Problem-identificerende spørgsmål vedrørende privatlivets fred

Appendiks 4
Håndbog i:
Privatlivsimplikationsanalyse

IT- og Telestyrelsen

INDHOLDSFORTEGNELSE

BRUG AF PROBLEMIDENTIFICERENDE SPØRGSMÅL

Når et givent projekt, løsning eller koncepts processer gennemgås med henblik på at identificere mulige problemområder relateret til privatlivets fred, kan det være en hjælp at stille sig selv konkrete, operationelle spørgsmål til de forskellige områder.

Med udgangspunkt i den canadiske PIA er udarbejdet nedenstående liste af spørgsmål til hvert område relateret til brugen af personoplysninger i PIA'en. Strukturen på spørgsmålene er tilpasset danske forhold, og PIA'ens generelle struktur.

Som tommelfingerregel kan man sige, at et område skal inddrages, hvis man kan svare ja til et spørgsmål indenfor området. Et positivt svar indikerer, at man har identificeret et område, der har betydning for hensynet til privatlivets fred (det være sig både positivt og negativt), og derfor bør indgå i nærmere analyse. Herudover bør man naturligvis analysere et område nærmere, såfremt at beskrivelsen af personoplysningerne er alarmerende.

Informationens karakter

1. Hvilken information indsamles, bruges, spredes eller vedligeholdes i systemet?
2. Hvad er systemets kilder til information (fx offentlige eller private databaser)?
3. Hvorfor indsamles, bruges, spredes eller vedligeholdes information i systemet?
4. Er det nødvendigt for sagsbehandlingen at indsamle personlige oplysninger som under og efter indsamlingen kan henføres til en person?
5. Er alle indsamlede personoplysninger nødvendige for formålet? Begrund.
6. Skal der indsamles yderligere information?
7. Hvordan indsamles information?
8. Hvordan kontrolleres, at information er korrekt?
9. Hvilken lovhjemmel findes til indsamling af information?
10. Er oplysningerne anonymiserede, når de anvendes til planlægning, prognoser, forskning og/eller evalueringsformål?

Brug af information

1. Beskriv brugen
2. Bevarer personen, som oplysningerne vedrører, kontrol med hvad oplysningerne bruges til?
3. Hvilke værktøjer bruges til at analysere data, og hvilken type data produceres i forbindelse hermed?
4. Hvis systemet bruger kommercielle eller offentlige data – beskriv hvorfor og hvordan data bruges?
5. Overvejes sekundære anvendelser for indsamlede oplysninger? Hvis ja, beskriv det.

6. Er det blevet overvejet, om der er særlige muligheder for at beskytte borgerens identitet under sagsbehandlingen?
7. Kunne sagsbehandlingen finde sted uden kendskab til, hvilken borger der sagsbehandles?
8. Bruges personoplysningerne til et formål, hvortil oplysningerne kan udleveres til en anden institution eller myndighed?
9. Når data samkøres, er det i overensstemmelse med det erklærede formål, som personoplysningerne er indsamlet til?

Opbevaring af information

1. Hvor længe opbevares information?
2. Sker opbevaring med lovmæssig hjemmel?
3. Er rammerne for opbevaring og sletning af personoplysninger fastlagt? Hvis ja, specificer.
4. Slettes personoplysningerne når de ikke længere er relevante?
5. Er alle muligheder for at minimere den rutinemæssige (automatiserede) indsamling af personoplysninger overvejet?
6. Er der udarbejdet planer for revision, overholdelse og håndhævelse af mekanismer for det tværoffentlige projekt?

Intern deling og offentliggørelse

1. Med hvem deles information internt / samme myndighed – og hvorfor – med hvilket formål?
2. Hvordan offentliggøres eller transmitteres informationen?
3. Er personoplysninger videregivet med samtykke fra den enkelte?
4. Offentliggøres person-id, såsom CPR-nummer?
5. Vil personoplysninger blive behandlet, videregivet eller opbevaret uden for Danmark?
6. Såfremt at personoplysninger ikke offentliggøres ud fra samtykke, findes der alternativt lovmæssig hjemmel til videregivelse?
7. Er der etableret en klar relation mellem de personoplysninger, der skal indsamles og projektets funktionelle og driftsmæssige krav?
8. Er der udarbejdet planer for fuld offentliggørelse af de formål, hvortil personoplysninger indsamles?
9. Er oplysningerne anonymiserede, når de anvendes til planlægning, prognoser, forskning og/eller evalueringsformål?
10. Kræver samkørsel af data en anmeldelse til Datatilsynet?

Ekstern deling og offentliggørelse

1. Med hvem deles information eksternt – og hvorfor – med hvilket formål?
2. Er deling foreneligt med oprindeligt formål, og er de dokumenteret mellem myndigheder?
3. Hvordan deles information? Hvordan sikres information under deling?
4. Er personoplysninger videregivet/delt med samtykke fra den enkelte?
5. Offentliggøres personid, såsom CPR-nummer?

