2.



Figur 2: Samspil mellem aktører giver privacyforbedringer.

Brugernes muligheder for at forbedre deres egen privacy er skitseret i notatet: "Privacy fremmende teknologier". Hvad, der derfor står tilbage, er, at give IT-leverandørerne og de professionelle kunder et redskab til at efterleve de principper for privacy, som er identificeret i det øvrige arbejde. Gennem deres forskellige indsats og de principper de følger, deres adfærd og de foranstaltninger de implementerer får vi bygget en mur af privacy omkring de personhenførbare data.

Vi vil definere to hovedgrupper, der har hver deres ansvar for at sikre brugernes privacy.

For det første har vi IT-leverandørerne, der her skal forstås som virksomheder, der fremstiller software eller leverer konsulentydelser indenfor IT.

For det andet har vi kunderne til disse løsninger. Denne kundegruppe kan inddeles i to undergrupper.

Dels de virksomheder, der er udbydere (til andre kunder) af IT-services og tekniske og forretningsmæssige tjenester som f.eks. indholdstjenester, programmer til computere og e-handel.

Dels de professionelle kunder, som indkøber løsninger, der skal anvendes til formål, hvor der behandles personlige oplysninger. Eksempler på disse kunder er f.eks. virksomheder og det offentlige, som bruger systemerne til administrative forhold som sagsbehandling, lønudbetaling, HR-aktiviteter og meget andet.

Såvel IT-leverandørerne som de to kundegrupper bør sikre, at de systemer, de anvender, kan efterleve basale privacy anbefalinger, som skitseret i denne "Praksis". Kunderne bør ligeledes sikre, at procedurer og processer, som anvendes i dagligdagen, ikke udvander den privacy, som er tilvejebragt i systemerne.

Principper for privacy

På baggrund af det arbejde med privacy, som er foretaget af OECD[7], Europarådet[8] samt EU[9], og som også afspejles i den danske Lov om behandling af personoplysninger (persondataloven)[10], kan vi opstille en række principper, som ligger til grund for privacy. Da principperne tager udgangspunkt i tekster, som er tiltrådt af Danmark og som direkte er blevet implementeres i dansk lovgivning, må de siges at være juridisk bindende. På baggrund af disse principper kan vi så give en række anbefalinger, som IT-leverandørerne og professionelle kunder bør tage højde for, når de arbejder med privacy i produkter og services. Man kan sige, at hvert enkelt princip er en byggeklods for privacy, og at byggeklodserne tilsammen udgør en privacy mur, som skal beskytte brugernes privacy.

Muren bliver hullet, hvis principperne ikke efterleves af leverandører og kunder. Desuden er der i principperne med vilje indbygget en række undtagelsesbestemmelser, som ligeledes udgør huller i muren. Undtagelserne er dog en del af principperne for privacy, fordi disse principper ofte vægtes

---

[7] "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

[8] "Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data Convention", http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

[9] "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data", http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DA:HTML.

[10] http://www.folketinget.dk/Samling/19991/lovforslag_som_fremsat/L147.htm.

mod andre behov og regler - f.eks. kriminalitetsbekæmpelse, omkostninger og bekvemmelighed. Afhængigt af hvordan man anskuer det, kan indgrebet i privacy dermed være regelbundet. En sådan afvejning danner et hul i privacy og bør derfor foretages med yderste forsigtighed. Yderligere er muren mest en gennemgang af de retslige principper for privacy. Andre principper, som er mere teknologiske, psykologiske, sociale og økonomiske er ikke nødvendigvis inkluderet – selv om disse jo gerne skulle ligge bag det retslige grundlag. Endelig vil muren være hullet, hvis brugeren handler uansvarligt, ikke selv sikrer, at de programmer, der anvendes, er opdaterede, ikke har slået privacy beskyttende funktioner til eller lignende, således at personer med ondsindede hensigter kan tilegne sig personhenførbare oplysninger fra eller om brugeren.

Principperne er som nævnt identificeret og gennemgået i detaljer i notatet ”Principper for privacy”. I denne ”Praksis” forudsættes de kendt fra notatet, og de er derfor kun oplistet her fordelt på hovedkategorier. Nedenstående figur skal alene fortolkes som byggeklodser! Der er ikke nogen indbyrdes systematik mellem de angivne klodser.

Principperne i nedenstående figur 3, svarer til muren fra figur 2 og man vil befinde sig i det gule område i figur 1. Hvis man har implementeret teknologier, som betyder at man befinder sig i det orange område i figur 1, er nedenstående principper af begrænset betydning. Men de vil alligevel være hensigtsmæssige at efterleve (ud over at de skal efterleves i det omfang der er tale om lovgivning) for i størst mulige omfang at beskytte de personlige data om en bruger i det tilfælde pseudonymet ophæves. Som det fremgår af nedenstående principper bør både data og processer vurderes ud fra denne "Praksis".

