Risikoanalyse af implikationer for privatlivets fred

Appendiks 5
Håndbog i:
Privatlivsimplikationsanalyse

IT- og Telestyrelsen

INDHOLDSFORTEGNELSE

RISIKOVURDERING AF IMPLIKATIONER FOR PRIVATLIVETS FRED

Gennemgangen af genstandsområdet for privatlivsimplikationsanalysen identificerer en række problemområder, hvori der findes implikationer for privatlivets fred. Der kan med fordel foretages en risikoanalyse ud fra betragtninger om konsekvens, sandsynlighed og motivation.

Terminologien og fremstillingen af risikoanalysen søger at bidrage til den samlede privatlivsanalyse ved at fremhæve, på hvilke områder (og måder indenfor disse områder) et projekt indebærer eller kan indebære mindre privatlivsbeskyttelse. Risikoanalysen præsenterer elementer, som allerede er lagt ind i løsningen til at adressere problemområderne, og der kigges på eventuelle andre muligheder for yderligere konkrete tiltag til ændring af løsningens design.

Risikoanalysen munder ud i en samlet vurdering af risikoen ved implikationer for privatlivets fred i den pågældende løsning. Såfremt der er tale om en middel eller højere risiko bør den samlede vurdering kvalificere det forretningsgrundlag eller samfundshensyn, der berettiger til en forringelse af privatlivet. Endelig bør en delmængde være vurdering af, om offentligheden vil kunne acceptere konceptet.

Metode for risikovurdering

Følgende præsenteres en kvalitativ risikoanalyse, der kategoriserer risikoen for en given hændelse med udgangspunkt i følgende aspekter:

- Sandsynligheden for, at hændelser på et identificeret risikoområde for beskyttelsen af privatlivets fred indtræffer
- Konsekvensen af, at en hændelse optræder
- Motivationen for at forårsage hændelsen. Motivation er typisk personligt eller økonomisk drevet. For økonomisk vinding vil der typisk være en større gruppe af individer, der har motivation til at udføre hændelsen

Konsekvens beskrivelse i henhold til Vejledning om risikovurdering på en firetrins skala[1]:

Konsekvens (betegnelse)	**Beskrivelse**
K1: Ubetydelig	Ingen særlig påvirkning.
K2: Mindre alvorlig	Der er formelle mangler i oplysninger til og om den enkelte, men ikke i graverende grad.

[1] Vejledning om risikovurdering for offentlige institutioner, IT- og Telestyrelsen, oktober 2007.

K3: Meget alvorlig (kritisk)	Den enkelte fratages råderet og valgmulighed med hensyn til egne data. Ikke-følsomme data videregives uretmæssigt.
K4: Graverende / uacceptabel (ødelæggende)	Den enkelte udsættes for uacceptable krænkelser af privatlivet. Der træffes bebyrdende afgørelser mod den enkelte på et forkert grundlag. Følsomme data videregives uretmæssigt.

Sandsynlighed betegner muligheden på en 5-punkts skala for, at der indtræffer en hændelse, der krænker beskyttelsen af privatlivet på et identificeret risikoområde.

Sandsynlighed (betegnelse)	**Beskrivelse**
S1: Ingen	Sikkerhedsværn og privatlivsbeskyttelse er etableret og fungerer efter hensigten.
S2: Lav	Sikkerhedsværn og privatlivsbeskyttelse er etableret og fungerer efter hensigten. Tiltag kan brydes af egne medarbejdere med gode ressourcer og kendskab. Eksterne personer kan med meget gode ressourcer og kendskab omgås foranstaltninger.
S3: Middel	Sikkerhedstiltag og privatlivsbeskyttelse er ikke fuldt etableret eller fungerer ikke efter hensigten. Egne medarbejdere kan omgås tiltag med normale ressourcer, eksternt personel kan omgås tiltag med kendskab til rutiner og små ressourcer.
S4: Høj	Sikkerhedstiltag og privatlivsbeskyttelse er ikke systematisk etableret og kan omgås af egne medarbejdere og eksterne personer må få eller ingen ressourcer.
S5: Sikker	Der er ikke truffet forebyggende foranstaltninger af nogen art.

Motivation er en medvirkende faktor i vurderingen af det samlede risikoniveau for mulige hændelser indenfor et givent område. Motivation, eller incitamentsfaktoren, kvalificeres ud fra følgende 5-punkts skala for, om hændelsen kan ske på baggrund af overlæg, forsæt eller uagtsomhed, samt de krævede ressourcer i forbindelse hermed.