6. Vil personoplysninger blive behandlet, videregivet eller opbevaret uden for Danmark?
7. Såfremt at personoplysninger ikke offentliggøres ud fra samtykke, findes der alternativ lovmæssig hjemmel til videregivelse?
8. Udføres en PIA af hver myndighed, der deler informationerne?
9. Er kontrol med personoplysninger blevet fastlagt for det tværoffentlige projekt, herunder:
    a. Er myndighedsansvaret, herunder ansvarlige personer hos den enkelte myndighed, identificeret og fastlagt for alle involverede organer og er der udarbejdet aftale herom?
    b. Er der for hver myndighed opsat målbare succeskriterier for deltagelse i projektet?
    c. Når en myndighed og/eller den private sektor ikke er omfattet af lov relateret til hensynet til privatlivets fred, er der så i stedet etableret en aftale, der sikrer de samme rettigheder som f.eks. persondataloven?
    d. Forsynes hver myndighed med resultaterne af regelmæssig revision og kontrol af personoplysninger i det tværoffentlige projekt?
10. Er bestemmelser/lovgrundlag mellem myndigheder afstemt og er undtagelser hertil identificeret og afstemt?
11. Er der anmodet om udtalelser fra juridisk eller politisk rådgivning om:
    a. krav til hensynet til privatlivets fred i hver myndighed vedrørende indsamling, brug, videregivelse, lagring og bortskaffelse af personoplysninger i forhold til projektet?
    b. eventuelle lovmæssige konflikter mellem myndigheder, samt hvordan konflikterne bliver løst?
    c. eventuelle krav til overgivelse af dataansvar i det tværoffentlige projekt, herunder fra den myndighed, der indsamler oplysninger, til at videregive eller opbevare personlige oplysninger, på tværs af myndigheder?
    d. behov for at ændre eller begrænse måden personoplysninger indsamles, anvendes eller videregives, som tilladt af projektets regler omkring privatlivshensyn, med henblik på at levere service tværoffentligt?
12. Har hver myndighed identificeret alle krav til beskyttelse af personoplysninger og er modstridende krav blevet løst?
13. Er de centrale aktører blevet forsynet med en lejlighed til at udtale sig om implikationerne i projektet?
14. Er Datatilsynets synspunkter om det foreslåede tværoffentlige projekt relevante og kendte? Hvis ja, angiv nærmere detaljer.
15. Når data udleveres til andre myndigheder er det så vurderet, om data fortsat skal kunne henføres til den pågældende borger?
16. Kræver det tværoffentlige projekt indsamling af flere personoplysninger end tidligere indsamlet af hver myndighed?
17. Vil enkeltpersoner blive overvåget med henblik på kvalitetssikring eller sikkerhed, og hvis ja, indsamles personoplysninger i forbindelse hermed?
18. Træffes foranstaltninger til at sikre offentlighedens tillid til overholdelse af privatlivets fred i projektet, når personoplysninger, som enkeltpersoner forventes at finde følsomme, indsamles?

Appendiks 4: Problemidentificerende spørgsmål

Samtykke

1. Er der indhentet samtykke før indsamling af information?
2. Kan individet nægte / undlade at give samtykke?
3. Kan individet give delvist samtykke – hvis ja, hvordan?
4. Er der standarder og mekanismer etableret, som sikrer, at den enkelte har mulighed for at tilbagekalde et samtykke?
5. Gives der varsel til personen, hos hvem personoplysningerne indsamles, på indsamlingstidspunktet, om det specifikke formål for indsamlingen, den indsamlende myndighed og angivelse af en officiel kontaktperson?
6. Hvordan indhentes samtykke?
7. Kræver samtykke en aktiv handling fra den pågældende person?
8. Eksisterer der tværoffentlige standarder, der kan administrere samtykkekrav med henblik på:
    a. At træffe afgørelse om, hvorvidt den enkelte har kapacitet til at give samtykke på baggrund af alder eller kapacitet?
    b. Anerkendelse af personer, der er bemyndiget til at træffe beslutninger på vegne af en inkapabel umyndiggjort person eller en mindreårig?
9. Er de foreslåede samtykkebestemmelser i overensstemmelse med gældende love og standarder i sammenlignelige områder i den offentlige eller den private sektor?
10. Hvis personoplysninger, der tidligere er indsamlet, skal bruges til et formål, der ikke tidligere er identificeret, er samtykke så påkrævet?

Adgang, godtgørelse og korrektion

1. Hvad er procedure for individet til at få adgang til egen information?
2. Hvad er procedure for at korrekte ukorrekt information?
3. Hvordan gøres individer opmærksom på procedure for ukorrekt information?
4. Hvis individet ikke formelt kan godtgøres, findes der andre alternativer?
5. Er der taget skridt til at sikre, at personoplysninger er korrekte, fuldstændige og opdaterede?
6. Angives den seneste opdatering af personoplysninger under registreringen af personoplysninger
7. Angives kilden til de oplysninger, der anvendes til at foretage ændringer?
8. Er der en procedure, automatisk eller manuel, til at give meddelelser om rettelser til tredjepart, til hvem personoplysninger tidligere er blevet videregivet?
9. Beholdes anmodninger om korrektioner eller beslutninger om ikke at berigtige oplysninger?
10. Er der en klart defineret proces for, hvornår en person kan få adgang til, vurdere, diskutere eller bestride rigtigheden af sine personoplysninger? Hvis ja, beskriv denne.
11. Er der udarbejdet planer for transparens i informationssystemer, således at enkeltpersoner informeres om, hvordan deres personoplysninger indsamles, anvendes og videregives?
12. Er klageproceduren for projektet, eller det system projektet omhandler, i overensstemmelse med krav i lovgivningen?