Brugerne skal kunne styre anvendelsen af data (3)

Dataindsamlingen skal være fair

Dataindsamlingen skal være lovlig

Dataindsamling skal ske med viden fra brugeren

Dataindsamling skal ske med accept fra brugeren

Dataindsamling kan være krævet af en kontrakt, loven, hensyn til brugeren og offentlig myndighedsudøvelse (3)

Dataindsamling kræver konkret afgrænset formål

Databehandling må kun finde sted til det formål de er indsamlet

Ved ændret formål skal data destrueres eller anonymiseres

Databehandlerens eventuelle videregivelse af data kræver at brugeren oplyses herom (og giver accept)

Data skal have god kvalitet i betydningen præcise, komplette og opdaterede

Brugeren har altid ret til at få adgang til egne data

Brugeren har altid ret at få indsigt i om en enhed har registreret data og i givet fald hvilke, deres anvendelse, formålet med at have dem og hvor de lagres

Databehandleren skal give indsigt til brugeren på en forståelig måde, indenfor en rimelig tid og til en rimelig pris

Databehandler skal udvise åbenhed overfor brugerens indsigt

Databehandler kan anvende betingelser for brugerens indsigt og i givet fald skal disse begrundes

Brugeren har ret til retslig prøvelse af sammenhæng mellem data og formål, datas kvalitet og eventuel manglende efterlevelse af privacypolitikker (1)

Brugeren har kun ret til indsigt med begrænset frekvens (1)

Databehandler har ansvar for data og disses sikkerhed

Dataflow over grænser er betinget til international handel, anvendelse af elektroniske services og dataflow internt i virksomheder. Dette bør reguleres gennem kontrakter

Databehandler skal sikre at privacyforanstaltninger implementeres under hensyn til det tekniske niveau (2)

Databehandler skal sikre at privacyforanstaltninger implementeres under hensyn til omkostninger (2)

Databehandler skal sikre at der findes en opdateret politik for privacy

Databehandler skal sikre at brugeren med rimelighed er bekendt med politikken og har accepteret den

Databehandler skal anmelde behandling af data til tilsynsmyndighed

De nævnte principper gælder ikke hvis der er særlige nationale interesser, der varetages bedre ved en undtagelse (3)

De nævnte principper gælder ikke hvis der er tale om behandling af kriminelle forhold (3)

De nævnte principper gælder ikke hvis det vurderes at være i brugerens interesse at undtage dem eller hvis det gælder andre personers frihed (3)

De nævnte principper gælder ikke hvis for særlige faggrupper – herunder anvendelse til historisk, journalistisk, videnskabeligt eller statistisk bearbejdelse (3)

De nævnte principper gælder ikke hvis behandling af data sker ved arbejdsmarkeds-forhold, foreninger, allerede offentliggjorte data, sygdomme og særlig lovgivning (3)

Databehandlers videre beskyttelse end de angivne principper er altid mulig

De angivne principper er overordnede og der kan der ske en gradbøjning af dataanvendelse (3)

De angivne principper er overordnede og der kan der ske en gradbøjning af foranstaltninger (3)

De angivne principper er overordnede og der kan der ske en gradbøjning af risici, som data kan udsættes for (3)

Figur 3: Principper for privacy.

Det blå område er princippernes udgangspunkt og baggrunden for de regler og teknologiske løsninger, der ligger på området. Det blå område efterleves ved enten at efterleve de øvrige principper eller ved at implementere teknologier omtalt i afsnittet: ”Brugernes kontrol med egne identiteter”. Det lilla område vedrører dataindsamling og -behandling. Det grønne område viser de rettigheder brugeren har i forhold til data, der allerede er indsamlet. Brugerens rettigheder er nøje sammenkædet med de øvrige principper idet stort set alle principperne kan vendes eller drejes således, at de bliver til en brugerrettighed, som brugeren har krav på at få efterlevet. Databehandlerens forpligtelser er angivet med pink. Og endelig er undtagelserne fra de enkelte principper angivet med hvidt.

Undtagelserne har alle fået et nummer. Nummeret angiver hvilket princip de er undtagelse fra.

Vi har nedenfor ikke anvendt den definition af databehandler, som fremgår af persondataloven. Databehandler er i denne sammenhæng den, som både indsamler, behandler og har ansvaret for lagring af data.

Praksis

For at lave en ”Praksis” for IT-leverandører og kunder er det nødvendigt at skrive alle disse principper om således, at de alene angiver anbefalinger til databehandleren, som i vores terminologi er kunden, i og med at det er dem, der udbyder services og behandler data i administrative systemer. Anbefalingerne til databehandleren, skal IT-leverandøren og kunderne så sammen sikre er efterlevet, således at brugerens privacy er beskyttet. Dermed får IT-leverandørerne og kunderne hver især et ansvar i processen. Men det endelige juridiske ansvar har databehandleren.

IT-leverandøren har som ansvar at sikre, at kunden får sine ønsker - herunder ønsker til privacyforanstaltninger - opfyldt, og at de er i stand til at levere et system, der implementerer dette. Kunden har et ansvar for at sikre, at systemet efterlever principperne. IT-leverandøren tilbyder således privacy funktionalitet til kunden, men det er kunden der vælger, om og hvordan funktionaliteten overfor brugeren skal udformes. Privacybeskyttelsen er derfor valgfri, men bør som standard været slået til. I det omfang at kunden blot specificerer af systemet skal efterleve principperne er det leverandørens ansvar at finde ud af, hvordan det kan gøres mest hensigtsmæssigt. IT-leverandøren bør også gøre kunden opmærksom på at principperne bør efterleves, hvis kunden ikke selv er opmærksom på dette.

