DIGITALISERINGSSTYRELSEN

Guide til konsekvensvurdering af privatlivsbeskyttelsen

Maj 2013

Guide til konsekvensvurdering af privatlivsbeskyttelsen

Udgivet maj 2013

Udgivet af Digitaliseringsstyrelsen

Publikationen er kun udgivet elektronisk

Henvendelse om publikationen
kan i øvrigt ske til:

Digitaliseringsstyrelsen
Landgreven 4
1017 København K
Tlf. 33 92 52 00

Publikationen kan hentes på
Digitaliseringsstyrelsens hjemmeside
www.digst.dk.

Foto Colourbox
Jeppe Gudmundsen
Job i Staten

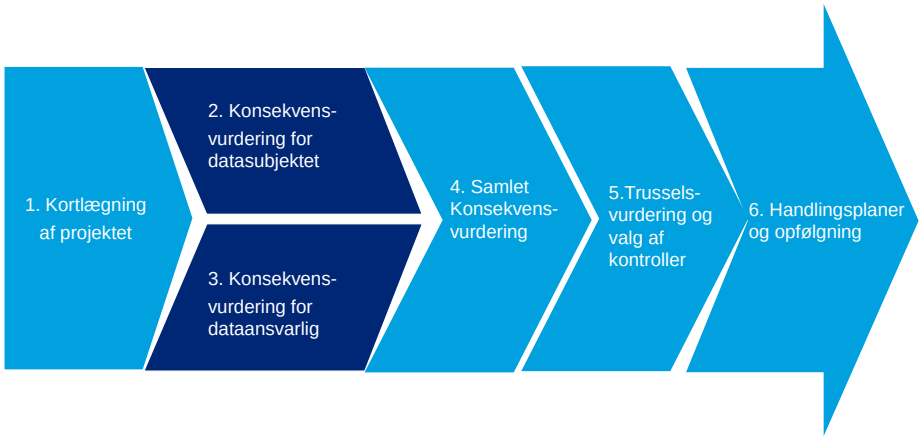
Elektronisk publikation
ISBN 978-87-995647-6-7

1. Introduktion

Hvis et projekts løsning medfører behandling af personoplysninger, eller hvis løsningen vil kunne medføre konsekvenser for privatlivet, er det relevant, at der gennemføres en konsekvensvurdering for privatlivet.

Konsekvensvurderingen for privatlivet er en proces, der består af seks trin. Processen skal munde ud i handlingsplaner og eventuelle oplæg til projektets styregruppe, så beslutningstagerne kan blive inddraget i det spørgsmål, som privatlivsbeskyttelse udgør for mange projekter.

Vurderingen skal gennemføres i projektets analysefase, men allerede i idéfasen bør der foretages en overordnet vurdering, i takt med at man identificerer projektets teknologi og data.



Denne guide giver en kort introduktion til metoden bag konsekvensvurdering for privatlivet. En udvidet beskrivelse af metoden findes i "Vejledning i vurdering af offentlige it-projekters potentielle konsekvenser for privatlivet". Til vejledningen er der udviklet et regneark, der kan bruges som hjælp til at gennemgå processens trin. Vejledning og regneark findes på Digitaliseringsstyrelsens hjemmeside.

2. Kortlægning

Før selve konsekvensvurderingen skal projektet, eller den løsning man ønsker at undersøge, kortlægges og beskrives. Kortlægningen skal gøre rede for teknologien, stamdata og informationsflow. Dokumentationen kan eventuelt skrives ind i det regnearksbaserede værktøj, der er udviklet i tilknytning til vejledningen.

Efter kortlægningen skal man identificere de relevante interessenter. Det grundlæggende projekts interessenter er i forvejen blevet identificeret i forbindelse med projektopstart, men på privatlivsområdet bliver kredsen af interessenter som regel udvidet. Ikke alle har samme opfattelse af grænserne for privatlivet, så derfor skal alle nuancer med i vurderingen, for at man kan få et retvisende billede af projektets omverden og begrænsninger.

Relevante interessenter er bl.a.

- De borgere/datasubjekter, projektet har en potentiel indvirkning på.
- Private virksomheder
- Interesseorganisationer
- Andre myndigheder.

Det er op til den enkelte projektleder at vurdere, hvordan interessenterne inddrages. Det kan ske i fokusgruppeundersøgelser, etablering af referencegrupper, meningsmålinger osv. Det afhænger af den enkelte projektleder og projektorganisations erfaringer.

3. Konsekvensvurdering

For at holde tingene adskilt anbefales det, at konsekvensanalysen deles op to særskilte vurderinger: Én vurdering for datasubjektet (borgere/brugere) og én vurdering for den dataansvarlige (organisation/institution).

I alt skal der gennemgås syv kriterier, der hver især giver en indikation af, om en krænkelse af privatlivet kan få **kritiske, generende** eller **ubetydelige** konsekvenser for datasubjektet eller den dataansvarlige. Hvis ét vurderingskriterium er vurderet som *kritisk*, er det ikke ensbetydende med, at projektets egenskaber samlet set forventes at indikere en risiko for kritiske konsekvenser. Det afhænger af, hvordan de resterende kriterier vurderes.

3.1 Datasubjektet

1. Oplysningernes følsomhed
De personlige omkostninger ved et brud på privatlivsbeskyttelsen og graden af dets alvorlighed hænger sammen med karakteren af de involverede oplysninger. Jo tættere oplysningerne er på intimsfæren, jo mere følsomme de er, jo mere alvorligt vil datasubjektet som udgangspunkt opfatte et brud.

