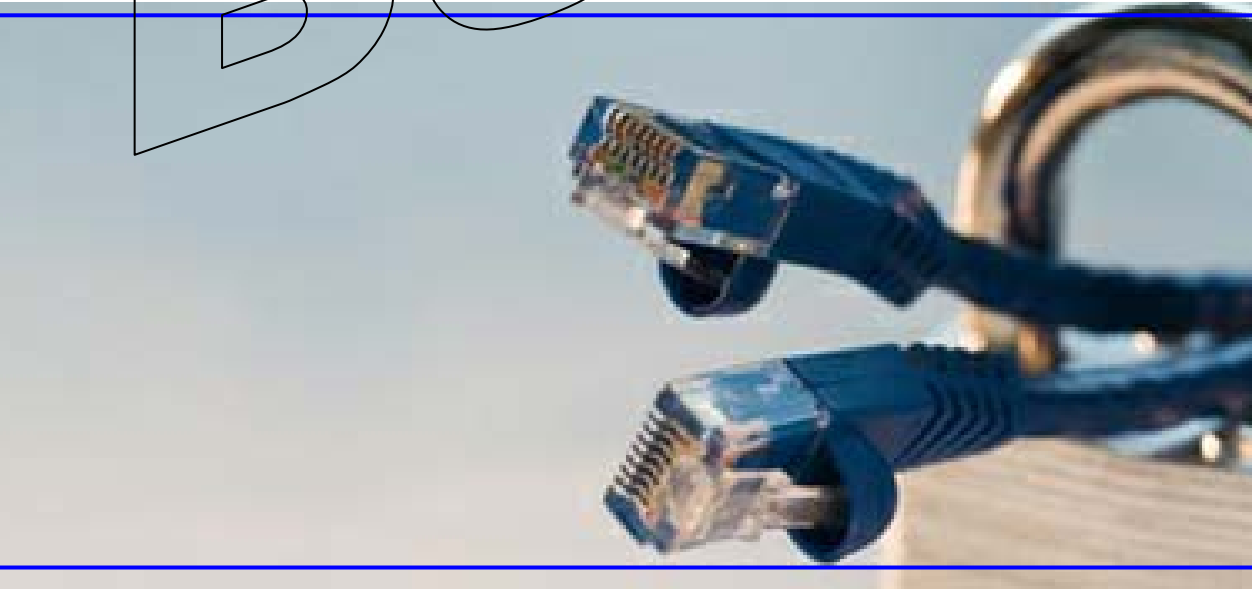
Beta

Håndbog i: Privatlivsimplikationsanalyse



IT- og Telestyrelsen
Marts 2010

>

Håndbog i:
Privatlivsimplikationsanalyse

Udarbejdet af:
IT- og Telestyrelsen

IT- & Telestyrelsen
Holsteinsgade 63
2100 København Ø

Telefon: 3545 0000
Fax: 3545 0010

Indholdsfortegnelse

<

>

Introduktion

>

Beskyttelsen af privatlivet

Beskyttelse af privatlivet (engelsk: privacy) er blevet en faktor, som i de seneste tiår har fået stadig større betydning for forretningslivet og offentlige myndigheder. De nye informationsteknologier har øget offentlighedens opmærksomhed på begrænsninger i beskyttelsen af privatlivet og den personlige integritet.

Privatlivets fred har længe været anerkendt som en del af menneskerettighederne, selv om begrebet fortsat er noget uklart eller tillægges forskellige betydninger. En fortolkning kunne være "den interesse som privatpersoner har i at opretholde et 'personligt frirum' uden indblanding fra andre mennesker og virksomheder".

Den europæiske Menneskerettighedskonvention formulerer rettigheden i artikel 8: “Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin korrespondance”. Nøglebegreberne er således beskyttelse af individets integritet og privatlivets fred, herunder individets kontrol over, hvornår og hvordan personhenførbare informationer frigives.

Ud over at privatlivets fred anerkendes som en menneskerettighed, er der indført specifik lovgivning på områder, hvor privatlivet er i fokus. Meget af den lovgivningsmæssige opmærksomhed har samlet sig om personrelaterede oplysninger, som indsamles, lagres, bruges og videregives af virksomheder og myndigheder. I Danmark er behandling af personoplysninger reguleret i persondataloven og en række bestemmelser i særlovgivningen. Datatilsynet er den centrale, uafhængige myndighed, der rådgiver om behandling af personoplysninger og fører tilsyn med, at persondataloven overholdes.

Der er også andre områder, hvor beskyttelse af privatlivet og den personlige integritet er aktuel, og som får stadig større interesse. Vigtige problemstillinger i dag er blandt andet overvågning af borgere, ansatte og kunders aktiviteter, aflytning og registrering af privatpersoners elektroniske kommunikation og disse personers elektroniske adgang til information. Endelig er der også et stigende fokus på brug af biometriske data, kropsvæsker og vævsprøver.

Hvordan håndteres betænkeligheder ved beskyttelsen af privatlivet?

Spørgsmål om beskyttelsen af privatlivet kan håndteres på forskellig måde. Som minimum skal virksomheder og myndigheder sikre sig, at de overholder de forskellige love, som beskytter privatlivet, herunder persondataloven

>

Mange går videre end det. Nogle virksomheder etablerer strategier for beskyttelse af privatliv og persondata og går aktivt ind for en kultur, der fokuserer på denne beskyttelse. Andre indarbejder processer, der kan tilgodese privatlivsbeskyttelse, når forretningsgangen tilrettelægges eller ændres. Det kan f.eks. gennemføres ved at tilpasse virksomhedens procedurer for systemudvikling og projektstyring.

Privatlivsimplikationsanalyse – Privacy Impact Assessment

Projekter, der omhandler personoplysninger eller bruger teknologier, som er indgribende overfor personer, giver anledning til bekymring for beskyttelsen af privatlivet.

Bekymringen udspringer af, at et projekts succes afhænger af, at brugerne anvender systemet. Det udgør derfor en betydelig risiko, hvis brugerne har betænkeligheder om deres personlige oplysningers sikkerhed. En risiko, som truer selve udbyttet af investeringen i det nye system.

For at imødegå den risiko kan det anbefales at bruge en risikostyringsteknik, hvor man vurderer risici i projektet med betydning for beskyttelsen af privatlivet. Teknikken kaldes i denne håndbog for "privatlivsimplikationsanalyse", forkortet PIA. Det er en oversættelse af det engelske begreb "privacy impact assessment", som også forkortes PIA.

En PIA er en proces, som sætter organisationer i stand til at forudse risici og tage højde for de sandsynlige konsekvenser af nye initiativer, foregribe problemer og finde frem til løsninger. Risici kan styres ved at indsamle og dele information med interessenter. Systemerne kan udformes, så der tages hensyn til privatlivet og beskyttelsen af personlig integritet. Allerede fra start kan der indbygges elementer, som modvirker en forringelse af privatlivsbeskyttelsen. En PIA resulterer i en rapport til afrapportering af analyseresultatet. Rapporten kan offentliggøres eller udsendes til en bredere kreds af interessenter.

En PIA bør gennemføres på et tidligt tidspunkt i projektet. Kontroller til sikring af overensstemmelse med lovgivningen, herunder både persondataloven og særlovgivning ("compliance-analyse") er en separat handling og gennemføres normalt senere, når alle systemvalg og – design er fastlagt.

>

En PIA kan gennemføres som en særskilt proces, parallelt med projektet. Alternativt kan det være hensigtsmæssigt at integrere PIA i den samlede projektplan eller i bredere aktiviteter til risikovurdering eller risikostyring.

Gennemførelsen af en PIA er ikke krævet i lovgivningen. Indholdet i denne håndbog er en vejledning til organisationer som en hjælp til at gennemføre egne vurderinger af projekter og deres risici med hensyn til beskyttelsen af privatlivet. Enhver organisation opfordres til at bruge håndbogen til at udforme og gennemføre en PIA-proces, som passer til det enkelte projekt.

Hvem henvender håndbogen sig til?

Formålet med indholdet i denne håndbog er at give en vejledning i, hvordan man udfører en PIA. Den henvender sig til projektmedarbejdere, der er involveret i større projekter, der kan komme til at berøre spørgsmål om beskyttelse af privatliv og personlig integritet. Også ledere på øverste niveau kan have gavn af at have kendskab til PIA'er for at kende de processer, som en moderne organisation skal gennemløbe som en del af en sund risikostyringspraksis.

Håndbogens opbygning

Både projekter og virksomheder varierer meget i størrelse og dermed også i spørgsmålet om håndtering af beskyttelsen af privatlivet. Det betyder, at visse af håndbogens afsnit ikke vil være lige relevante for alle projekter.

Håndbogen bygger på den engelske PIA håndbog, og er bygget op, så det er muligt hurtigt at påbegynde arbejdet med en PIA. Der forudsættes et vist forhåndskendskab til forhold vedrørende beskyttelse af privatliv for at gennemføre en PIA. Er man interesseret i generelle oplysninger forud for opstarten af PIA-processen, kan man finde baggrundsinformation om beskyttelse af privatlivet og PIA'er i kapitel I.