IT-leverandøren kan ikke tvinge kunden til at efterleve principperne. Hvis kunden ikke vægter fokus på privacy og overholdelse af lovgivningen i sin løsning, kan leverandøren, som jo er i konkurrence med andre leverandører, ikke bygge efterlevelse af privacy principperne ind i sit tilbud.

På denne måde er begge de to grupper, som vi skitserede i indledningen, omfattet af denne ”Praksis” idet de hver især har en rolle at spille i at forbedre privacy.

Det skal bemærkes, at de undtagelser, der er nævnt ovenfor, som regel behandles sammen med det princip, de er undtagelser fra. I nedenstående gennemgang er der derfor færre principper end i ovenstående figur 3[11].

[11] Det skal også bemærkes at spørgsmålene til de enkelte principper skal ses som en indledende øvelse, der sagtens kan udbygges ved f.eks. at anvende Datatilsynets vejledning til sikkerhedsbekendtgørelsen eller andre vejledninger og udtalelser, http://www.datatilsynet.dk/lovgivning/indhold.asp. Man kan også tage udgangspunkt i de

- **Brugerne skal kunne styre anvendelsen af egne data**
  Det vigtigste overordnede princip er, at brugerne skal kunne styre anvendelsen af egne data. Hvis dette ikke var udgangspunktet, var der ikke noget grundlag for at lave en lov om beskyttelse af brugernes data. Ideelt set skulle loven og foranstaltningerne gerne bringe data op i det orange område i figur 1. Imidlertid er det kun få løsninger, der kan tilvejebringe den pågældende pseudonymisering af brugeren som skal til for at give brugeren kan styre anvendelsen af data og derfor bevæger loven og de fleste teknologier sig rundt i det gule område, hvor det handler om at sikre data så man kommer længst muligt til højre i figuren. Konkret betyder det, at databehandleren skal sikre, at IT-systemerne er indrettes således, at systemerne alene indsamler de relevante data og at brugerne kan få kontrol med de data, de afgiver om sig selv. Dette kan ske enten gennem direkte interaktion med IT-systemet eller gennem kontakt til databehandleren, som så kan viderebringe oplysningerne til brugeren. Hvad der forstås med brugerens styring af anvendelse af data, er skitseret i de øvrige principper i denne "Praksis".

  Der er en række undtagelser fra princippet om brugerens kontrol med egne data. Disse undtagelser falder i to kategorier: Der er de undtagelser som er vedtaget politisk og vedrører forhold, hvor der må tages særlige hensyn. Der er f.eks. tale om særlige nationale interesser, behandling af kriminelle forhold, forhold hvor det vurderes at være i brugerens interesse at undtage dem, situationer hvor andre personers frihed berøres, særlige faggruppers arbejde (historisk, journalistisk, videnskabeligt eller statistisk bearbejdelse) og endelig arbejdsmarkedsforhold, foreninger, allerede offentliggjorte data, sygdomme og særlig lovgivning Desuden er der undtagelser som er af mere frivillig eller ufrivillig tilfældig karakter og som vedrører gradbøjning af dataanvendelse, gradbøjning af beskyttelsesforanstaltninger og risici, som data kan udsættes for.

---

praksisser som anvendes af store private udviklere – se f.eks. http://www.microsoft.com/downloads/details.aspx?FamilyID=c48cf80f-6e87-48f5-83ec-a18d1ad2fc1f&displaylang=en.

Leverandør	Kunde/databehandler
Foretages der en overordnet analyse af privacybehovene i det konkrete system?[12] Er der allokeret et ansvar for at sikre den fornødne privacy i systemet? Findes der i systemet muligheder for at der kan genereres et overblik over alle registreringer om hver enkelt bruger, således at brugeren let kan få kontrol med data? Tager systemet hensyn til de politisk fastsatte undtagelser? Sker der test af de mere tilfældige undtagelser ikke er af graverende karakter? Foretages der opfølgning i forhold til ændringer i systemer og politikker?	Foretages der en overordnet analyse af privacybehovene i det konkrete system? Er der allokeret et ansvar for at sikre den fornødne privacy i systemet? Kan systemet generere en rapport over alle registreringer om alle brugere? Er der er processer, som kan håndtere henvendelser fra brugerne om udlevering af data? Findes der retningslinier for udlevering af personhenførbare data? Tager systemet hensyn til de politisk fastsatte undtagelser? Sker der kontrol af de mere tilfældige undtagelser ikke er af graverende karakter? Foretages der opfølgning i forhold til ændringer i systemer og politikker?

- **Dataindsamlingen skal være fair**
  En fair indsamling af data betyder at de øvrige principper i denne "Praksis" skal overholdes ved indsamlingen af data. Brugeren må ikke kunne snydes til at afgive data og der må ikke afgives flere data end nødvendigt for formålet. Processen skal således være fair og gennemskuelig overfor brugeren.

