Struktur på privatlivs-implikationsrapporten

Appendiks 6
Håndbog i:
Privatlivsimplikationsanalyse

IT- og Telestyrelsen

Appendiks 6: Struktur på rapport

INDHOLDSFORTEGNELSE

Appendiks 6: Struktur på rapport

STRUKTUR PÅ RAPPORT OVER PRIVATLIVSIMPLIKATIONSANALYSEN

Udarbejdelse af PIA-rapporten er fjerde fase i processen med udarbejdelse af en privatlivsimplikationsanalyse. PIA-rapportens udarbejdelse har en række formål:

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

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.

Introduktion

Dette afsnit introducerer systemet eller konceptet og beskriver væsentlig kontekstuelle faktorer. Afsnittet begrunder udarbejdelse af PIA, herunder formål

med PIA'en. Dele af spørgsmål fra screeningsprocessen kan med fordel gengives under begrundelse af PIA.

Analyse

Analyseafsnittet beskriver brugen af personoplysninger i det pågældende system eller koncept og identificerer privatlivsimplikationer i forbindelse hermed.

Det kan være en fordel struktureret at gennemgå typer af personoplysninger i løsningen samt de processer og funktionsområder i løsningen, der involverer brugen af denne type information. For at sikre, at relevante processer behandles, kan en livscyklus betragtning for informationsanvendelse bruges som inspiration.

Med udgangspunkt i den amerikanske skabelon til en PIA, udarbejdet af Homeland Security (XX LINK), samt den canadiske analyseskabelon til en PIA, kan analysen inspireres af følgende 10 områder:

1. Typer af personoplysninger
    a. Hvilke typer personoplysninger indsamles, bruges, spredes eller vedligeholdes i systemet, og hvor kommer informationen fra?
    b. Hvorfor indsamles, bruges, spredes eller vedligeholdes personoplysninger i systemet?
    c. Hvordan indsamles personoplysninger?
    d. Hvordan kontrolleres, at personoplysninger er korrekt?
    e. Hvilken lovhjemmel findes til indsamling af personoplysninger?

2. Brug af personoplysninger
    a. Beskriv anvendelse og opdatering
    b. Bruges værktøjer til at analysere personoplysninger og hvilken type data produceres i forbindelse hermed?
    c. Hvis systemet bruger personoplysninger, der er anskaffet kommercielt eller fra den offentlige forvaltning – beskriv da hvorfor og hvordan data bruges?

3. Opbevaring
    a. Hvor længe opbevares personoplysninger?
    b. Hvilken lovhjemmel findes til opbevaring af personoplysninger?

4. Intern deling og offentliggørelse
    a. Med hvem deles personoplysninger internt / samme myndighed – og hvorfor – med hvilket formål?
    b. Hvordan offentliggøres og/eller transmitteres personoplysningerne?

5. Ekstern deling og offentliggørelse
    a. Med hvem deles personoplysningerne eksternt – og hvorfor – med hvilket formål?
    b. Er deling kommensurabelt med oprindeligt formål?
    c. Hvordan transmitteres personoplysninger? Hvordan sikres personoplysninger under deling?

6. Samtykke
    a. Er der indhentet samtykke før indsamling af personoplysninger?
    b. Kan individet nægte / undlade at give samtykke?
    c. Kan individet give delvist samtykke – hvis ja, hvordan?

7. Adgang, godtgørelse og korrektion
    a. Hvordan får individet adgang til personoplysninger om sig selv?
    b. Hvad er proceduren for at rette ukorrekte personoplysninger?
    c. Hvordan gøres individer opmærksom på proceduren til at rette ukorrekte personoplysninger?
    d. Hvis individet ikke formelt kan godtgøres, findes der andre alternativer?

8. Teknisk adgang og sikkerhed
    a. Hvilke procedurer findes for brugeradgang (autorisation og autentifikation) og hvordan er de dokumenteret?
    b. Vil underleverandører have adgang til systemet?
    c. Hvilken privacy træning er iværksat af brugere?
    d. Hvilke procedurer for revision og tekniske foranstaltninger til forhindre misbrug af personoplysninger er iværksat?