Inden man går i gang med at gennemføre en PIA anbefales det at foretage en screening. Screeningen viser, om en PIA er nødvendig og hvilket omfang den eventuelt skal have. Kapitel II i håndbogen indeholder en vejledning om, hvordan man forbereder og gennemfører screeningen. Efter screeningen bør det være klart, om der skal gennemføres en PIA i fuld skala eller i mindre, eller om en PIA ikke er nødvendig for projektet.

Kapitel I – Hvordan afgør man om en PIA er nødvendig?

Dette afsnit indeholder en introduktion til de hensyn, som tilgodeses ved privatlivsimplikationsanalyser. Medlemmer af projekt- eller PIA-grupper, som ikke er bekendt med behovet for beskyttelse af privatliv og personlig integritet, vil have fordel af materialet.

Hvorfor skal man foretage en PIA?

For mange virksomheder er hensynet til beskyttelsen af privatlivet forbundet med risici, som må håndteres professionelt i lighed med andre hensyn. Virksomheder, som behandler persondata, har brug for at overvåge deres aktiviteter løbende, hvad enten de har at gøre med klienter, ansatte eller offentligheden generelt. Særligt vigtigt er initiativer indeholdende avancerede teknologier, der bringer både nye muligheder og nye trusler med sig.

En virksomhed eller myndighed skal foretage en PIA for at:

- Identificere og styre risici.
- Undgå omkostninger.
- Undgå tab af tillid og omdømme.

Identificere og styre risici

De typer af projekter, som giver anledning til betænkeligheder ved beskyttelsen af privatlivet, er gerne forbundet med betydelig indsats og investering. Direktører har et ansvar for at sikre, at risici identificeres, vurderes og håndteres. Ansvaret omfatter en kontrol af, om der eksisterer problemer i relation til beskyttelsen af privatlivet. Hvis dette er tilfældet, må risikoen vurderes, og der må udformes og iværksættes en risikostyringsplan. PIA på myndighedens eller virksomhedernes overordnede niveau er en del af god virksomhedsledelse og god forretningsskik.

På projektstyringsniveau er en PIA et middel til at håndtere projektrisici. Risikostyring dækker et væsentligt større område end blot beskyttelsen af privatlivet, og det kan være hensigtsmæssigt at planlægge en PIA inden for rammerne af risikostyring i øvrigt.

En vigtig del i beskyttelsen af privatlivet er informationssikkerhed, jf. standarden for informationssikkerhed DS 484/ISO 27001, og nogle af elementerne i en PIA bør afspejle dette.

Undgå omkostninger

Ved at foretage en PIA tidligt i et projektforløb undgås det, at der opdages problemer på et senere stadium, når ændringer af komponenter er meget dyrere. Præcisering af et projekts målsætninger, virksomhedens krav og berettigelsen af bestemte designelementer er alle forhold, som er af væsentlig nytte for den generelle projektstyring. Det skal ikke blot ses som en del af risikovurderingen for beskyttelsen af privatlivet.

En yderligere fordel ved at indbygge følsomhed over for beskyttelsen af privatlivet i projektets design fra begyndelsen er, at der skabes grundlag for et fleksibelt og tilpasningsvenligt system, som nedbringer omkostningerne ved fremtidige ændringer, fremmer konkurrence- og innovationsevnen, samt sikrer en længere levetid for applikationen.

Undgå tab af tillid og omdømme

Borgerne tillægger beskyttelsen af privatlivet stor værdi. En PIA er et middel til at sikre, at systemer ikke sættes i drift med mangler i henseende til beskyttelsen af privatlivet, som vil pådrage sig opmærksomhed fra medier, konkurrenter, lobbygrupper eller tilsynsmyndigheder, der varetager offentlighedens interesse. Eller med mangler, som giver anledning til bekymring hos borgerne. I denne sammenhæng er PIA en hjælp til at opretholde eller styrke en virksomheds omdømme.

Hvad udløser en PIA?

Behovet for en PIA i fuld skala kan udløses på flere måder.

- En PIA kan være et lovkrav. På det tidspunkt, hvor denne håndbog skrives, er der ingen love Danmark, der kræver en PIA.
- Den virksomhed eller myndighed, som gennemfører eller er involveret i et projekt kan vurdere, at et forslag har væsentlige konsekvenser, som bør gøres til genstand for undersøgelse. Motivationen kan være den offentlige politik, forretningsetik / etisk ledelse, eller et ønske om opnå tillid hos offentligheden og forbrugerne og dermed sikre sig afkast på sine investeringer.
- Der kan eksistere betænkeligheder i offentligheden ved det pågældende forslag eller ved forslag af denne art, måske affødt af historier, som er fremkommet i medierne.

Den mest almindelige udløsende faktor for en PIA er imidlertid, at myndigheden finder at et forslag kan give anledning til betænkeligheder i offentligheden,

hvilket vil udgøre en betydelig projektrisiko. For at håndtere dette er en risikostyringsplan påkrævet.

Hvornår skal en PIA foretages?

Enhver ændring i specifikationer og enhver rettelse af fejl kræver mere arbejde. Det medfører forsinkelser, og omkostningerne ved ændringer stiger, jo senere i projektet de foretages. Privacy-beskyttende elementer bør derfor indgå tidligt i projektfasen, f.eks. i systemdesignet og ikke "skrues på" senere. For at opnå dette, foreslås følgende retningslinjer.

- Start tidligt med at sikre, at projektrisici identificeres og klarlægges, før problemerne forankres i designet.
- Om muligt, påbegynd en PIA som en del af projektets iværksættelsesfase (eller hvad der svarer dertil i den anvendte projektmetode).
- Er projektet allerede i gang, start da i dag, således at eventuelle større problemer klarlægges med mindst mulig forsinkelse.

En PIA kan formuleres og gennemføres som en engangsforeteelse. I så fald tager den højde for de foreliggende oplysninger om projektet på det givne tidspunkt og sender ideer videre til projektets design. Men den kan ikke afspejle information, af mere detaljeret art, som bliver tilgængelig på et senere stadium.

En PIA kan gennemføres som en selvstændig aktivitet ved siden af projektet og adskilt herfra. Dette kan imidlertid skabe afstand mellem de medarbejdere, som foretager PIA'en, og projektgruppen, og modvilje mod indsigt affødt af PIA'en.

Imidlertid gælder det, navnlig ved større projekter, at den mest fordelagtige og omkostningseffektive fremgangsmåde er at gribe PIA'en an som en tilbagevendende proces, en proces sammenkædet med projektets eget forløb og en proces, der tages op igen ved hver ny projektfase.

Hver version kan tage hensyn til de detaljerede specifikationer, som aktuelt er til rådighed i planen, samt resultatet af tidligere PIA-faser.

Endelig kan virksomheden foretage en mere generel risikovurdering som en del af projektet, eller den kan operere med fælles processer for risikostyring. I så fald kan det overvejes at foretage PIA'en inden for rammerne af en bredere risikostyring.

Kapitel II PIA-screeningen

>

Gennemfører man en screening som noget af det første i projektet vil det fremgå, om der skal gennemføres en PIA i fuld skala, i mindre skala, om der bør udarbejdes en compliance-analyse – dvs. en kontrol af overensstemmelse med lovgivning eller om en PIA ikke er relevant for projektet.

Forberedelse til PIA-screening

For at man kan bruge kriterierne i screeningen må man først indsamle tilstrækkelige oplysninger. Tre trin foreslås:

1. Udarbejd en projektskitse,
2. foretag en interessentanalyse, og
3. udfør en miljøscanning.

1. Udarbejd en projektskitse

Risikostyring er mest effektiv, hvis den påbegyndes tidligt i et projektforløb. Under de tidlige stadier af et projekt har man kun begrænset viden, og der kan være uklarhed om projektets omfang og elementerne i det planlagte system. Tidligt i et projektforløb er informationskilderne som regel følgende:

- Dokumenter til iværksættelse af projektet, f.eks. et projektgrundlag eller kommissorium, og
- interviews med relevante medarbejdere i den ledende virksomhed, centrale interessenter, medlemmer af projektets styregruppe og eventuelt andre.

Ud fra disse oplysninger kan der udarbejdes en kort beskrivelse på 1-2 sider af projektet som grundlag for efterfølgende analyser.

Udarbejdes projektbeskrivelsen på et senere stadie af projektet, vil der være mere viden til rådighed. Projektskitsen bør derfor indeholde henvisninger til relevante dokumenter, herunder beskrivelser af relevante teknologier, tidligere systemer og/eller lignende projekter andetsteds. Også foregående PIA'er fra en tidligere fase af projektet eller i forbindelse med udviklingen af systemet er nyttige, når man udarbejder projektskitsen.

2. Foretag en interessentanalyse

Projektets interessenter bør identificeres så tidligt som muligt. Det kan bl.a. være:

- Den virksomhed eller myndighed, som gennemfører projektet, og måske også forskellige undervirksomheder eller -afdelinger inden for denne,

>

- andre virksomheder eller myndigheder, som er direkte involveret i projektet,
- virksomheder, myndigheder og privatpersoner, som skal have nytte af projektet,
- virksomheder, myndigheder og privatpersoner, som kan være berørt af projektet, og eventuelt
- virksomheder, som leverer teknologi og serviceydelser til realisering af projektet.