Leverandør	Kunde/databehandler
Er formålet med dataindsamlingen tydeligt specificeret? Er løsningen designet så brugeren kun afgiver de nødvendige oplysninger eller indsamles unødvendige oplysninger i den pågældende løsning? Er der gennemført brugervenlighedsanalyser, som sikrer, at systemet virker gennemskueligt for brugeren, så brugeren ikke føler sin privacy krænket?	Er formålet med dataindsamlingen tydeligt specificeret? Kan systemet siges kun at indsamle de oplysninger, der er brug for? Er der dokumentation for at de oplysninger der indsamles er relevante? Kan brugeren føle sig snydt til at afgive informationer eller til at få bestemte services - f.eks. elektroniske nyhedsbreve?

- **Dataindsamlingen skal være lovlig**
  Dataindsamlingen skal efterleve bestemmelserne i Lov om behandling af personoplysninger samt andre love der eventuelt måtte være relevant i en konkret situation. Databehandleren skal sikre at systemer og processer er i overensstemmelse med loven.

Leverandør	Kunde/databehandler

[12] Der kan foretages en Privacy Impact Assessment, PIA. Dette dokument kan ses som en introduktion til emnet. Men der kan også henvises til andre meget omfattende metodikker – se f.eks. det canadiske datatilsyns metodik her: http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/siglist_e.asp.

Hvordan er de kontraktlige forpligtelser mellem leverandør og kunde i forhold til overholdelse af loven? Kan leverandøren underskrive en erklæring om at det er sikkert at systemet overholder lovens krav eller vil dette være for usikkert for leverandøren? Sikres det at personlige data ikke linkes sammen ved hjælp af personnummer?	Er lovens overholdt, så brugere ikke kan rejse sager og føler sig trygge? Findes der i eller i tilknytning til virksomheden personer, som kan vejlede om ændringer i lovgivningen, der kan få konsekvenser for systemernes virkemåde?

- **Dataindsamling skal ske med viden fra brugeren**
  Databehandleren skal med rimelighed kunne sandsynliggøre, at brugeren er bekendt med, at indsamling af data finder sted. Dette gælder uanset om, der er tale om en manuel eller automatiseret indsamling. Såfremt indsamling finder sted løbende over længere tid, vil det være rimeligt om brugeren med jævne mellemrum informeres om at indsamling fortsat finder sted.

Leverandør	**Kunde/databehandler**
Hvordan informerer systemet brugerne om, at der indsamles oplysninger om dem? Sikres det at brugeren, som afgiver data, har givet tilsagn? Logges det (enten automatisk eller manuelt), hvordan og hvornår brugeren har givet udtryk for at han er i besiddelse af denne viden om, at indsamling finder sted? Erindres brugerne med faste intervaller om, at der fortsat indsamles oplysninger om dem?	Hvordan informerer systemet brugerne om, at der indsamles oplysninger om dem? Sikres det at brugeren, som afgiver data, har givet tilsagn? Hvilken viden om indsamlingen og behandlingen giver systemet brugerne? Kan systemet dokumentere, at brugerne er bekendt med, at der indsamles og behandles oplysninger om dem?

- **Dataindsamling skal ske med accept fra brugeren dog med den undtagelse at det kan være krævet af en kontrakt, loven, hensyn til brugeren og offentlig myndighedsudøvelse**
  Brugeren skal have givet accept til databehandleren om at indsamling af data må påbegyndes. Accepten kan gives elektronisk f.eks. ved udfyldelse af en online form. Databehandleren skal gemme bevis for metoden for og tidspunktet hvor accepten er givet. Tillige med dokumentation for de omstændigheder under hvilke tilsagnet blev givet.

Leverandør	**Kunde/databehandler**
Registreres det hvis indsamlingen sker som følge af kontraktlige forhold, loven, hensyn til brugeren eller offentlig myndighedsudøvelse? Logges det (enten automatisk eller manuelt), hvordan og hvornår brugeren har givet tilsagn om at indsamling finder sted? Kan systemet håndtere at en bruger trækker sit tilsagn tilbage?	Viser systemet om indsamlingen sker som følge af en frivillig aftale med forbrugeren eller som følge af kontraktlige forhold, loven, hensyn til brugeren eller offentlig myndighedsudøvelse? Kan systemet bevise at brugeren har givet tilsagn om at indsamling og behandling må findes sted? Er der betingelser (ud over formål) (f.eks.

	tidshorisont) tilknyttet indsamlingen og behandlingen af data? Er der procedurer (tekniske såvel som forretningsmæssige) som sikrer at brugeren kan trække et tilsagn tilbage?

- **Dataindsamling kræver konkret afgrænset formål**
  Databehandleren må kun indsamle personhenførbare data til et på forhånd konkret og tydeligt afgrænset og specificeret formål, hvorfor det skal sikres, at et sådant findes. Det skal sikres, at brugeren er bekendt med det pågældende formål og har accepteret, at det er til dette formål de personhenførbare data afgives.

Leverandør	Kunde/databehandler
Sikrer systemet at der kun indsamles data i overensstemmelse med det skitserede formål?	Er indsamling af data begrænset til kun at kunne foregå indenfor et afgrænset formål? Er der processer, der sikrer løbende vurdering af hvilke formål der er relevante?

