PIA-screening

Vejledningsmateriale marts 2010

>

Vejledning i PIA-screening

Udarbejdet af:
IT- og Telestyrelsen

IT- & Telestyrelsen
Holsteinsgade 63
2100 København Ø

Telefon: 3545 0000
Fax: 3545 0010

Indholdsfortegnelse

>

Hvad er en Privacy Impact Assessment (PIA) analyse? >

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 privacy impact assessment, forkortet PIA.

En PIA er en proces, som sætter organisationer i stand til at forudse risici, 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 kan umiddelbart virke som en forhindring på vejen til det nye it-system. Men i bund og grund handler en PIA blot om, at man allerede fra projektets begyndelse udviser det fornødne hensyn til borgeren. Jo mere behandlingen af personfølsomme oplysninger digitaliseres, desto større bliver risikoen for, at der kan forekomme uhensigtsmæssige læk af data. Informationsteknologien rummer fantastiske muligheder for at forbedre den offentlige service, men dette potentiale kan kun realiseres, hvis borgerne nærer tillid til de anvendte it–systemer.

For hver gang der forekommer uheldige læk af personfølsomme oplysninger undermineres denne tillid. En PIA skal derfor ses som et effektivt værktøj, der skal ruste systemejer og andre relevante beslutningstagere til at designe it-løsninger, som sikrer en sund omgang med persondata.

Skal – skal ikke?

>

Før man kaster sig ud i at lave en PIA, skal man først vurdere om det overhovedet er nødvendigt. Hvis systemet skal bruges til at behandle personhenførbare oplysninger bør man under alle omstændigheder overveje at foretage en PIA, og som minimum lave en kontrolanalyse af overensstemmelse med relevant lovgivning. Hvis systemet skal logge trækfugles migrationsmønstre er det derimod ganske unødvendigt at lave en PIA.

Der er også forhold, man skal være særlig opmærksom på. Persondataloven fastlægger i § 7 og § 8 en række kategorier af 'følsomme persondata', som kræver særlig agtpågivenhed. Dette er oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold, strafbare forhold, væsentlige sociale problemer og oplysninger om andre rent private forhold.

Der er også grund til særlig opmærksomhed på projekter, hvor der indgår oplysninger om personnumre. Behandling af oplysninger om personnumre giver ofte anledning til bekymring hos borgerne – og desværre har en række sager vist, at der ofte sker fejl, hvor personnumre gives til uvedkommende eller ligefrem offentliggøres på internettet. Der er andre kategorier af persondata, som også skal overvejes nøje, herunder oplysninger om økonomiske forhold og andre fortrolige data, samt data som kan muliggøre identitetstyveri.

For at opsummere: Behandler projektet personhenførbare oplysninger – eller er du i tvivl – så forsæt med PIA-screeningen for at afgøre, hvordan du bedst inddrager hensynet til privatlivsbeskyttelsen i projektet.

Screening for omfanget af PIA-analyse >

Der skelnes mellem to PIA-processer, hhv. en mindre og mere omfangsrig analyse. Før man går i gang med analysearbejdet, er det derfor oplagt at afgøre analysens omfang. For at bistå med denne vurdering kan man gennemgå følgende tjekliste.

1. Involverer løsningen flere organisationer?
2. Anvender løsningen ny teknologi til at identificere borgeren?
3. Kan løsningen vække særlig bekymring hos borgeren?
4. Anvender løsningen persondata fra flere forskellige datakilder?
5. Kræver løsningen, at der dispenseres for gældende lovmæssig beskyttelse?
6. Involverer løsningen videregivelse af personhenførbare data til tredjemand?
7. Omhandler løsningen forhold angående offentlig sikkerhed?

Såfremt der kan svares ja til bare ét eller flere af spørgsmålene, bør man overveje at foretage en PIA i fuld skala. Screeningsspørgsmål findes i det følgende afsnit, side 7.

Hvis man ikke umiddelbart kan svare ja til nogle af ovenstående spørgsmål, bør man overveje at lave en PIA i mindre skala. Screeningsspørgsmålene for, om en PIA i mindre skala er nødvendig findes i afsnittet side 11.

Screeningsspørgsmål til PIA i fuld skala >

På basis af den engelske PIA håndbog er udarbejdet 11 spørgsmål, der skal hjælpe med at afgøre, om der skal laves en PIA i fuld skala på et givent projekt. Vurderingen er en samlet vurdering af besvarelserne på alle 11 spørgsmål.

Spørgsmålene er angivet med kursiv. Vejledning til fortolkning af hvert spørgsmål er angivet som almindelig tekst.