2. Indskrænket handlefrihed
Konsekvensen ved en konkret krænkelse af privatlivet kan med fordel vurderes på baggrund af den indskrænkning, den medfører for den enkeltes personlige frihed. Graden af alvorlighed er proportional med indskrænkningens størrelse og invaliderende karakter.

3. Teknologiens potentiale til at krænke privatlivet
Projektet kan bruge teknologier, som er indrettet til at indsamle personoplysninger eller til at behandle dem på måder, som ligger uden for rammerne og formålet af projektet. Teknologierne vil på den måde kunne være krænkende for datasubjekter, hvis de bliver udnyttet. Dette kan fx være RFID-teknologier, der kan indsamle oplysninger om individers opholdssteder eller færden.

Selvom projektet ikke har til formål at indsamle og behandle personoplysninger af denne karakter, udgør teknologiens muligheder stadig en risiko for, at en uønsket eller uforudset behandling af personoplysninger vil kunne ske på et senere tidspunkt. Det er derfor afgørende for vurderingen, om teknologien i sig selv kan udgøre en mulig risiko for en krænkelse af privatlivet.

4. Oplysningernes potentiale til at identificere enkeltpersoner
Oplysningernes potentiale til at identificere enkeltpersoner bør også indgå i konsekvensvurderingen. Ikke som et isoleret vurderingskriterium, men som et element der 'forstærker' de andre kriteriers betydning. Hvis oplysningerne fx kun omfatter fornavnene på en gruppe individer, er det sværere at identificere de enkelte personer. Et eventuelt brud kan derfor vurderes som mindre alvorligt, end hvis oplysningerne både omfatter for- og efternavne og adresser.

5. Størrelsen på brugergruppen
Det har også betydning for konsekvensvurderingen, hvor mange brugere der skal have adgang til en den nye løsning. En stor brugergruppe, som er spredt over flere selvstændige organisatoriske enheder, vil alt andet lige forstærke risikoen for krænkelse af privatlivet; risikoen for spredning af oplysningerne er stigende med brugergruppens størrelse. Hvis brugergruppen oven i købet er spredt ud over flere enheder, forringes den dataansvarliges mulighed for at kontrollere oplysningerne.

Den samlede konsekvensvurdering for datasubjektet
De tre første vurderingskriterier, *oplysningernes følsomhed, indskrænket handlefrihed og teknologiens potentiale til at krænke privatlivets fred på et senere tidspunkt*, siger noget om styrken eller intensiteten af en potentiel krænkelse for datasubjektet.

Identificeringspotentialet og størrelsen på brugergruppen har en begrænset selvstændig betydning, men har den egenskab, at de forstærker konsekvensen af de brud, som de tre øvrige vurderingskriterier er indikatorer for.

For at få en samlet konsekvensscore for datasubjektet kan man bruge følgende beregningsmodel:

3.2 Den dataansvarlige

6. Påvirkning af den dataansvarliges omdømme
I tilfælde af alvorlige brud på privatlivet risikerer den dataansvarlige også at lide omdømmemæssige konsekvenser. Det kræver en skønsmæssig og subjektiv vurdering.

7. Vurdering af den økonomiske konsekvens for den dataansvarlige
Det sidste element vedrører de forventede økonomiske tab for den dataansvarlige, hvis der sker et alvorligt brud på privatlivet. De økonomiske tab vil sandsynligvis bestå i bøder fra Datatilsynet, ikke-budgetterede udgifter til ekstra arbejde eller tab, hvis projektet opgives.

Den samlede konsekvensvurdering for den dataansvarlige
Den samlede konsekvensvurdering for den dataansvarlige er resultatet af den højeste vurdering af det 6. og 7. vurderingskriterium, *påvirkning af den dataansvarliges omdømme* og *den økonomiske konsekvens*. Rationalerne bag begge vurderinger skal indgå i den endelige analyse, men en fuldstændig vurdering giver et sammenligneligt overblik over, hvor projektet samlet set befinder sig i risikobilledet.

4. Trusler og handlingsplan

Et nyt projekt bør altid følges af en struktureret vurdering af de trusler, der kan have betydning for projektet og eventuelt resultere i krænkelser af privatlivet.

Der er flere typer af trusler, som kan udløse brud på privatlivsbeskyttelsen. Der kan skelnes mellem trusler knyttet til projektets løsningsdesign, projektets drift eller relationen til datasubjekter.

Hvert trusselområde indeholder en række konkrete trusler. For hver trussel, som vurderes at udgøre en risiko for projektet, bør der tages stilling til sikringsforanstaltninger, der kan reducere projektets sårbarhed. *Vejledning til konsekvensvurdering for privatlivet* indeholder et trusselsregister med forslag til tilhørende sikringsforanstaltninger.

Når konsekvensvurderingen er gennemført, bør der udarbejdes en kort rapport, der redegør for den samlede konklusion af konsekvensvurderingen.

Rapporten bør indeholde en sammenfatning af de kvalitative vurderinger, der er foretaget for hvert kriterium. Den bør også indeholde en handlingsplan til at håndtere de aspekter ved projektet, der indikerer en særlig risiko for alvorlige konsekvenser ved krænkelser på privatlivsbeskyttelsen.

Rapporten skal gives til projektets styregruppe, så der kan følges op på den og tages stilling til handlingsplanen. En styregruppe kan efter omstændighederne også vælge at acceptere risici. Det vil altid være afgørende for en projektleder at få styregruppen til at forholde sig til konsekvenser for privatlivet. Styregruppens valg bør under alle omstændigheder dokumenteres.