- **Databehandling må kun finde sted til det formål data er indsamlet**
  Databehandleren må kun indsamle personhenførbare data til et på forhånd konkret og tydeligt afgrænset og specificeret formål, hvorfor det skal sikres, at et sådant findes.

Leverandør	Kunde/databehandler
Sikrer systemet at der kun behandles data i overensstemmelse med det skitserede formål?	Er behandling af data begrænset til kun at kunne foregå indenfor et afgrænset formål? Kan behandling kun finde sted af personer, der har tilknytning til et givent formål? Er der processer, der sikrer løbende vurdering af hvor længe et givent formål stadig er relevant?

- **Ved ændret formål skal data destrueres eller anonymiseres**
  Databehandleren skal sikre, at data, der er indsamlet til et bestemt formål, destrueres eller anonymiseres, hvis formålet ikke længere er relevant eller ændres i en sådan grad, at det må vurderes at være et andet formål end det, der oprindeligt gav anledning til indsamlingen.

Leverandør	Kunde/databehandler
Sikrer systemet at grupper af data kan slettes eller anonymiseres? Er der indbygget funktionalitet, som løbende overvågner om der findes data, der ikke er blevet "behandlet" i en længere periode?	Er der processer og/eller tekniske foranstaltninger, som sikrer at data, der ikke længere er i overensstemmelse med et gyldigt formål, slettes eller anonymiseres?

- **Databehandlerens eventuelle videregivelse af data kræver at brugeren oplyses herom (og giver accept)**
  Databehandler kan ikke vilkårligt videregive data, der er indsamlet til et bestemt formål. Såfremt data videregives til tredjeparter, skal det - i det omfang de fortsat er

personhenførbare - ske med tilsagn fra brugeren. Såfremt data er anonymiseret - og dermed ikke længere personhenførbare - kan data videregives.

Leverandør	Kunde/databehandler
Sikrer systemet at grupper af data kan slettes eller anonymiseres? Sikrer systemet at der ikke kan ske automatiske "store" udtræk og videregivelse uden nødvendig autorisation? Sker videregivelse af data til udlandet?	Findes der retningslinier for, hvornår data kan videregives? Er der rutiner for indhentelse af fornyet tilsagn fra bruger såfremt der er behov for at ændre formålet? Sker videregivelse af data til udlandet?

- **Data skal have god kvalitet i betydningen at data er præcise, komplette og opdaterede**
  Data skal altid have god kvalitet, således at de afspejler, den bruger, som de giver sig ud for, på retvisende måde. Databehandleren har i mange sammenhænge en selvstændig interesse heri - f.eks. hvis data bruges til at udskrive regninger eller hvis data bruges til statistiske formål. Data må således ikke være fejlbehæftede eller give et billede af brugeren, som fordrejer sandheden.

Leverandør	Kunde/databehandler
Sikrer systemet at data er kan opdateres evt. med logning af hvem, hvornår og hvorfor data ændres? Er der lavet automatiseret validering af data præcision i det omfang det er muligt (f.eks. for at undgå tastefejl)? Registreres det hvornår og af hvem data ændres?	Findes der procedurer, som sikrer, at data til stadighed er præcise og opdaterede?

- **Brugeren har altid ret til at få adgang til egne data**
  Brugeren skal altid have ret til at få at vide hvilke kategorier af data, databehandler har registreret om ham og desuden kunne få indblik i de registrerede data. En undtagelse herfra er dog implementeret i den danske persondatalov, således at en bruger kun kan anmode om data hver 6. måned.

Leverandør	Kunde/databehandler
Kan systemet oplyse (enten ved brugerens egen interaktion eller gennem henvendelse til databehandler) hvilke data, der er registreret om en bruger?	Er der procedurer for håndtering af brugerhenvendelser om hvilke oplysninger, der er registreret om brugeren? Kan der fra systemerne genereres en oversigt over de data, databehandler han registreret om brugeren?

- **Brugeren har altid ret at få indsigt i om en enhed har registreret data og i givet fald hvilke, deres anvendelse, formålet med at have dem og hvor de lagres**
  Databehandleren skal sikre at brugeren kan få adgang til de data der er registreret om ham tillige med en række andre oplysninger der vedrører data - herunder hvad data anvendes til, til hvilket formål data er registreret og hvor de lagres.

Leverandør	Kunde/databehandler
Kan systemet afgive data alle data om en konkret bruger tillige med en række oplysninger i tilknytning til data - herunder hvad data anvendes til, til hvilket formål data er registreret og hvor de lagres?	Er der en politik for hvilke supplerende oplysninger, der udleveres i forbindelse med udlevering af data? Kan systemet afgive data alle data om en konkret bruger tillige med en række oplysninger i tilknytning til data - herunder hvad data anvendes til, til hvilket formål data er registreret og hvor de lagres?

- **Databehandleren skal give indsigt til brugeren på en forståelig måde, indenfor en rimelig tid og til en rimelig pris**
  Databehandleren skal udlevere oplysninger om lagrede data til brugeren på en rimelig måde, således at brugeren kan forstå det materiale, der udleveres, tillige med at materialet skal udleveres indenfor en rimelig tid til en rimelig pris. Det vil altid være et skøn hvad rimelig tid og rimelige omkostninger er afhængig af hvad der ønskes udleveret. Men en udleveringstid på nogle uger og til omkostninger svarende til, hvad det koster databehandleren at finde frem til data synes at være rimeligt.