Teknologi

(1) *Anvender projektet nye eller udvidede informationsteknologier, som har betydeligt potentiale for indskrænkning af beskyttelsen af privatlivet?*

Eksempler herpå omfatter bl.a. chipkort, mærkater til radiofrekvensidentifikation (RFID), biometriske data, teknologier til stedbestemmelse (herunder stedbestemmelse af mobiltelefoner, anvendelse af GPS-systemer og intelligente transportsystemer), visuel overvågning, digitale billed- og videooptagelser, profildata, datamining og logning af elektronisk trafik.

Identitet

(2) *Omfatter projektet nye identifikatorer, genanvendelse af eksisterende identifikatorer, eller privatlivskrænkende identifikation, autentificering af identitet eller processer til identitetsstyring?*

Eksempler på relevante projektelementer omfatter tiltag vedrørende digital signatur, identifikatorer med flere anvendelsesmuligheder, interviews og fremlæggelse af identitetsdokumenter som en del af en registreringsordning samt privatlivskrænkende identifikatorer i form af biometridata. Alle ordninger af denne art har potentielt stor konsekvens for beskyttelsen af privatlivet; de kan give anledning til bekymring i offentligheden og indebærer således en risiko for projektet.

>

(3) *Kan projektet forårsage, at anonymitet og pseudonymitet nægtes, eller at transaktioner, som tidligere kunne gennemføres anonymt eller pseudonymt, ændres til identificerbare transaktioner?*

Mange myndigheder kan ikke varetage deres opgaver effektivt uden at have adgang til klientens identitet. Imidlertid kræver mange andre ingen identitet. En vigtig overvejelse er, om det skal være muligt at have kontakt med virksomheden uden at opgive sin identitet.

Flere forskellige virksomheder

(4) *Omfatter projektet flere forskellige virksomheder, enten i form af statslige styrelser (f.eks. ved fælles statslige initiativer) eller virksomheder i privatsektoren (f.eks. som outsourcede tjenesteudbydere eller forretningspartnere)?*

Projekter af denne art omfatter ofte opsplitning af eksterne datalagre (siloer), der indeholder persondata og identiteter. Det kan give anledning til spørgsmål om, hvordan lovgivningen om beskyttelse af privatlivet kan overholdes. Opsplitningen kan være ønskelig med henblik på at opdage og forebygge svindel og i nogle tilfælde af hensyn til en effektiv forretningsgang. Datasiloer og identitetssiloer har imidlertid eksisteret i flere år og har i mange tilfælde ydet effektiv beskyttelse af privatlivet. Man må derfor være ekstra omhyggelig i relation til udarbejdelse af et forretningsgrundlag, som berettiger indgreb i beskyttelsen af privatlivet ved projekter, som omfatter flere forskellige virksomheder. Beskyttelsesforanstaltninger af kompenserende art bør overvejes.

Data

(5) *Omfatter projektet ny eller væsentlig ændret behandling af persondata, som giver anledning til særlig betænkelighed hos privatpersoner?*

Persondataloven fastlægger i § 7 og § 8 en række kategorier af 'følsomme persondata', som kræver særlig agtpågivenhed. Dette er oplysninger om racemæssig eller etnisk baggrund, politisk, religiøs

>

eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold og oplysninger om helbredsmæssige og seksuelle forhold, strafbare forhold, væsentlige sociale problemer og oplysninger om andre rent private forhold.

Der er også grund til særlig opmærksomhed på projekter, hvor der indgår oplysninger om personnumre. Behandling af oplysninger om personnumre giver ofte anledning til bekymring hos borgerne – og desværre har en række sager vist, at der ofte sker fejl, hvor personnumre gives til uvedkommende eller ligefrem offentliggøres på internettet. Der er andre kategorier af persondata, som også skal overvejes nøje, herunder oplysninger om økonomiske forhold og andre fortrolige data, samt data som kan muliggøre identitetstyveri.

(6) Omfatter projektet ny eller væsentlig ændret behandling af en større mængde persondata vedrørende hver privatperson i databasen?

Eksempler herpå er intensiv databehandling som f.eks. socialforvaltning, patient og sundhedspleje, forbrugerkredit og forbrugermarketing baseret på intensive profiler.

(7) Omfatter projektet ny eller væsentlig ændret behandling af persondata vedrørende et stort antal privatpersoner?

Al databehandling af denne art er fordelagtig for virksomheder og privatpersoner, som søger at finde frem til folk eller at opbygge/udbygge profiler af disse.

(8) *Omfatter projektet ny eller væsentlig ændret sammenkædning, krydshenvisning eller tilpasning af persondata fra flere kilder?*

Når et projekt medfører sammenkædning af personoplysninger, der ikke før er har været sammenstillet eller lagret samme sted, skal man være speciel opmærksom. Der kan opstå spørgsmål i relation til graden af sammenføring, datakvalitet samt opbevaring af data over længere tid end på meget kort sigt.