13. Er der etableret en procedure for at logge og regelmæssigt revidere art, hyppighed og løsning af klager?
14. Er systemet designet til at sikre, at en borger kan få adgang til hans/hendes personoplysninger, formålet med databehandlingen m.m., jf. persondatalovens §31?
15. Er systemet designet således, at borgeren kan få adgang til, i hvilken sagsbehandling hans/hendes personoplysninger er blevet brugt?
16. Er systemet designet til at sikre, at en person får meddelelse om, at en rettelse til hans/hendes oplysninger er blevet foretaget?

Teknisk adgang og sikkerhed

1. Er der udført en risikovurdering for projektet?
2. Hvilke procedurer findes for brugeradgang (autorisation og autentifikation) og hvordan er de dokumenteret?
3. Vil underleverandører have adgang til systemet?
4. Hvilken privacy træning er iværksat af brugere?
5. Hvilke procedurer for revision og tekniske foranstaltninger til forhindre misbrug af data er iværksat?
6. Beskyttes personoplysningerne i overensstemmelse med teknologiens aktuelle stadium?
7. Er sikkerhedsprocedurer for indsamling, indberetning, opbevaring, adgang og bortskaffelse af personoplysninger dokumenteret?
8. Er projektets deltagere uddannet i varetagelsen af beskyttelse af personoplysninger, og er de bekendt med de relevante politikker vedrørende brud på sikkerhed eller fortrolighed?
9. Er der etableret kontroller for processer, der kan give tilladelse til at ændre, tilføje eller slette personoplysninger fra registre?
10. Er systemet designet således, at adgang og ændringer af personoplysninger kan auditeres ved brug af dato og brugeridentifikation?
11. Er brugerkonti, adgangsrettigheder og sikkerhedstilladelser formelt kontrolleret af et system eller en proces?
12. Er adgangsrettigheder til personoplysninger udleveret til brugerne på en "need-to-know basis" i overensstemmelse med indsamlingens erklærede formål?
13. Er sikkerhedsforanstaltninger i overensstemmelse med følsomheden af de registrerede oplysninger?
14. Er der nødplaner og procedurer til at identificere og reagere på sikkerhedsbrud, samt fejlmæssige offentliggørelser af personinformationer?
15. Er der etableret procedurer til at kommunikere sikkerhedsbrug eller fejlbehæftede offentliggørelser til den pågældende person, myndigheder og relevante projektledere?
16. Er der en plan for kvalitetssikring og revision af projektet, herunder af sikkerhedsforanstaltninger?
17. Har alle projektets deltagere kendskab til en persons ret til adgang og til proces for klager?
18. Er der udviklet eller planlagt procedurer for, hvordan man kan anmode om korrektion af personoplysninger?

19. Er det overvejet, hvordan enkeltpersoner rutinemæssigt og eventuelt automatiseret gives adgang til deres personoplysninger?
20. Er det relevant at forsyne personer med adgang til deres personoplysninger i et alternativt format? Hvis ja, er dette etableret?
21. Er der mulighed for, at en borger kan få forklaret indholdet af hans/hendes personoplysninger, f.eks. sundhedsdata?

Teknologi og organisation

1. Hvilke struktureret metode blev brug til udvikling af systemet?
2. Hvordan blev data integritet og sikkerhed analyseret som del af udviklingen?
3. Hvilke designvalg blev gjort for at sikre privatlivets fred?
4. Er der anvendt privacy enhancing technologies (PET)?
5. Bruges ID-nøgler, såsom CPR-nummer, til at forbinde på tværs af flere databaser?

Overordnede spørgsmål til projektet

1. Vil resultaterne af en PIA blive gjort tilgængelige for offentligheden? Hvis nej, hvorfor ikke? Hvis ja, hvordan?
2. Er politikker og praksis i forbindelse med projektets styring og håndtering af personoplysninger tilgængelige for offentligheden?
3. Er der en kommunikationsplan med henblik på forklaring til offentligheden, hvordan personoplysninger vil blive forvaltet og beskyttet?
4. Er der en klart defineret og nem proces for privatpersoner til at få adgang til sådanne oplysninger og/eller kommunikere med passende personer med hensyn til politik og praksis, vedrørende forvaltning og beskyttelse af personlige oplysninger?
5. Er centrale aktører forsynet med en lejlighed til at udtale sig om beskyttelse af privatlivets fred i projektet?
6. Vil der finde en offentlig høring finde sted omkring privatlivshensyn i projektet? Hvorfor ikke?
7. Vil leverandører til et projekt få adgang til PIA'en, så tilbud, udvikling, implementering og service kan gøres i overensstemmelse med den PIA, som projektet ønsker?