Leverandør	Kunde/databehandler
Kan systemet levere de ønskede brugerdata på en god pædagogisk måde, indenfor rimelig tid og til rimelige omkostninger?	Kan systemet levere de ønskede brugerdata på en god pædagogisk måde, indenfor rimelig tid og til rimelige omkostninger?

- **Databehandler skal udvise åbenhed overfor brugerens indsigt, men kan anvende betingelser for brugerens indsigt og i givet fald skal disse begrundes**
  Som det fremgår ovenfor skal databehandleren være imødekommende overfor brugere, der ønsker indsigt i deres egne data. Imidlertid kan der måske i konkrete sammenhænge være rimelige begrundelser for at afslå udlevering af alle eller dele af data. I givet fald skal dette begrundes.

Leverandør	Kunde/databehandler
Er det let for brugeren at få adgang til den rette databehandler? Er alle aktører instrueret om brugernes ret til adgang til egne data? Offentliggøres sikkerheds- og privacyanalyser af systemerne?	Er det let for brugeren at få adgang til den rette databehandler? Er alle aktører instrueret om brugernes ret til adgang til egne data? Har virksomheden et beredskab til at vurdere om data skal udleveres eller ej? Såfremt data ikke kan udleveres har virksomheden så et beredskab til at håndtere denne kundekontakt? Offentliggøres sikkerheds- og privacyanalyser af systemerne?

- **Brugeren har ret til retslig prøvelse af sammenhæng mellem data og formål, datas kvalitet og eventuel manglende efterlevelse af privacypolitikker**
  Databehandler skal være opmærksom på, at brugerne har til - efter at have skabt sig et billede af hvilke data, der opbevares om vedkommende - at få prøvet sammenhæng mellem

data og formål, datas kvalitet og eventuel manglende efterlevelse af privacypolitikker ved retten.

Leverandør	Kunde/databehandler
	Findes der et beredskab til at håndtere sagsanlæg på privacyområdet og til at vurdere konsekvenser af en kendelse, der går imod virksomheden? Findes der nogle i virksomheden, som kan vurdere konsekvenserne af en tabt sag i forhold til andre brugeres eventuelle lignende sagsanlæg?

- **Brugeren har kun ret til indsigt med begrænset frekvens**
  Brugerne har ifølge dansk lovning kun ret til indsigt i hvilke informationer, der er registeret i en given enhed hver 6. måned. Dette er vedtaget for ikke at pålægge unødige administrative byrder på databehandler.

Leverandør	Kunde/databehandler
Registrerer systemet hvornår en bruger har bedt om indsigt i data og hvad status på indsigten er?	Findes der procedurer, som sikrer at indsigtsreglerne overholdes?

- **Databehandler har ansvar for data og disses sikkerhed**
  Databehandler skal beskytte de personhenførbare oplysninger, på en sådan måde, så brugeren kan være sikker på at de ikke ændres til noget ukorrekt og således at de ikke afsløres for uvedkommende. Generelt bør integritet, autenticitet, tilgængelighed, fortrolighed og uafviselig sikres. Personhenførbare oplysninger bør opfattes med en meget høj grad af beskyttelse. Der henvises i almindelighed til ITEK og Dansk Industris sikkerhedshæfter og -vejledninger for at forbedre virksomhedens sikkerhed.

Leverandør	Kunde/databehandler
Er personhenførbare data beskyttet i henhold til god IT-sikkerhedsskik - som f.eks. gennemgået i DS484? Er der herunder foretaget risikoanalyse? Er adgangen til data begrænset til de, der har en rolle at spille i forbindelse med data? Logges det hvem der tilgår data? Er der rettighedsstyring, således at det kan bestemmes hvem der må gøre hvad med data? Et systemerne i overensstemmelse med kundens IT-sikkerhedspolitik? Er der nødprocedurer for eventuelle brister på sikkerheden?	Efterlever systemerne IT-sikkerhedspolitikken?

- **Dataflow over grænser er betinget til international handel, anvendelse af elektroniske services og dataflow internt i virksomheder. Dette bør reguleres gennem kontrakter**
  I lov om behandling af persondata er der fastslået en række særlige bestemmelser for personhenførebare oplysninger, der krydser landegrænser. Særligt interesserede bør sætte sig ind i denne del af lovgivningen, hvis det skønnes relevant, idet det ikke for nærværende gennemgås i denne "Praksis".

Leverandør	Kunde/databehandler
Er systemer indrettet således, at det logges, hvis personhenførbare data krydser landegrænser og dette sker i en usædvanlig sammenhæng?	Registreres det om og i givet fald hvilke personhenførbare data der krydser landegrænser? Er databehandler opmærksom på lovgivningen i de lande, som virksomhedens personhenførbare data, krydser?