>

Fritagelse og undtagelser

(9) *Vedrører projektet databehandling, som helt eller delvist er fritaget fra lovgivningsmæssig beskyttelse af privatlivet?*

Eksempler herpå er pressens registre, herunder redaktionelle informationsdatabaser samt andre områder, hvor beskyttelsen af privatlivet i nogen eller fuldt omfang er ophævet ved fritagelse eller undtagelse i henhold til lovgivningen.

(10) *Omfatter projektets motivering væsentlige tiltag til foranstaltninger vedrørende offentlig sikkerhed?*

Foranstaltninger, som træffes af hensyn til kritisk infrastruktur og befolkningens fysiske sikkerhed, har i reglen en væsentlig konsekvens for beskyttelsen af privatlivet

(11) *Omfatter projektet systematisk videregivelse af persondata til, eller adgang for, tredjemand, som ikke er underlagt tilsvarende regulering af beskyttelsen af privatlivet?*

En sådan videregivelse kan hidrøre fra forskellige mekanismer, f.eks. salg, udveksling, ubeskyttet offentliggørelse i papirform eller som elektronisk adgang, eller fra outsourcing af elementer i databehandlingen til underleverandører.

Tredjeparter kan være undtaget fra bestemmelser om beskyttelsen af privatlivet, da de ikke er underlagt bestemmelserne i persondataloven eller andre lovbestemmelser, f.eks. hvis de befinder sig under udenlandsk jurisdiktion.

Hvis man kan svare ja til flere af ovenstående spørgsmål i stort omfang bør man udarbejde en PIA i fuld skala. Kan man svare ja til et eller flere af spørgsmålene i mindre omfang bør man som minimum lave en compliance-analyse i forhold til kontrol af overensstemmelse med relevant lovgivning. IT- og Telestyrelsen har offentliggjort en betaudgave af en PIA håndbog, som kan downloades på http://www.itst.dk/publikationer.

Screeningsspørgsmål til PIA i mindre skala >

På basis af den engelske PIA håndbog er udarbejdet 15 spørgsmål, der skal hjælpe med at afgøre, om der skal laves en PIA i mindre skala på et givent projekt. Vurderingen er en samlet vurdering af besvarelserne på alle 15 spørgsmål.

Spørgsmålene er angivet med kursiv. Vejledning til fortolkning af hvert spørgsmål er angivet som almindelig tekst.

Teknologi

(1) *Omfatter projektet nye eller i sig selv privatlivskrænkende teknologier?*

Eksempler på *privatlivskrænkende* teknologier er chipkort, mærkater til radiofrekvensidentifikation (RFID), biometriske data, teknologier til stedbestemmelse (herunder stedbestemmelse af mobiltelefoner, anvendelse af GPS-systemer og intelligente transportsystemer), visuel overvågning, digitale billed- og videooptagelser, profildata, datamining og logning af elektronisk trafik. Teknologier, der i sig selv er privatlivskrænkende, og teknologier, der er nye og lyder truende, kan vække betydelig bekymring i offentligheden og repræsenterer således en risiko for projektet.

For at besvare dette spørgsmål, må det bl.a. overvejes:

- om alle de informationsteknologier, som skal anvendes i projektet, allerede er godt kendt af offentligheden,
- om konsekvensen for beskyttelsen af privatlivet er velkendt i virksomheden og offentligheden,
- om der foreligger indarbejdede foranstaltninger, der eliminerer negative konsekvenser for beskyttelsen af privatlivet eller i det mindste reducerer disse til et niveau, der er tilfredsstillende for de parter, hvis privatliv berøres, og
- om alle disse foranstaltninger bruges i udformningen af projektet.

>

Berettigelse

(2) *Er berettigelsen af den nye databehandling uklar eller ikke offentliggjort?*

Generelt set kan privatpersoner i langt højere grad acceptere foranstaltninger, som i nogen grad er krænkende for beskyttelsen af privatlivet, hvis tabet afbalanceres af andre goder, enten for dem selv eller for samfundet som et hele. På den anden side gælder det, at vage påstande om, at foranstaltningerne er nødvendige 'af sikkerhedsgrunde' eller 'for at undgå svindel', har meget mindre chance for at dæmpe offentlig bekymring.