9. Teknologi og organisering
    a. Hvilken struktureret metode blev brug til udvikling af systemet?
    b. Hvordan blev data integritet og sikkerhed analyseret som del af udviklingen?
    c. Hvilke design valg blev gjort for at sikre privatlivets fred?

Der skal understreges, at ethvert PIA-projekt har sine specifikke udfordringer, som skal vægtes. Ovenstående generiske områder bør derfor tilpasses PIA og løsningens specifikke kontekst.

Vurdering

Vurderingsafsnittet i PIA-rapporten kan med fordel tage afsæt i en risikovurdering, se appendiks 5.

Appendiks 6: Struktur på rapport

Afsnittet præsenterer en samlet vurdering af konceptet eller løsningen, der kvalificeres ved kort og præcist at redegøre for følgende 6 punkter:

1. På hvilke områder og måde kan projektet medføre en mindsket privatlivsbeskyttelse?
2. På hvilke områder kan en forringelse af privatlivsbeskyttelsen ikke undgås – og hvad er det forretningsgrundlag eller samfundshensyn, der berettiger forringelsen af privatlivet?
3. På hvilke områder kan løsningens design ændres, således at konsekvenserne afbødes eller formindskes?
4. Hvilke elementer er allerede inddraget i løsningen til at mindske krænkelser af privatlivet?
5. Hvilke elementer kan yderligere inddrages i løsningen til yderligere at mindske krænkelser af privatlivet – og vil dette føre til en ændret risikovurdering?
6. Kan offentligheden acceptere løsningen i sin nuværende udformning?
7. Kan offentligheden acceptere løsningen hvis yderligere elementer til mindskelse af privatlivets fred inddrages?

Bilag

Der kan være behov for at vedlægge bilag til PIA-rapporten for at understøtte rapportens konklusioner og proces.

Mulige bilag er:

- Et resumé af de høringsprocesser, som er foretaget.
- Kontaktdetaljer for virksomheder og privatpersoner, som har været genstand for høring.
- Det eller de projektoplæg, som har været forelagt høringsparter.
- PIA-projektplan.
- Spørgsmålsregisteret og/eller rapporten om designelementer vedrørende beskyttelsen af privatlivet.
- Henvisninger til relevante love, regelsæt og retningslinjer.

Såfremt der iværksættes en dybdegående kontrol af konceptet eller løsningens 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.

Appendiks 6: Struktur på rapport

Forslag til struktur (indholdsfortegnelse)

Med udgangspunkt i foregående afsnit, kan en PIA-rapport tage udgangspunkt i følgende forslag til indholdsfortegnelse:

1. Resumé
   - kort oprids af kontekst for PIA, samt samlet vurdering fra afsnit 6.4

2. Indholdsfortegnelse

3. Indledning
   - herunder definitioner på fagtermer i rapporten

4. Introduktion til projektet, løsningen eller konceptet
   4.1. Kvalificering af privatlivsimplikationsanalysen
   4.2. Formål og anvendelse af privatlivsimplikationsanalysen
   4.3. Kommunikation vedrørende privatlivsimplikationsanalysen

5. Brug af personoplysninger
   5.1. Informationens karakter
   5.2. Brug af information
   5.3. Opbevaring
   5.4. Intern deling og offentliggørelse
   5.5. Ekstern deling og offentliggørelse
   5.6. Samtykke
   5.7. Adgang, godtgørelse og korrektion
   5.8. Teknisk adgang og sikkerhed
   5.9. Teknologi og organisering

6. Implikationer for beskyttelsen af privatlivets fred
   6.1. Metode for risikovurdering
   6.2. Risikovurdering
   6.3. Tiltag til minimering af risici
   6.4. Samlet vurdering af implikationer for beskyttelsen af privatlivets fred

7. Referenceliste
8. Bilag