Screeningsspørgsmål til udarbejdelse af PIA i fuld skala

Appendiks 1
Håndbog i:
Privatlivsimplikationsanalyse

IT- og Telestyrelsen

INDHOLDSFORTEGNELSE

Appendiks 1: Screeningsspørgsmål til PIA, fuld skala

SCREENINGSSPØRGSMÅL TIL PIA I FULD SKALA

Den engelske PIA håndbog har 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.