Identitet

(3) *Omfatter projektet yderligere anvendelse af en eksisterende identifikator?*

(4) *Omfatter projektet anvendelse af en ny identifikator til flere forskellige formål?*

(5) *Omfatter projektet nye eller væsentligt ændrede krav til autentificering af identitet, som rejser spørgsmål om integritetskrænkelse?*

Offentligheden forstår, at en identifikator sætter en virksomhed i stand til at samle data om en privatperson, og at identifikatorer, som anvendes til flere forskellige formål, gør samkøring af data mulig. Man er også bevidst om de stadig mere byrdefulde registreringsprocesser og dokumentationskrav, som forlanges af virksomhederne i de senere år. Fra projektlederens synsvinkel er dette et advarselssignal om mulige risici for beskyttelsen af privatlivet.

Data

(6) *Vil projektet resultere i behandling af en væsentlig mængde nye data om hver person eller væsentlig ændring i eksisterende datalagre?*

>

(7) *Vil projektet resultere i behandling af nye data om et væsentligt antal mennesker eller væsentlig ændring i befolkningsmæssig dækning?*

(8) *Omfatter projektet ny sammenkædning af persondata med data i andre samlinger eller væsentlig ændring i sammenkædningen af data?*

Opmærksomheden omkring et projekt er større, hvis data overføres uden for deres normale sammenhæng. Udtrykket 'sammenkædning' omfatter mange slags aktiviteter, som f.eks. dataoverførsel, lagring af identifikatorer, som anvendes i andre systemer for at lette fremtidig søgning i aktuelle registerindhold, funktioner med dataopslag fra anden lokation (f.eks. til støtte for såkaldt 'frontend-verifikation'), og sammenstilling af persondata fra flere kilder.

Databehandling

(9) *Omfatter projektet ny eller ændret politik eller praksis for dataindsamling, som kan være uklar eller privatlivskrænkende?*

(10) *Omfatter projektet nye eller ændrede processer for kvalitetssikring af data og datastandarder, som kan være uklare eller utilfredsstillende?*

(11) *Omfatter projektet nye eller ændrede forhold om datasikkerhed, som kan være uklare eller utilfredsstillende?*

(12) *Omfatter projektet nye eller ændrede forhold om adgang til eller videregivelse af data, som kan være uklare eller lemfældige?*

(13) *Omfatter projektet nye eller ændrede forhold om lagring af data, som kan være uklare eller vidtgående?*

(14) *Omfatter projektet ændring af mediet for videregivelse af offentlig tilgængelig information, så der bliver lettere adgang til data end før?*

>

Fritagelse

(15) *Vil projektet give anledning til ny eller ændret databehandling, som på nogen måde er fritaget fra lovgivningsmæssig beskyttelse af privatlivet?*

Som det er tilfældet for en PIA i fuld skala, kan man komme til at overse risici, medmindre spørgsmålene betragtes ud fra interessegruppernes forskellige synsvinkler. På samme måde kan det i relation til de privatpersoner, som berøres af projektet, være utilstrækkeligt at beskæftige sig med borgere eller beboere i almindelighed eller befolkningen som helhed. For at sikre forståelse hos de forskellige segmenter af befolkningen, som har interesse i projektet eller berøres heraf, kan det være nødvendigt at detaljere interessentanalysen i det forberedende trin. Der er ofte forskellige konsekvenser eller virkninger for forskellige dele af befolkningen.

Hvis man kan svare ja til flere af ovenstående spørgsmål i stort omfang bør man udarbejde en PIA i mindre skala. Kan man svare ja til et eller flere af spørgsmålene i mindre omfang bør man som minimum lave en compliance-analyse i forhold til kontrol af overensstemmelse med relevant lovgivning.

IT- og Telestyrelsen har offentliggjort en betaudgave af en PIA håndbog, som kan downloades på http://www.itst.dk/publikationer.

Screeningsprocessen output >

Screeningsprocessen sætter fokus på de forskellige aspekter ved et projekt, der kan medføre implikationer for beskyttelsen af privatlivets fred.

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.

For at udføre screeningen kan det være nødvendigt at indhente yderligere information og eksempelvis lave en foreløbig interessentanalyse.

Outputtet af screeningsprocessen er et kort notat, der ud fra besvarelsen af spørgsmålene kort besvarer, om projektet behandler personhenførbare informationer og om det på dette grundlag er nødvendigt at:

- Gennemføre en PIA i fuld skala, eller
- gennemføre en PIA mindre skala, og/eller
- gennemføre en compliance-analyse i forhold til relevant lovgivning, i særdeleshed persondataloven

Besvarelsen af screeningsprocessens spørgsmål kan også tjene som gode guidelines for, hvilke områder af projektet og systemet, det er nødvendigt at tage hul på først.

IT- og Telestyrelsen har offentliggjort en betaudgave af en PIA håndbog, som kan downloades på http://www.itst.dk/publikationer.