Motivation (betegnelse)	Beskrivelse
M1: Meget høj	Hændelse til krænkelse af privatlivets fred kan ske på basis af overlæg med store ressourcer og kræver således høj motivation for udførelse.
M2: Høj	Hændelse til krænkelse af privatlivets fred kan ske på basis af forsæt med store ressourcer for interne medarbejdere, men kræver høj kompetence og overlæg for eksterne personer.
M3: Middel	Hændelse til krænkelse af privatlivets fred kan ske på basis af forsæt med små ressourcer for interne medarbejdere, men kræver dog høj kompetence og forsæt for eksterne personer.
M4: Lav	Hændelse til krænkelse af privatlivets fred kan ske på basis af uagtsomhed for interne medarbejdere, men kræver dog nogen kompetence og forsæt for eksterne personer.
M5: Ingen	Hændelse til krænkelse af privatlivets fred kan ske på basis af uagtsomhed, og kræver ingen speciel motivation eller ressourcer til udførelse.

Konsekvens, sandsynlighed og motivation danner de samlede risiko for, at en given hændelse indenfor et identificeret risikoområde forekommer. Risikoen kategoriseres efter en skala på fem trin:

Risiko (betegnelse)	Beskrivelse
R1: Ingen	Et højt niveau af beskyttelse af privatlivets fred, som væsentlig overvurderer informationens sensitivitet.
R2: Lav	Et stærkt niveau af beskyttelse af privatlivets fred, som vurderer informationens sensitivitet højt.
R3: Middel	Et passende niveau af beskyttelse af privatlivets fred, som afspejler informationens sensitivitet.

R4: Høj	Et ringe niveau af beskyttelse af privatlivets fred, der vurderer informationens sensitivitet lavt.
R5: Meget høj	Et kritisabelt lavt niveau af beskyttelse af privatlivets fred, som væsentligt undervurderer informationens sensitivitet.

Det påpeges, at en risikovurdering er et øjebliksbillede. Det er en del af anbefalingerne til udførelse af en PIA, at vurderingen opdateres og vedligeholdes løbende. Dette ansvar påhviler opdragsgiver.

Risikovurdering

Problemområder identificeres ud fra den foregående analyse i PIA på processer, der inddrager behandling af personoplysninger. Problemområderne opstilles i efterfølgende matrice, der giver det samlede risikobillede for hvert område .

Risikoområde	Mulige trusler til privatlivet	Begrundelse for udformning	K	S	M	Risikovurdering
1						
2						
3						
..						
N						

Matricen skal klart fremstille de måder og områder, hvor et projekt kan indebære en mindsket privatlivsbeskyttelse, og i kolonnen ”Begrundelse for udformning” klart argumentere for, hvorfor funktionaliteten eller anvendelsen er berettiget for systemet.

Tiltag til minimering af risici

I den efterfølgende matrice, der opstiller problemområder, bør der identificeres tiltag til minimering af risici indenfor identificerede risikoområder, både tiltag allerede adresseret i løsning, samt yderligere tiltag.

Som udgangspunkt bør overvejes tiltag, der forøger valgmulighederne for brugeren og mindsker afgivelsen af personoplysninger. Muligheden for inddragelse af eventuelt relevante privatlivsfremmende teknologier bør afvejes.

Tiltag kan opstilles i følgende matrice:

Risikoområde	Mulige trusler til privatlivet	Allerede etablerede tiltag	Mulige andre tiltag	Ny risikovurdering
				R2
				R2
				R2
				R2
				R1
				R2

Formålet med denne matrice er at præsentere de elementer, som allerede er lagt ind i løsningen til at adressere problemområderne samt andre muligheder for yderligere konkrete tiltag til ændring af løsningens design, herunder især hvad implementeringen af yderligere tiltag vil betyde for risikovurderingen for hvert af problemområderne.

Samlet vurdering

På basis af foregående laves den overordnede vurdering af risikoen for beskyttelsen af privatlivets fred. Vurderingen skal præsentere den samlede risikovurdering for systemet og kvalificere denne 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, så konsekvenserne afbødes eller formindskes?
4. Hvilke elementer er allerede inddraget i løsningen til at mindske krænkelser af privatlivet?
5. Hvilke andre elementer kan 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?