3. Udfør en miljøscanning

Det kan være relevant at søge information om forudgående projekter af lignende art. Hvis der skal bruges ny teknologi, eller hvis projektet anvender eksisterende teknologi på nye måder, er det en hjælp til vurderingen, hvis der indsamles beskrivelser af teknologien og tilhørende applikationer. Følgende kilder kan overvejes:

- Forudgående PIA'er om lignende projekter, hvad enten de er gennemført inden for virksomheden eller myndigheden, af andre virksomheder eller i andre lande,
- faktablade, hvidbøger, rapporter og artikler, som er udgivet af brancheorganisationer, teknologileverandører og forskningscentre,
- erhvervssammenslutninger,
- reguleringsmyndigheder, herunder navnlig Datatilsynet,
- andre reguleringsmyndigheder, f.eks. vedrørende forbrugerrettigheder,
- virksomheder, som repræsenterer eller rådgiver parter, der potentielt bliver berørt af projektet.

Disse undersøgelser kan afdække design og designmæssige elementer, som andre projektgrupper har fundet frem til.

Anvend kriterierne

Når de tilgængelige oplysninger er samlet sammen og dokumenteret, kan screeningen gennemføres. Formålet med screeningen er at sikre, at investeringen i det nye projekt står i rimeligt forhold til de forbundne risici.

Hvis der er utilstrækkelige oplysninger til rådighed

Det er muligt, at der ikke er tilstrækkelige oplysninger om projektet til at nå frem til en klar konklusion. I så fald har man følgende muligheder:

- Drøft sagen yderligere med medarbejdere hos den ledende virksomhed, interessenter og andre relevante parter.

>

- Påbegynd en PIA i fuld skala, idet det kan være nødvendigt at afkorte processen, hvis projektet viser sig kun at have begrænset konsekvens for beskyttelsen af privatlivet.
- Udsæt PIA-screeningen, til der er opnået en afklaring.
- Se efter informationskilder længere borte, f.eks. PIA'er som er gennemført for projekter, som har fælles træk med det aktuelle projekt.

PIA-screeningen

Det kan være dyrt for en myndighed eller virksomhed, hvis man for sent opdager, at et projekt har betydelige konsekvenser for privatlivet. På den anden side vil det være spild af ressourcer at gennemføre en unødvendig PIA. Derfor kan det godt betale sig at foretage en foreløbig vurdering for at afgøre, om en PIA er nødvendig.

Denne del af håndbogen indeholder et screeningsværktøj for PIA. Svarene på spørgsmålene om projektet giver en indikation for, om en PIA er nødvendig, og i givet fald om projektet kræver en PIA i fuld skala eller en PIA i mindre skala. Endvidere indeholder screeningsværktøjet overvejelser om nødvendigheden af at kontrollere overensstemmelse med relevante lovbestemmelser, herunder navnlig persondataloven med tilhørende bekendtgørelser.

Privatlivsimplikationsanalyse

Trin 1: Er en PIA i fuld skala nødvendig?	Indikerer projektets vigtigste karakteristika, at der er behov for en PIA i fuld skala? Se screeningsspørgsmål i appendiks 1		
	Hvis ja	Så	Foretag en PIA i fuld skala
		Og	Overvej trin 3
	Hvis nej	Så	Gå til trin 2
Trin 2: **Er en PIA i mindre skala nødvendig?**	Indikerer projektets karakteristika, at der er behov for en PIA i mindre skala? Se screeningsspørgsmål i appendiks 2		
	Hvis ja	så	Foretag en PIA i mindre skala
		og	Overvej trin 3

Compliance-analyse for overensstemmelse med persondataloven og anden relevant lovgivning

Trin 3: **Er det nødvendigt at kontrollere overensstemmelse med lovbestemmelser om beskyttelse af privatlivet?**	Er nogle af aktiviteterne underkastet nogen form for lovbestemmelser om beskyttelse af privatlivet? Se appendiks 3

>

	Hvis ja	så	Kontrollér overensstemmelse med lovgivningen om beskyttelse af privatlivet
		og	overvej trin 4
Trin 4: **Er det nødvendigt at kontrollere overensstemmelse med persondataloven?**	Indbefatter aktiviteterne behandling af 'persondata'? Se appendiks 3		
	Hvis ja	Så	Kontrollér overensstemmelse med persondataloven

Trin 1 - Kriterier for en PIA i fuld skala

Vurderingsprocessen omfatter 11 spørgsmål om projektets vigtigste karakteristika og det system, der skal leveres og anvendes til at afgøre, om der skal udarbejdes en PIA i fuld skala. Spørgsmålene er listet appendiks 1.

Synspunkter som må tages i betragtning

Forskellige interessegrupper kan have varierende synspunkter med hensyn til vurdering af screeningsspørgsmål. Hvis analysen foretages alene ud fra virksomhedens egen synsvinkel, er det ikke usandsynligt, at visse risici vil blive overset. Det anbefales derfor, at interessenternes synspunkter så vidt muligt tages i betragtning, efterhånden som hvert spørgsmål besvares.

I relation til de privatpersoner, som berøres af projektet, må man fokusere mere præcist end blot på borgere eller beboere i almindelighed eller befolkningen som helhed. For at sikre fuld forståelse af de forskellige segmenter af befolkningen, som har interesse i projektet eller berøres heraf, kan det være nødvendigt at detaljere den interessentanalyse, som blev foretaget som et led i det forberedende trin.

Anvendelse af kriterierne

Når de 11 spørgsmål er besvaret hver for sig, må svarene betragtes som et hele for at kunne konkludere, om en PIA i fuld skala er berettiget. Hvis det er tilfældet, skal nødvendigheden af, at udføre en compliance-analyse i forhold til lovgrundlaget også afgøres (trin 3 og 4 af screeningen).

Trin 2 - Kriterier for en PIA i mindre skala

Dette afsnit indeholder vejledning til vurdering af, om der skal foretages en PIA i mindre skala. Vurderingsprocessen omfatter også her et sæt spørgsmål om

projektets karakteristika eller det system, som skal leveres. Spørgsmålene er angivet i appendiks 2 med kursiv. Fortolkningen af spørgsmålene er angivet som almindelig tekst.

Anvendelse af kriterierne

Hvis svarene på spørgsmålene er "ja", skal man være opmærksom på konsekvensen for beskyttelsen af privatlivet og den deraf følgende risiko for projektet. Jo større betydningen er, jo større sandsynlighed er der for, at en PIA i mindre skala er berettiget.

Hvis kun et eller to forhold giver anledning til overvejelser om beskyttelsen af privatlivet, må PIA-processen indrettes med fokus herpå. Hvis derimod flere spørgsmål besvares med "ja", er det relevant at foretage en mere omfattende vurdering. En PIA i mindre skala beskrives i kapitel 4.

Såfremt man ønsker at komplementere PIA-analysen med en compliance-analyse for overensstemmelse med relevant lovgivning herunder persondataloven, er processen for dette beskrevet i appendiks 3.

Trin 3 og 4 - Compliance-analyse

Myndigheden eller virksomheden skal sikre sig, at projektet, de behandlede persondata og de anvendte forretningsprocesser er i overensstemmelse med al relevant lovgivning, herunder også persondataloven. Dette er ikke en anbefaling i denne håndbog, men et krav ifølge lovgivningen.

Såfremt screeningen indikerer, at der er særlig grund til at kontrollerer overensstemmelse med lovgivningen, kan en compliance-analyse udføres. I modsætning til en PIA, der bedst påbegyndes på et tidligt tidspunkt i projektforløbet, foretages den såkaldte overensstemmelseskontrol normalt senere, når designet er nået så langt som til detailstadiet, eller umiddelbart før implementering påbegyndes.

Datatilsynet er for nuværende i gang med at udarbejde en vejledning i compliance-analyse for kontrol af overensstemmelse med persondataloven, som anbefales anvendt ved belysning af lovmæssige forhold. Appendiks 3 indeholder tillige en kort oversigt over de væsentligste spørgsmål, der skal kunne besvares i en compliance-analyse.

Kapitel III - PIA i fuld skala >

Dette afsnit indeholder en beskrivelse af, hvordan man gennemfører en PIA i fuld skala. Afsnittet indledes med definition på en PIA, og rammerne for arbejdet med PIA. Arbejdet gøres nemmere ved en tidlig inddragelse af interessenter, etablering af en PIA-projektgruppe, ligesom de nødvendige ressourcer bør være tildelt projektledelsen inden analysen igangsættes.

Hvad og hvorfor?

En privatlivsimplikationsanalyse *(Privacy Impact Assessment, PIA)* kan defineres således:

En proces, hvor et projekts mulige risici for beskyttelsen af privatlivet klarlægges og undersøges fra relevante interessenters synspunkter, og hvor man forsøger at finde en måde, hvorpå sådanne konsekvenser og virkninger kan undgås eller minimeres.

Projekter med væsentlige konsekvenser kræver en omfattende PIA-proces for at sikre, at problemstillingerne belyses og behandles. Den omfatter analyse af teknologier og forretningsprocesser såvel som høring af interessenter. Udfaldet af en PIA berører projektets planlægning, processer og udformning.