- **Databehandler skal sikre at privacyforanstaltninger implementeres under hensyn til det tekniske niveau og med undtagelse for overvejelser om økonomiske omkostninger**
  Databehandleren har ansvar for at de løsninger, der implementeres har et tidssvarende teknisk niveau. Dette skal forstås således, at hvis man skal vælge mellem to systemer til behandling af personhenførbare data, vil det være relevant at vælge den løsning, som kan tilbyde privacy. Hvis en sådan løsning ikke findes, skal den udvikles, såfremt det kan ske indenfor en rimelig omkostningsmæssig ramme. Hvis man ikke indenfor en rimelig omkostningsmæssig ramme kan få et system, der kan tilfredsstille kravene til privacy, må man forsøge sig frem med alternative procedurer. Man kan altså ikke bare vælge det billigste system, der ikke har privacy implementeret og så tro man kan slippe af sted med det. Ældre systemer må antages at være underlagt en rimelighedsvurdering i forhold til hvilke data der behandles og hvordan.

Leverandør	Kunde/databehandler
Er der i den konkrete situation behov for et system, der har indbygget privacy? Stiller kunden krav til privacy eller skal han informeres om mulighederne herfor? Evalueres systemerne med henblik på at implementere nye privacyteknologier?	Hvilke behov for privacy (om nogen) er der i tilknytning til et konkret system? Kan den konkrete implementering bære omkostningerne til privacy eller skal der anvendes alternative procedurer? Evalueres systemerne med henblik på at implementere nye privacyteknologier?

- **Databehandler skal sikre at der findes en opdateret politik for privacy**
  Der skal tilvejebringes en egentlig privacypolitik, som er offentlig tilgængelig for brugerne. Man kan eventuelt søge inspiration hos OECDs privacy policygenerator.

Leverandør	Kunde/databehandler
Er der dokumentation for den privacy, som et givent system kan tilvejebringe?	Finder der en offentlig tilgængelig privacy politik, som kan tilgås af systemets brugere?

- **Databehandler skal sikre at brugeren med rimelighed er bekendt med politikken og har accepteret den**

Databehandleren skal med rimelig sikre, at brugerne er bekendt med privacypolitikken. Dette kan f.eks. ske ved at gøre denne overskuelig, indarbejde den i licensbetingelser og/eller ved at kræve at brugeren skal krydse af, at han er bekendt med politikken, inden han får adgang til en service.

Leverandør	**Kunde/databehandler**
Indhenter systemet dokumentation for at brugeren er bekendt med privacypolitikken inden systemet tages i brug?	Indhenter systemet dokumentation for at brugeren er bekendt med privacypolitikken inden systemet tages i brug? Gemmes den pågældende dokumentation sammen med data?

- **Databehandler skal anmelde behandling af data til tilsynsmyndighed**
  Man skal have en særlig tilladelse til at behandle personhenførbare data. Dette skyldes at man fra lovgivers side gerne vil sikre særlig beskyttelse af disse data. Den tilsynsførende myndighed i Danmark er Datatilsynet. Tilsynet står gerne til rådighed med oplysninger om hvad der skal til i en konkret situation for at behandle data.

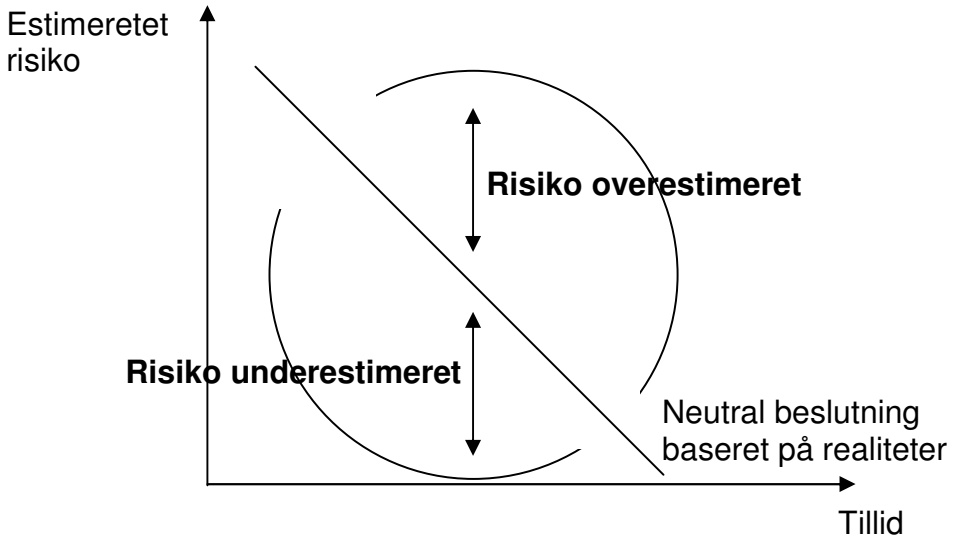
Leverandør	**Kunde/databehandler**
Er der indhentet tilladelse fra Datatilsynet til at systemet kan behandle personhenførbare data?	Er der indhentet tilladelse fra Datatilsynet til at systemet kan behandle personhenførbare data?

- **Databehandlers videre beskyttelse end de angivne principper er altid mulig**
  Det er altid muligt for databehandler at give bedre beskyttelse end angivet i loven og/eller denne "Praksis".

Leverandør	**Kunde/databehandler**
	Er der i den konkrete situation forretningsmæssige behov for at stille brugeren bedre end angivet i loven, "best practises" og andre kilder?