For at en PIA skal være effektiv, skal den både fokusere på proces og resultat (rapport). PIA-processen går endvidere ud over kontrol og overholdelse af eksisterende love relateret til beskyttelsen af privatlivet. Compliance-analyse finder sted som et led i en komplementerende kontrol af overensstemmelse med relevante lovbestemmelser om beskyttelse af privatlivet, herunder navnlig persondataloven. Vejledning til denne proces findes i appendiks 3.

Resultaterne af en effektiv PIA-proces er:

- fastlæggelse af risici for projektet med hensyn til beskyttelse af privatlivet,
- vurdering af konsekvenser af risici, under hensynstagen til relevante interessenters perspektiver,
- forståelse af, om projektet kan accepteres af dem, der vil blive berørt,
- fastlæggelse og vurdering af alternativer, der i mindre grad krænker privatlivet,
- fastlæggelse og vurdering af alternativer, der ikke krænker privatlivet,
- hvor negative konsekvenser for beskyttelsen af privatlivet ikke kan undgås, klarhed over, hvilket forretningsmæssigt behov der berettiger dem, og
- dokumentation og publikation af resultaterne.

>

Rammer for PIA i fuld skala

'Rammer' er her anvendt for at betegne de foranstaltninger, som må træffes på overordnet ledelsesniveau, før man kan begynde på en PIA. Foranstaltningerne skal sikre, at processen bliver rigtigt struktureret.

Forholdet til projektet som et hele

En PIA er en del af den samlede proces for risikovurdering og risikostyring. Det er derfor hensigtsmæssigt at klarlægge forholdet mellem PIA'en og andre rutinemæssige aktiviteter til risikovurdering og -reduktion, som de benytter sig af.

Inddragelse af interessenter

En væsentlig risiko for projektet er, hvis deltagerne ikke føler sig fuldt forpligtede eller senere trækker sig ud fra deltagelse i projektet. For at sikre, at denne risiko kan styres, gennemføres en interessentanalyse normalt fra begyndelsen, så ledelsesform og den anvendte proces kan sikre en passende inddragelse af centrale interessenter. Relevante interessenter kan bland andet være:

- Virksomheden selv,
- andre deltagende virksomheder (i nogle tilfælde indbefatter disse eventuelt også underenheder med noget forskellige krav), og
- virksomheder, som har en reguleringsmæssig rolle. Udover offentlige organer som Datatilsynet og Finanstilsynet kan dette også omfatte brancheforeninger, og
- virksomheder og privatpersoner, som skal have nytte af projektet og/eller berøres af det. Disse er i reglen fra forskellige 'markedssegmenter', som har nytte eller berøres på forskellig måde.

Ledelsesstruktur

Virksomhedens direktører og øverste ledelse bør styre PIA-processen og forpligte sig. Misfornøjede interessenter udgør en risiko for projektets succes og afkast på investeringen i projektet.

Der er adskillige alternative måder, hvorpå strukturen af projektledelse og -processer kan udvides til at omfatte alle interessenter. For store projekter er det almindeligt at etablere en tilsynsgruppe. En projektstyregruppe har normalt beføjelse til at give anvisninger om projektforløbet, hvorimod en rådgivnings-, reference- eller konsulentgruppe ikke har.

>

Hvis der er flere interessenter med interesse i projektets aspekter vedrørende beskyttelsen af privatlivet, kan det være nyttigt at nedsætte en undergruppe, eller en rådgivnings-, reference- eller konsulentgruppe vedrørende PIA. I denne håndbog er anvendt "konsulentgruppe" for den engelske betegnelse PIA konsulent gruppe (PIA Consultative Group, PCG). Ved nogle projekter kan det være ønskeligt at give gruppen bredere fokus, som f.eks. offentlig politik eller reguleringsforhold. Hvis der arbejdes med en sådan struktur, må der etableres effektive links mellem de to niveauer af projektgrupper.

Ved mindre projekter er sådanne arrangementer ikke praktisk anvendelige, men der er behov for foranstaltninger, som sikrer klar kommunikation mellem de tre grupper: den øverste ledelse, projektgruppen samt repræsentanter og talsmænd for de forskellige interessenter.

Projektledelse

En almindelig fremgangsmåde er at etablere en projektstyregruppe (en gruppe med lederbeføjelser), og/eller en rådgivningsgruppe, referencegruppe eller konsulentgruppe (en repræsentativ gruppe hvis funktion er at diskutere, rådgive og assistere, men som ikke har nogen formel beføjelse til at lede processen). Uanset om der anvendes formelle ledelsesstrukturer eller ej, så bør der udarbejdes og vedtages et generelt kommissorium for PIA. Vigtige elementer i kommissoriet er bl.a.:

- Funktioner som skal udføres,
- slutprodukterne,
- de ønskede resultater,
- omfanget af vurderingen,
- rolle- og ansvarsfordeling for de forskellige parter, som medvirker i PIA'en.

Etablering af PIA-projektgruppen

PIA'en kræver en omfattende forståelse for selve projektet, kendskab til beskyttelse af privatlivet og ekspertise i at udføre risikovurderinger i almindelighed og privatlivet i særdeleshed. Nogle virksomheder har nogen eller al nødvendig ekspertise til rådighed internt. Andre skal bruge eksterne ressourcer til nogle af opgaverne, navnlig hvis deres erfaring med PIA'er er begrænset.

På grund af spredningen i ekspertise og interesser er det usædvanligt, at en PIA udføres af en enkelt person. Mere almindeligt er det at etablere en mindre PIA-

>

projektgruppe, som tilsammen har ekspertise på en række områder. Medlemmernes engagement vil formentlig strække sig over et vist tidsforløb, men behøver kun at være intensiv i relativt korte perioder.

Ressourcer

Ressourcetildelingen omfatter bl.a. medlemmerne af selve PIA-projektgruppen. Der kan være behov for, at den øverste ledelse med det overordnede ansvar for projektet midlertidigt omfordeler ansvarsområder for at afsætte tilstrækkelig tid til at få gennemført PIA'en på en grundig måde.

Planlægning af processen

Når rammerne for PIA'en først er fastlagt, må man planlægge at gennemføre aktiviteten. Dette afsnit beskriver følgende hovedpunkter for en PIA i fuld skala, som er ansvaret for en PIA, målsætningerne for en PIA og PIA-projektplanen.

Ansvaret for en PIA

Den virksomhed, som er den primære drivkraft i projektet, må påtage sig ansvaret for PIA'en. Det er denne virksomhed, som vil opnå størst fordel af PIA'en og vil lide størst skade, hvis en PIA ikke foretages, eller foretages på en måde, som ikke er optimal.

Når ansvaret for PIA'en skal uddelegeres til en egnet projektleder, har ledelsen to alternativer: enten at udpege lederen inden for den samlede projektgruppe eller at udpege en uden for projektet.

Uddelegeringen kan ske til et ledende medlem af projektgruppen som ansvarlig eller kontakt for spørgsmålet vedr. beskyttelse af privatlivet i projektet. Personen må have et klart mandat til at deltage aktivt i beslutninger om projektdesign, så det sikres, at sådanne beslutninger afspejler resultaterne af PIA-processen. Den privatlivsansvarlige skal også levere løbende rådgivning og feedback til den ansvarlige overordnede leder.

Målsætningerne for en PIA

Ved at indtage en positiv holdning bliver en PIA en lejlighed for virksomheden til at sikre, at dens forretningsprocesser er på linje med virksomhedens mission og samlede strategi. Dette afsnit beskæftiger sig med de forskellige målsætninger, som kan være relevante.

Primært er PIA'en en form for risikostyring. Den gør det muligt at imødegå projektrisici som f.eks.:

>

- Tab af offentlig troværdighed som følge af forhold, der opfattes som skadelige for beskyttelsen af privatlivet, eller bristede forventninger med hensyn til beskyttelse af personoplysninger
- Pålæg af reguleringsmæssige vilkår med tilbagevirkende kraft som reaktion på betænkeligheder i offentligheden
- Lav grad af anvendelse idet hele konceptet eller bestemte elementer i udformningen heraf opfattes som uhensigtsmæssigt
- Behov for ændring af systemdesign eller renovering af systemelementer på et sent tidspunkt i udviklingen
- Betydelige omkostninger, sammenbrud af projektet eller endog det færdige system som følge af negativ presseomtale, og/eller tilbagetrækning af støtte fra virksomheden eller fra en eller flere centrale deltagende virksomheder, eller
- Udføres også en compliance-analyse kan ses på manglende overensstemmelse på grund af overtrædelse af relevante lovbestemmelser om beskyttelse af privatlivet, herunder navnlig persondatalovens hensigter.

Ved planlægning af en PIA må den ansvarlige leder inden for virksomheden sikre sig, at alle disse muligheder er overvejet, og at virksomheden søger at få passende resultater ud af investeringen.

På overordnet niveau foreslås følgende som relevante målsætninger for en PIA:

1. Sikre effektiv styring af de projektrisici, der opstår som følge af projektets konsekvenser for beskyttelsen af privatlivet
2. Undgå kostbar omarbejdelse og renovering af projektelementer ved at opdage problemstillingerne tidligt
3. Udtænke løsninger på et tidligt tidspunkt af projektforløbet og sikre, at de gennemføres.

For at nå disse målsætninger kan der i projektplanlægningen tages udgangspunkt i følgende som operationelle mål for en PIA:

a) Fastlæg klart virksomhedens forretningsmæssige behov.
b) Fastlæg klart projektets design, herunder:
    a. de tekniske elementer,
    b. de relevante datastrømme,
    c. de relevante forretningsprocedurer,

>

c) Find elementer i designet, som udgør en risiko for beskyttelsen af privatlivet.
d) Sørg for, at berørte virksomheder og talsmænd får mulighed for at:
    a. opnå en forståelse af projektet,
    b. vurdere det ud fra egne synspunkter,
    c. få deres synspunkter forstået af andre interessenter,
    d. forstå andre interessenters synspunkter,
    e. få deres synspunkter afspejlet i projektdesignet.
e) Sørg for, at projektdesignet tilstræber maksimering af de positive konsekvenser og virkninger af projektet.
f) Sørg for, at de negative konsekvenser og virkninger af projektet undgås eller i det mindste reduceres.
g) Undgå fremkomst af nye krav på et sent stadium af designprocessen (eller endnu værre, under konstruktion, ibrugtagning eller endog drift), når ændringer er langt dyrere, langsommere og risikoudsatte.
h) Bevar offentlig troværdighed, så den offentlige tillid til projektet styrkes, og minimér risikoen for, at projektet møder vanskeligheder med hensyn til offentlig accept.
i) Sørg for information til:
    a. den øverste ledelse, chefer og driftspersonale i virksomheden og andre deltagende virksomheder,
    b. repræsentanter og talsmænd for interessenterne,
    c. relevante segmenter i offentligheden.
    d. Kom mulige fejlinformationskampagner i forkøbet.
j) Gør repræsentanter og talsmænd for interessenterne forpligtet til at støtte projektet for at undgå, at der dukker modstand op på et senere og dyrere tidspunkt af designprocessen.

PIA-projektplanen

En PIA i fuld skala er tilstrækkelig vigtig og kompleks til, at den i sig selv kan berettige en formel projektplan.

Andre deltagende virksomheder kan forventes at have et ønske om at deltage i udviklingen af projektplanen og komme med bidrag hertil. I mange tilfælde vil den mest hensigtsmæssige måde at varetage projektledelsen på indebære, at der skal oprettes en projektstyregruppe.

Gennemførelse af processen

Det er mest praktisk at bruge almindelige projektstyringsmetoder, når man vurderer konsekvenser for beskyttelse af privatlivet. Teknikker såsom

>

faseopdeling, opgave og leverancer inden for de enkelte faser. Nedenstående figur illustrerer på overordnet plan PIA-processen.

1. Indledende fase

Formålet med denne fase er at sikre, at der etableres et fast grundlag for at gennemføre PIA'en på en effektiv og hensigtsmæssig måde. De foreslåede slutprodukter er en projektplan og et projektoplæg.

2. Forberedende fase

Formålet med denne fase er at foretage de nødvendige dispositioner, så den kritiske fase 3 kan afvikles gnidningsløst. De foreslåede slutprodukter er en interessentanalyse, en høringsstrategi og høringsplan samt etablering af en konsulentgruppe for PIA *(PCG)*.

3. Hørings- og analysefase(r)

Når disse rammer er på plads, fokuserer denne fase på høring af interessenter, risikoanalyse, erkendelse af problemer og søgning efter løsninger. Det kan tænkes, at nogle aktiviteter skal udføres mere end én gang (f.eks. indkaldelse af mere end ét møde i PCG-gruppen).

Den største værdi for virksomheden opstår, når PIA'en påbegyndes på et tidligt stadium i det samlede projektforløb. I disse tilfælde bør der fastlægges flere hørings- og analysefaser, som gennemføres parallelt med faserne for planlægning, analyse, design, konstruktion og gennemførelse i det samlede projekt.

De foreslåede slutprodukter er ændringer af de relevante projektdokumenter, et register over spørgsmål og en rapport om designelementer vedrørende beskyttelsen af privatlivet.

4. Dokumentationsfase

Formålet med denne fase er at dokumentere processen og resultaterne. Det foreslåede slutprodukt er en PIA-rapport.

>

5. Revurderings- og revisionsfase

Formålet med denne fase er at sikre, at de designelementer, der fremkommer som resultat af PIA'en, gennemføres og er effektive. Det foreslåede slutprodukt er en revurderingsrapport.

PIA i fuld skala, indledende fase

Dette er fase 1 af den foreslåede PIA-proces på fem faser.

Formålet med denne fase er at sikre, at der etableres et fast grundlag for gennemførelse af PIA'en på effektiv og hensigtsmæssig måde. De foreslåede slutprodukter er en projektplan og et projektoplæg. Fasen indeholder følgende opgaver:

- Revurdér (eller om nødvendigt, udarbejd) kommissorium for PIA-projektet.
- Revurdér resultaterne af PIA screeningen.
- Revurdér (eller om nødvendigt, fastlæg) omfanget af PIA'en. I mindste udstrækning kan omfanget begrænses til ét eller to bestemte forhold eller en bestemt proces (som f.eks. indsamling af data, indhentning af samtykke eller videregivelse af information), eller en særlig teknologi (f.eks. chipkort). I største udstrækning vil PIA'en kunne omfatte en samfundsrelateret konsekvensvurdering. Da der er tale om en form for risikovurdering, bør omfanget af en PIA i fuld skala udtrykkes forholdsvis bredt.
- Revurdér (eller om nødvendigt, udarbejd) interessentanalysen, for at sikre, at hovedaktører i projektet er udpeget.
- Revurdér (eller om nødvendigt, udarbejd) projektplanen for PIA. Uanset om der foreslås en række faser, opgaver og resultater, må projektplanen tage højde for de specielle forhold i det pågældende projekt og afvige herfra, hvis det er nødvendigt.
- Hold indledende drøftelser med relevante virksomheder. Disse drøftelser vil i reglen fokusere på relevante dele af virksomheden selv og de vigtigste af eventuelt deltagende virksomheder. I nogle tilfælde kan det også være tilrådeligt at afholde tidlige drøftelser med eksterne virksomheder, herunder Datatilsynet.
- Gennemfør indledende drøftelser med repræsentanter og talsmænd for interessentgrupper. Dette kan være vigtigt, hvis bestemte eksterne parter i væsentlig grad er berørt af projektet og slutprodukter.
- Foretag en indledende identifikation af privatlivsrelaterede problemområder. Dette kan passende begynde med en fornyet og mere detaljeret overvejelse af resultaterne af screening-processen.

>

- Revurdér (eller om nødvendigt, udarbejd) scanningen for miljøspørgsmål for at sikre en opdateret forståelse af forskning, publikationer og medieaktivitet og af den måde, hvorpå andre virksomheder og myndighedsområder har grebet lignende projekter an.
- Revurdér ressourcetildelingen i lyset af det forståelsesniveau, der er tilvejebragt indtil dato.
- Udarbejd projektoplægget. Dette dokument vil udgøre grundlaget for drøftelser med interessenter.

PIA i fuld skala, projektoplæg

Den indledende fase af PIA-processen fører frem til et projektoplæg for det projekt, som underkastes PIA'en. Formålet med projektoplægget er at etablere et solidt grundlag for efterfølgende udarbejdelse, høring og analyse.

Projektoplægget kan med fordel berøre et eller flere af følgende punkter:

- En beskrivelse af sammenhængen eller rammerne, inden for hvilke forslaget fremsættes (herunder relevante samfundsmæssige, økonomiske og teknologiske overvejelser).
- En angivelse af de motiveringer, faktorer eller muligheder, der ligger til grund for projektet.
- En angivelse af projektets målsætninger, omfang og forretningsbegrundelse.
- En beskrivelse of projektets design, som afspejler virksomhedens aktuelle forståelse af, hvorledes projektet vil tage form. Projektoplægget kan beskrive flowet af personoplysninger med passende detaljeringsgrad. Disse kan indsættes som diagrammer med procesbeskrivelser og/eller procestabeller over relevante persondata.
- En indledende vurdering af potentielle privatlivets fred-relaterede risici, herunder både åbenbare eller direkte konsekvenser og langsigtede eller sekundære konsekvenser for beskyttelsen af privatlivet.
- Kortfattede beskrivelser af valgmuligheder og underliggende delmuligheder, som den ledende virksomhed har fundet frem til, både dem som allerede er forkastet og dem som stadig overvejes.
- Forretningsgrundlaget som forklarer berettigelsen af de elementer, der har mulige konsekvenser for privacy, udtrykt både som:
    - en forklaring på, hvorledes hovedelementerne i konceptet vil sikre opnåelse af målsætningerne og eventuelt
    - en cost-benefit analyse.