Brugernes kontrol med egne identiteter

Ovenstående gennemgang er baseret på, at loven overholdes, og at der sker en vis privacyforbedring gennem teknologiske foranstaltninger. Imidlertid baserer ovenstående sig på, at brugerne har tillid til, at disse to faktorer er opfyldt. Det baserer sig også på at brugeren har tillid til, at de systemer, som lagrer hans personhenførbare data, er sikre og ikke misbruges bevidst eller ubevidst af hackere, kriminelle eller andre. Det vil sige, at brugeren i ovenstående paradigme er nødt til at udvise tillid og acceptere den opfattede involverede risiko. Dette kan vi illustrere ved at se på sammenhængen mellem risiko og tillid, som illustreret i nedenstående figur 4.



Figur 4: Sammenhængen mellem risiko og tillid.

I figur 4 ser vi, at brugeren baserer sin tillid på den risiko han estimerer – des højere opfattet risiko desto lavere grundlag for tillid. Figuren inddrager også, at estimering af risiko er subjektiv, og at vi dermed oftest vil se en spredning af brugergruppen afhængigt af, hvilken risiko de estimerer, de står overfor. Der findes imidlertid systemer, som har til formål at reducere risikoen for dermed at øge tilliden. En egentlig ændring af risikoen kan ske ved at reducere mængden af data eller fjerne risikoen for identitetsrelateret kriminalitet såsom misbrug af kreditkortoplysninger. Dette kan bl.a. tilvejebringes gennem pseudonymer, og vi befinder os dermed i det orange område i figur 1.

Gennem anvendelsen af pseudonymer får brugeren kontrol med egne identiteter og dermed egne data. Hvis databehandler selv eller i samarbejde med en tredjepart ikke er i stand til at identificere brugeren - uden at brugeren har forbrudt sig mod gældende lovgivning eller frivilligt med fuldt samtykke indgået aftale - vil en relation med en bruger automatisk overholde de principper, der er skitseret ovenfor. I samme øjeblik identifikation bliver mulig bør de ovenfor skitserede principper overholdes hver for sig. Efterlevelsen af dette princip for kontrol med egne identiteter betyder, at man befinder sig i det orange område i figur 1. Dette princip er ikke udledt af lovningen, men er en måde at implementere og sikre overholdelse af denne på, samtidig med at brugeren får kontrol med egne data.

Ved at anvende løsningen bag dette princip kan brugeren vælge at oprette forskellige identiteter til forskellige formål. Brugeren autentificerer sig med en særskilt identitet overfor et system uden at identificere sig overfor systemet eller f.eks. kun at identificerer sig overfor en del af systemet (f.eks. overfor lægen, men ikke alle andre i sundhedssektoren med adgang til databasen). Hver sådan identitet er et såkaldt pseudonym eller en formålsspecifik identitet, der kan have forskellige måder at etablere sporbarhed og (gen)skabe en kobling til brugerens faktiske identitet. En anonym identitet har ingen måder at etablere sporbarhed på, bortset hvis brugen selv foretager sig handlinger, der muliggør identifikation. Sådanne identiteter kan ofte kun etableres med brug af privatlivsfremmede kommunikationsservices, som ikke er en del af selve systemet. Eksempler på sådanne services kan være anonymiseringsnetværk, credential services som både kan bevise positive (har fast arbejde) eller modbevise negative identitetselementer (ikke dømt for pædofili og ikke på oversigten over eftersøgte), anonyme digitale kontanter og postboks adresser.

I dette paradigme får brugeren kontrol med egne identiteter, herunder at han - så længe han ikke har uindfriede forpligtelser såsom gæld - beslutter, hvornår han ikke længere vil have, at en identitet kan identificeres. Databehandleren sikrer at systemet er indrettet således, at brugeren kan bruge pseudonyme identiteter overfor systemet. Databehandler må i dette paradigme kun hvis det er påviseligt nødvendigt (for eksempel for at forhindre snyd med en afstemningen) blokere for, at brugeren kan have flere forskellige identiteter overfor det samme system.

Leverandør	**Kunde/databehandler**
Er der behov for, at systemet giver mulighed for, at brugerne kan oprette, slette og ændre sin egen identitet eller flerhed af identiteter og de øvrige registreringer, der følger med en sådan identitet?	Er der behov for, at systemet giver mulighed for, at brugerne kan oprette, slette og ændre sin egen identitet eller flerhed af identiteter og de øvrige registreringer, der følger med en sådan identitet? Er der behov for at systemet før ændringer eller sletning af identiteter giver meddelelse herom til databehandler?

Opsummering

Denne vejledning har vist hvordan man kan forbedre privacy i elektroniske løsninger. Konklusionen er at man kan vælge en fremgangsmåde, hvor man efterlever en lang række alment anerkendte principper for privacy og her igennem opnår et niveau for privacy som dels opfylder loven og dels er i overensstemmelse med hvad der er almindeligt accepteret i samfundet. Alternativt kan man vælge en teknologisk løsning, som på baggrund af pseudonymer giver højere grad af privacy end lovgivningen kan tilvejebringe og samtidig giver muligheden for at dele data og tilvejebringe bedre services uden at skabe risiko for brugeren.