>

- Beskrivelser af den samlede projektplan, PIA-processen inden for denne samt høringsprocesser i forbindelse med PIA.
- Lister over implicerede virksomheder, interessentgrupper, repræsentanter og talsmænd, som er eller vil blive opfordret til at bidrage til PIA'en.
- Eventuelle vedhæftede bilag, som vil bidrage til forståelse af projektet og dets mulige konsekvenser for beskyttelsen af privatlivet.

Der kan være behov for supplerende oplysninger i tilfælde af projekter, hvor der anvendes teknologier, der er nye eller på anden måde er vanskelige at forstå for deltagere i høringsprocessen. For at opnå en effektiv høringsproces kan det være nødvendigt for at stille teknisk dokumentation og vejledninger til rådighed og eventuelt foretage demonstrationer. Eksempler på teknologier, hvor der i øjeblikket kan formodes at være behov for dette, omfatter:

- Kontaktbaserede chipkort,
- kontaktfrie chipkort og RFID-mærkater,
- identitetsstyring,
- portaler til tjenester og autentificering,
- data warehousing *(dataopbevaring)* og data mining *(dataopsøgning)*,
- teknologier til stedbestemmelse, og
- biometri.

PIA i fuld skala, forberedende fase

Dette er fase 2 af den femfasede PIA-proces.

Formålet med denne fase er at foretage de dispositioner, som er nødvendige for at den kritiske fase 3 kan afvikles gnidningsløst. De foreslåede slutprodukter er en interessentanalyse, en høringsstrategi og -plan samt etablering af konsulentgruppen for PIA (PCG*)*.

Følgende opgaver foreslås:

- Uddyb interessentanalysen yderligere. Den skal bygge på den tidligere interessentanalyse for at sikre, at alle relevante grupper er udpeget.
- Fastlæg en høringsstrategi. Dette tilsikrer, at drøftelser med interessenter er effektive.
- Opret en PIA-konsulentgruppe *(*PCG*)*. Dette indbefatter repræsentanter for interessentgrupper.

>

- Fordel projektoplægget til PCG. Dette sikrer, at PCG-medlemmerne kan forstå karakteren af forslaget.

PIA i fuld skala, interessentanalyse

Den forberedende fase omfatter analyse af interessenter i projektet. Målsætningerne for en PIA kan ikke opnås, og målene med projektet som helhed kan lide alvorlig skade, hvis en PIA-proces finder sted bag lukkede døre. Nutidens informationssystemer har en sådan art, at mange virksomheder er indblandet på forskellig vis; det kan være partnere, deltagere, outsourcede tjenesteleverandører eller teknologileverandører. For statslige projekter og offentlige-private partnerskaber er pågældende minister eller ministre optaget af, hvordan projektet skrider frem.

Formålet med interessentanalysen er at skabe grundlag for en effektiv høringsproces. Det sikrer man ved at finde frem til alle parter, der kan have en interesse i projektet. Nedenfor er angivet en liste over mulige interessenter:

- Virksomheden selv, og eventuelt afdelinger inden for virksomheden, som har en væsentlig interesse i sagen
- Deltagende virksomheder
- Reguleringsmyndigheder som f.eks. Datatilsynet
- De personer, som projektet retter sig imod, hvilket kan omfatte:
  - registrerede erhvervsvirksomheder, af forskellig størrelse og i varierende roller,
  - registrerede foreninger og sammenslutninger, af forskellig størrelse og i varierende roller, samt
  - privatpersoner generelt, i varierende roller, herunder forbrugere, klienter, borgere, ansatte, leverandører, forretningsdrivende og borgere, der er underkastet statslig regulering
- Eventuelt offentligheden.
- Eventuelt leverandører af relevante teknologier og tjenester.

PIA i fuld skala, høringsstrategi

Ethvert projekt kan berettige til en PIA i fuld skala, hvis det er tilstrækkelig komplekst og omfangsrigt og indeholder en trussel mod beskyttelsen af privatlivet. Den forberedende fase af den femfasede PIA-proces omfatter udvikling af en høringsstrategi.

>

Formålet med en høringsstrategi er at medvirke til håndtering af de risici for beskyttelsen af privatlivet, som er forbundet med projektet. For virksomheden er målet med at gennemføre en høring at:

- indsamle information om et projekts konsekvenser for beskyttelsen af privatlivet set fra alle synspunkter,
- få hjælp til at udveksle information blandt deltagerne,
- sikre forståelse for hinandens synspunkter blandt de forskellige grupper,
- klarlægge problemstillinger,
- skabe mulige løsninger,
- sikre feedback på accept af mulige løsninger fra de berørte parter,
- undgå, at der opdages problemer på et sent stadium af projektet, hvor alle de mulige løsninger er dyre,
- undgå, at de berørte parter på et sent stadium fremsætter berettigede klager om, at de ikke havde kendskab til projektet, bestemte elementer heri eller projektets konsekvenser, og
- få sikkerhed for, at alle relevante parter har mulighed for at bidrage til PIA'en, og selv oplever at have haft en sådan mulighed.

Udvikling af en strategi

Effektiv høring forudsætter, at alle interessenter er tilstrækkelig informeret omkring projektet. Det indbefatter, at interessenterne har mulighed for at videregive deres synspunkter og betænkeligheder, og at de udvikler en tiltro til, at deres synspunkter afspejles i designet.

Det er almindeligt, at høringsprocessen resulterer i ændringer i projektet og dets design. For at bidrage maksimalt til risikostyringen med mindst mulige omkostninger bør høringen derfor påbegyndes tidligt og fortsætte under hele projektforløbet. De vigtigste kendetegn for effektive høringsprocesser er:

- igangsættelse af drøftelser ved at give indledende information om projektet,
- medvirken af repræsentanter og talsmænd for interessentgrupper med relevant viden om de pågældende teknologier, systemer og konsekvenser for beskyttelsen af privatlivet,
- lettelse af samspillet mellem deltagerne, og
- resultater som viser, at parterne har taget hensyn til andre interessenters synspunkter.

>

De vigtigste forhold, der må tages i betragtning ved udarbejdelse af høringsstrategien, er følgende:

- En tilstrækkelig spredning i deltagerkredsen for at sikre, at alle relevante synspunkter er repræsenteret, og at al relevant information er samlet.
- Runder som nødvendigt med:
  - udsendelse af information fra virksomhedens side,
  - tiltag som fremmer samspillet mellem de forskellige interessenter.
- Indarbejdelse af alle parters informationsbidrag i efterfølgende runder af design- og iværksættelsesaktiviteter.

PIA i fuld skala, hørings- og analysefase

Fase 3 omfatter høring af interessenter, risikoanalyse, klarlægning af problemer og søgning efter løsninger. Formålet med denne fase er at sikre, at problemerne bringes for dagen tidligt, at man finder effektive løsninger, og at designet tilpasses efter disse løsninger.

De foreslåede slutprodukter er ændringer af projektdokumenterne, et register over spørgsmål og en rapport om designelementer vedrørende beskyttelsen af privatlivet. Følgende opgaver foreslås:

- Iværksæt den høringsstrategi, som blev fastlagt under foregående fase. Dette vil normalt omfatte en PCG-proces, med workshops og møder ansigt til ansigt, suppleret af elektroniske drøftelser og eventuelt også formelle bidrag.
- Analyser projektet og identificer mulige problemområder i relation til beskyttelse af privatlivets fred, der kan med fordel tages udgangspunkt i appendiks 4 – problemidentificerende spørgsmål
- Vurdér risici ved de identificerede problemområder (se appendiks 5 for vejledning i udarbejdelse af risikoanalyse)
- Tag problemområderne op til fornyet overvejelse. Fokuser på de forskellige fremgangsmåder, der er til rådighed for at løse problemerne:
  - foranstaltninger til at undgå konsekvenser for beskyttelsen af privatlivet,
  - foranstaltninger til at reducere konsekvenser for beskyttelsen af privatlivet, og
  - teknologier til forbedring privatlivsbeskyttelse (se appendiks 7 for en uddybning)

- Hvis det vurderes nødvendigt, kan problemer og løsninger dokumenteres løbende efterhånden. Ved store projekter er der risiko for, at "koncernhukommelsen" vil gå tabt, hvis PIA'en udføres i flere faser.
- Overvej de fremkomne vurderinger fra risikoanalysen vedrørende beskyttelsen af privatlivet.
- Rapporten vedrørende beskyttelsen af privatlivet leveres til PCG-gruppen og projektgruppen.
- Foretag høringer af PCG-gruppen.
- Indarbejd beslutninger om problemområder vedrørende beskyttelsen af privatlivet i designet, og hvis der er uløste spørgsmål, fortsæt høring og analyse.

Denne fase indebærer i reglen, at processen må gentages et antal gange. Den mest effektive fremgangsmåde er at gennemløbe processen første gang ved projektets iværksættelse og derpå sørge for, at efterfølgende gennemløb modsvarer de senere faser af projektet (f.eks. kravanalyse, logisk design, fysisk design, konstruktion, integration og ibrugtagning af det nye system).

Det må formodes, at projektoplægget vil kræve gradvise ændringer for at kunne afspejle udviklingen gennem projektet.

Som det vil fremgå af de anførte beskrivelser, er det normalt, at en PIA resulterer i ændringer af designet for at kunne reducere eller undgå negativ påvirkning af privatlivsbeskyttelsen. Ændringer på et sent tidspunkt kan naturligvis være dyre. Dette er en vigtig grund til, at det anbefales at påbegynde en PIA tidligt.

Problemområder relateret til beskyttelsen af privatlivet

Bestræbelser på at klarlægge og beskrive problemområder vil give udbytte i efterfølgende fase, for jo bedre et problem forstås, jo lettere bliver det at finde frem til måder at håndtere det på. Særlige forhold, der må tages i betragtning i PIA'er er bl.a.:

Brede spørgsmål vedrørende ***personoplysninger***, herunder:

- **Datafølsomhed** (udtrykket anvendes her i bred forstand i modsætning til det meget specifikke udtryk *følsomme personoplysninger*, som benyttes om de oplysningstyper, der er nævnt i persondatalovens § 7 og § 8). Dette vedrører særlige data om alle, der er involveret i databehandlingen (f.eks. sygdomme og handicaps, økonomiske oplysninger, familieforhold), alle data om en bestemt person (f.eks. truede personer), og særlige data om privatpersoner,

>

hvilket kan være af langsigtet art (f.eks. privatadresse), men også data af kort gyldighed (f.eks. midlertidig adresse, rejseplaner).

- **Datakvalitet** - Dette omfatter mange specifikke egenskaber, navnlig nøjagtighed, tilstrækkelighed og relevans i henseende til formålet. Jo længere data kommer væk fra deres oprindelige sammenhæng, jo større er sandsynligheden for, at de misfortolkes, og jo større er virkningen af selv små indskrænkninger i kvaliteten.
- **Databetydning.** Dette varierer betydeligt, men ofte umærkeligt, fra en sammenhæng til en anden, hvori udtrykket anvendes. For eksempel er 'ægtefælle' og 'barn' i høj grad flertydige udtryk. Forskelle i betydningen af tilsyneladende identiske oplysninger kan give anledning til misforståelser og fejl, hvilket kan resultere i skade for privatpersoner.
- **Sletning og tilintetgørelse af data.** Der må være en positiv indstilling for at sikre, at data kun opbevares så længe, som deres oprindelige formål tilsiger. Beskyttelse af privatlivet opnås ved at have specifikke formål i stedet for brede formål, som begrunder langvarig opbevaring. Tilintetgørelse af data gælder både data i oprindelig form og persondata, som anvendes til bestemte formål (f.eks. evaluering af programmer, revision eller analyse over tid).

Identitet, herunder*:*

- Flere forskellige anvendelser af identifikatorer.
- Nægtelse af anonymitet.
- Identifikatorer som direkte viser persondata (f.eks. indlejret fødselsdato).
- Identifikatorer som er forbundet med autentifikatorer (f.eks. kreditkortnummer plus supplerende detaljer), fordi det indebærer en risiko for identitetssvindel og i ekstreme tilfælde endog identitetstyveri.
- Biometriske data, som giver anledning til betænkeligheder med hensyn til beskyttelsen af privatlivet.

Funktionsforskydning, ud over den oprindelige sammenhæng for anvendelsen, i relation til:

- Anvendelse af personoplysninger.
- Anvendelse af identifikatorer.

Registrerings- og autentificeringsprocesser, herunder den byrde, som sådanne processer pålægger, disses krænkende karakter samt statens udøvelse af magt over for privatpersoner.

>

Overvågning, uanset om dette er i form af lyd, visuelt, ved hjælp af data, med eller uden elektronisk støtte, og uanset om observationerne registreres eller ikke.

Stedbestemmelse og sporing, uanset om dette er inden for geografiske områder eller online f.eks. IP-adresser, selv hvor det finder sted tilfældigt, og navnlig hvor det giver anledning til registrering.

Krænkelse af personlig privatliv, især tvungen aflevering af prøver af væv eller kropsvæsker samt biometrisk måling.

Ovenstående områder kan med fordel konkretiseres med udgangspunkt i problemidentificerende spørgsmål, angivet i appendiks 4.

PIA i fuld skala, dokumentationsfase

Formålet med fase 4 er at dokumentere PIA-processen og udfaldet heraf. Det foreslåede slutprodukt en endelig PIA-rapport.

En konsekvensvurdering for beskyttelsen af privatlivet er imidlertid først og fremmest en proces. Værdien for virksomheden, som gennemfører processen, kommer i form af læring og tilpasning. Dels opnår interessenterne læringen, dels den virksomhed og gruppe, som er ansvarlig for projektet. Selv om processen er i fokus, er der fordele ved at udarbejde et endeligt dokument hen i mod afslutningen af PIA-processen. Følgende opgaver foreslås:

- Saml beslutningerne om foranstaltninger for at forhindre og reducere konsekvenser i en endelig version af risikoanalysen vedrørende beskyttelsen af privatlivet.
- Udarbejd en PIA-rapport.
- Send PIA-rapporten til PCG-gruppen.
- Offentliggør PIA-rapporten (idet sikkerhedsfølsomme oplysninger tilbageholdes i fortrolige eller lukkede bilag).

PIA-rapporten

Grundene til at udarbejde en PIA-rapport er:

a. En form for regnskabsaflæggelse for at vise, at PIA-processen er gennemført
b. Et grundlag for en efterundersøgelse og revision

>

c. Et bidrag til virksomhedens hukommelse, så det sikres, at de vurderinger, som er samlet under projektet, vil være til rådighed for dem fremover – også hvis de oprindelige medarbejdere forlader virksomheden
d. Et bidrag til vidensdeling - at gøre det muligt at dele den viden, som er opnået under projektet med fremtidige PIA-grupper og andre uden for virksomheden

En PIA-rapport består af tre hovedområder samt bilag:

1. Introduktion: Projektet og dets kontekst beskrives kort.
2. Analyse: Områder, processer og designelementer, hvori personoplysninger anvendes for mulige krænkelser af privatlivet beskrives og analyseres. Væsentligste problemområder, og trusler i forbindelse hermed, identificeres.
3. Vurdering: PIA-rapporten fremstiller sin vurdering af mulige problemområder, måder og elementer, hvori privatlivets fred kan risikere at blive krænket. I vurderingen skal det forretningsgrundlag, der berettiger krænkelsen af privatlivet, inddrages, ligesom der kort skal redegøres for implementerede tiltag og yderligere alternativer. Endelig skal det vurderes, om offentligheden på basis af resultatet af den udarbejdede analyse kan acceptere konceptet eller løsningen og dets anvendelsesmuligheder.
4. Bilag: Herunder f.eks. projektoplæg og projektplan.

Hvis det kontrolleres, at designet er i overensstemmelse med lovgivningen, kan det være hensigtsmæssigt at tilføje følgende yderligere bilag til PIA-rapporten:

- undersøgelse af overensstemmelse med relevante lovbestemmelser om beskyttelse af privatlivet,
- undersøgelse af overensstemmelse med persondataloven.

En PIA-rapport skrives i forventning om, at den skal offentliggøres. Herved opfylder rapporten dets formål som: regnskabsaflæggelse, efterundersøgelse, revision, input til fremtidige gentagelser af PIA samt baggrundsinformation for medarbejdere, der foretager PIA'er i fremtiden. Imidlertid kan nogle af de oplysninger, der anvendes i en PIA-proces, være følsomme i sikkerhedsmæssig eller kommerciel henseende. Disse oplysninger kan henlægges til fortrolige bilag, men bør begrænses til kun at ske i berettiget omfang.

Appendiks 5 uddyber indholdet af PIA-rapporten og en mulig struktur i udarbejdelsen.

>

PIA i fuld skala, revurderings- og revisionsfase

Dette er fase 5 i PIA-processen. Formålet med denne fase er at sikre, at de forpligtelser, som hidrører fra hørings- og analysefasen, føres videre frem til det idriftsatte system eller gennemførte projekt. Det foreslåede slutprodukt er aflevering af disse forpligtelser i form af rapporten om designelementer vedrørende beskyttelsen af privatlivet.

Følgende opgaver foreslås:

- Foretag en revurdering af, om foranstaltninger til at reducere og undgå konsekvenser for beskyttelsen af privatlivet, som blev dokumenteret i spørgsmålsregisteret og/eller rapporten om designelementer vedrørende beskyttelsen af privatlivet, er blevet gennemført.
- Udarbejd en revurderingsrapport.
- Fremlæg revurderingsrapporten om beskyttelsen af privatlivet for PCG-gruppen.
- Gør revurderingsrapporten om beskyttelsen af privatlivet offentlig tilgængelig.

Som i de foregående faser er det en fordel at gennemføre denne fase på et hensigtsmæssigt tidspunkt i det samlede projektforløb. Dette kunne for eksempel være ved en milepæl som den detaljerede revurdering af designet, eller hvad der svarer dertil med pågældende projektmetode.

En anden hensigtsmæssig eller omkostningseffektiv fremgangsmåde er at indbygge revurderingen af udførelsen i virksomhedens standard, periodisk eller lejlighedsvis gennemførte interne revision eller eksterne revisionsprocesser.

Kapitel IV - PIA i mindre skala >

Indledning

Projekter med væsentlige konsekvenser berettiger en PIA-proces i fuld skala. Andre projekter kræver opmærksomhed, men berettiger ikke så stor en investering i tid og ressourcer. En PIA i mindre skala omfatter analyse af de spørgsmål vedr. beskyttelsen af privatlivet, som screeningen har sat fokus.

Processen for en PIA i mindre skala afviger væsentligt fra en PIA i fuld skala. Særligt bemærkes:

- den er mindre formaliseret,
- den betyder mindre investering,
- den kræver mindre omfattende analyse og dataindsamling, og
- den har i reglen fokus på specifikke punkter i projektet snarere end projektet som helhed.

Da projekter er vidt forskellige, må der findes en proces, som opfylder behovet. Processen skal være så omfattende, som behovet tilsiger, men kun er så ressourcekrævende, som det er hensigtsmæssigt efter omstændighederne.

Dette kapitel er baseret på PIA-processen i fuld skala, således som denne er beskrevet i kapitel III i håndbogen, men er meget kortere. Vejledningen er i to dele:

1. Baggrundsinformation, der skal hjælpe virksomhederne til at opnå en forståelse af de typer af projekter, hvor en PIA i mindre skala er hensigtsmæssig.
2. PIA-processen, herunder indledende fase, forberedende fase, hørings- og analysefase(r), dokumentationsfase og revurderings- og revisionsfase.

PIA i mindre skala, baggrundsinformation

Omfanget af PIA'en må afspejle karakteren af projektet som helhed. Nedenfor er angivet eksempler på en række forskellige projekttyper, hvor en PIA i mindre skala kan være hensigtsmæssig.

- Udskiftning af et eksisterende persondatasystem med ny færdig softwarepakke med påfølgende ændringer af forretningsprocesser og eventuelt datalagring.
- Design og udvikling af et nyt persondatasystem, der kun skal indeholde data om mennesker, der har givet deres samtykke.

- Udbygning af et eksisterende system med henblik på at indsamle, lagre og anvende flere supplerende persondataelementer.

Vigtige kendetegn for en effektiv PIA i mindre skala er:

- En PIA er en form for risikostyring.
- En PIA tjener virksomhedens eget behov, idet den klarlægger spørgsmål vedr. beskyttelsen af privatlivet på et tidligt tidspunkt og gør det muligt at håndtere det på en hurtig og billig måde, så de ikke bliver til større problemer senere.
- For at tjene virksomhedens behov må en PIA afspejle alle interessenters synspunkter i projektet, herunder ikke mindst de berørte privatpersoner.
- En PIA drejer sig både om proces og produkt.
- En PIA er ikke en kontrol af overensstemmelse med lovgivningen.
- En effektiv gennemførelse af PIA'en forudsætter, at den nødvendige ekspertise er til rådighed..

PIA i mindre skala, processen

Det er hverken muligt eller ønskeligt at specificere en fast proces for en PIA i mindre skala som følge af de mange forskellige omstændigheder, der kan spille ind. Overordnet bør processen for et bestemt projekt afspejle:

- projektets art (f.eks. nyt system, erstatningssystem, udbygning af eksisterende system, ny teknologi, outsourcing, ændrede forretningsprocesser eller instruktioner til medarbejdere, udskiftet brugergrænseflade, revideret politikerklæring vedrørende beskyttelsen af privatlivet, udarbejdelse af lovændringer),
- de specifikke aspekter i projektet, som screeningen har sat fokus på,
- eventuelle relevante PIA'er som tidligere er foretaget, og
- virksomhedens erfaringsniveau med hensyn til at foretage PIA'er.

Nedenstående vejledning er således af generel karakter og er beregnet på at hjælpe virksomhederne med at udvikle deres egen projektplan. Der kan anvendes konventionelle projektstyringsteknikker i processen, når man vurderer konsekvensen for beskyttelsen af privatlivet. Dette afsnit indeholder en overordnet beskrivelse af en foreslået række faser for en PIA i mindre skala.

I hvert enkelt tilfælde kan man søge yderligere information i den detaljerede vejledning i PIA'en i fuld skala. Det skyldes, at disse afsnit har en mere

>

omfattende behandling af forhold, som kan være relevante for de foreliggende omstændigheder. Omfanget af en PIA i mindre skala bevirker dog, at det kan være hensigtsmæssigt at kombinere faser, integrere opgaver, eller reducere antallet af slutprodukter ved at lægge flere dokumenter sammen til ét.

De her anvendte udtryk (f.eks. 'indledende fase') er hovedsagelig af beskrivende art og er ikke i sig selv af væsentlig betydning. Virksomheder kan anvende andre udtryk, som er i overensstemmelse med deres egne interne standarder, politikker og praksis.

Følgende foreslåede faser beskrives nedenfor:

1. Indledende fase,
2. forberedende fase,
3. hørings- og analysefase(r),
4. dokumentationsfase,
5. revurderings- og revisionsfase.

1. Indledende fase

Formålet med den indledende fase er at sikre, at der etableres et fast grundlag for at gennemføre PIA'en på en effektiv og hensigtsmæssig måde. Afhængigt af projektets omfang og projektlederens erfaring med PIA'er, kan det være hensigtsmæssigt at udarbejde og vedligeholde en projektplan. Generelt anbefales det at udarbejde et projektoplæg, også selv om dette vil være ret kortfattet.

Da omstændighederne for PIA'er i mindre skala varierer så meget, indeholder håndbogen ikke nogen specifik vejledning vedrørende denne fase. Der forefindes imidlertid en nyttig tjekliste, som beskriver de opgaver, der er forbundet med den tilsvarende fase af PIA'er i fuld skala. At udføre alle opgaver, som anbefales i tjeklisten, vil være for vidtgående for et lille projekt. Ideerne kan dog være til hjælp og vil kunne anvendes på en mindre byrdefuld måde, f.eks. kombineret eller selektivt, alt efter omstændighederne.

2. Forberedende fase

Formålet med den forberedende fase er at foretage de dispositioner, som er nødvendige for at den kritiske fase 3 kan afvikles gnidningsløst. I denne fase kan virksomhederne foretage en interessentanalyse, udvikle en høringsstrategi og -plan samt etablere en konsulentgruppe for PIA *(PIA consultative group, PCG)*. Det vil være nyttigt at kigge på tjeklisten, som beskriver de opgaver, der er forbundet

med den tilsvarende fase af PIA'er i fuld skala. Det kan dog være nødvendigt at afpasse ideerne fra dette dokument, så de kan anvendes for det aktuelle projekt.

3. Hørings- og analysefase(r)

Hørings- og analysefasen bygger på det grundlag, som er tilvejebragt under de første to afsnit. Den omfatter høringer af interessenter, risikoanalyse, problemformulering og søgning efter konstruktive løsninger.

Det kan være nødvendigt at udføre nogle aktiviteter mere end én gang (f.eks. ved at have flere efterfølgende drøftelser med en central interessent). På den anden side gælder, at hvis der udarbejdes et omfattende og klart projektoplæg, og deltagerne har erfaring, eller problemstillingerne er relativt simple, så kan det lade sig gøre at gennemføre processen i et ret hurtigt tempo.

Det væsentligste slutprodukt er et dokument (f.eks. en beskrivelse af problemområder vedrørende beskyttelsen af privatlivet eller en rapport over udfaldet af møder), som gør det muligt at meddele resultaterne til de involverede parter.

Der forefindes også en nyttig tjekliste, som beskriver de opgaver, der er forbundet med den tilsvarende fase af PIA'er i fuld skala. Det kan dog være nødvendigt at afpasse ideerne fra dette dokument, så de kan anvendes for det aktuelle projekt.

4. Dokumentationsfase

Formålet med dokumentationsfasen er at dokumentere processen og udfaldet heraf. Slutproduktet er en PIA-rapport. Afhængigt af sammenhængen kan dette være et relativt kort 'notat til arkiv' med kopi til relevante parter, men omstændighederne kan dog berettige et mere omhyggeligt udarbejdet dokument.

5. Revurderings- og revisionsfase

Formålet med dette afsnit er at sikre, at de designelementer, der fremkommer som resultat af PIA'en, gennemføres og er effektive. Slutproduktet er en revurderingsrapport. Igen gælder det, at et 'notat til arkiv', hvor kopi er fordelt til relevante parter, kan være tilstrækkeligt til at efterkomme dette krav. I andre tilfælde kan en væsentlig større investering være berettiget.

Kapitel V - Appendiksliste >

Håndbog i privatlivsimplikationsanalyse refererer til nedenstående appendiks, der er vedlagt håndbogen i separate dokumenter:

Appendiks 1: Screeningsspørgsmål til udarbejdelse af PIA i fuld skala
Appendiks 2: Screeningsspørgsmål til udarbejdelse af PIA i mindre skala
Appendiks 3: Kriterier for kontrol af overensstemmelse med lovgivning
Appendiks 4: Problem-identificerende spørgsmål vedrørende privatlivets fred
Appendiks 5: Risikoanalyse af implikationer for privatlivets fred
Appendiks 6: Struktur på privatlivsimplikations-rapporten
Appendiks 7: Privatlivsfremmende teknologier