Kriterier for kontrol af overensstemmelse med lovgivning

Appendiks 3
Håndbog i:
Privatlivsimplikationsanalyse

IT- og Telestyrelsen

INDHOLDSFORTEGNELSE

KRITERIER FOR KONTROL AF OVERENSSTEMMELSE MED LOVGIVNING OM BESKYTTELSE AF PRIVATLIVET

Det følgende appendiks er ment som en hjælp til virksomheder i forhold til at sikre, at lovgivningen om beskyttelse af privatliv, herunder persondataloven, overholdes. Appendikset sammenfatter en beskrivelse af trin 3 og trin fire af håndbog i privatlivsimplikationsanalyse. Det kan være nødvendigt med bistand fra en juridisk rådgiver med relevant sagkundskab.

Endvidere skal fremhæves, at Datatilsynet i 2010 arbejder på en vejledning for udførsel af compliance-analyse. Når en sådan vejledning udkommer, anbefales at tage udgangspunkt i denne frem for nærværende appendiks. Nærværende appendiks kan eventuelt benyttes som supplement.

Trin 3: Kriterier for udarbejdelse af compliance-analyse for relevant lovgivning ud over persondataloven

Hvis nogle af nedenstående spørgsmål besvares med "ja", så er det nødvendigt at overveje at foretage en kontrol, det vil sige en compliance-analyse for overensstemmelse med relevant lovgivning om beskyttelse af privatlivet :

1. *Omfatter projektet aktiviteter (herunder enhver form for databehandling), som er underlagt bestemmelser om beskyttelse af privatlivet eller tilsvarende bestemmelser i nogen lov eller anden form for regulering ud over persondataloven?*

Hvor projekterne er af tværjurisdiktionel karakter, kan der indgå mere end ét lands lovgivning, og der kan også være behov for at tage andre lovbestemmelser i betragtning.

2. *Omfatter projektet aktiviteter (herunder alle former for databehandling), som er underlagt begrænsninger ifølge regeler med relevans for beskyttelsen af privatlivet?*

3. *Omfatter projektet aktiviteter (herunder alle former for databehandling), som er underlagt mindre formelle krav i henhold til god praksis med relevans for beskyttelse af privatlivet?*

Især må branchestandarder og -kodekser tages i betragtning:

Før man foretager en compliance-analyse på overensstemmelse med relevant lovgivning ud over persondataloven skal trin 4 af screening-processen i håndbogen gennemløbes for at afgøre, om kontrol af overensstemmelse med persondataloven også skal indgå i projektplanen. Trin 4 er beskrevet efterfølgende i dette appendiks. Aktiviteter vedrørende overensstemmelseskontrol foretages

normal sent i den samlede projektplan, når de nærmere oplysninger om forretningsprocesser og forretningsregler foreligger.

Trin 3: Udarbejdelse af compliance-analyse for overensstemmelse med relevant lovgivning udover persondataloven

Virksomheden bør overveje at sikre sig, at projektet, de behandlede persondata og de anvendte forretningsprocesser er i overensstemmelse med al relevant lovgivning. I modsætning til en PIA, der bedst påbegyndes på et tidligt tidspunkt i projektforløbet, foretages den såkaldte overensstemmelseskontrol normalt senere, når designet er nået så langt som til detailstadiet, eller umiddelbart før implementering påbegyndes.

Ansvar

Virksomheden bør foretage en undersøgelse af lovgivning, som er relevant for projektet og de databehandlings- og forretningsprocesser, som projektet giver anledning til. Dette bør ligeledes gøres af alle deltagende virksomheder i forbindelse med deres engagement i projektet. Almindeligvis skal virksomheden gøre brug af fagfolk med relevant juridisk sagkundskab ved denne procedure.

Kilder til lovgivning og andre regler

Lovgivningen omfatter retsregler vedtaget i folketinget , bekendtgørelser mv. udstedt af regeringen og relevant praksis fra domstole og myndigheder. .

Yderligere dokumenter kan være relevante, f.eks. adfærdskodekser og politikerklæringer vedrørende beskyttelsen af privatlivet, navnlig hvor virksomheden har afgivet en eller anden forpligtelse til at overholde disse. Dette kan eventuelt hidrøre fra en officiel tiltrædelseserklæring (som f.eks. medlemskab af foreningen som udsteder adfærdskodeksen) eller vilkår i et dokument, som virksomheden selv har udgivet. Der er også forhold vedrørende samfundets interesser, som ikke indgår i formel lovgivning, men som er almindelig anerkendt.

Overensstemmelseskontrol

Virksomheden må vurdere projektprocessen og projektresultaterne (herunder design, databehandling og bredere forretningsaktiviteter) for at sikre sig, at alle forhold er i overensstemmelse med alle relevante bestemmelser i alle relevante love). Hver deltagende virksomhed må vurdere de aktiviteter, den vil foretage som en del af projektet og som en del af det resulterende system eller koncept for at sikre, at den overholder alle relevante bestemmelser i alle relevante love.

Udsættelse af gennemførelse og tilpasning af design

I den udstrækning, designet ikke overholder bestemmelserne, vil det være ulovligt at idriftsætte det nye eller tilpassede system eller koncept. Det vil være

nødvendigt at ændre designet før ibrugtagningen, således at der opnås overensstemmelse.

Trin 4: Kriterier for udarbejdelse af compliance-analyse for persondataloven

Formålet med dette afsnit er at hjælpe virksomhederne med at overholde alle relevante love. Det kan være nødvendigt med bistand fra en juridisk rådgiver med relevant sagkundskab.

Hvis nedenstående spørgsmål besvares med "ja", så er det nødvendigt at foretage en vurdering af overensstemmelse med persondataloven:

1. *Omfatter projektet behandling af data, der er personoplysninger, således som dette udtryk er anvendt i persondataloven?*

'Personoplysning' er defineret som ”Enhver form for information om en identificeret eller identificerbar fysisk person” (persondatalovens § 3, nr. 1).

Trin 4: Udarbejdelse af compliance-analyse for overensstemmelse med persondataloven

Virksomheden må sikre sig, at projektet, de behandlede persondata og virksomhedens forretningsaktiviteter overholder persondataloven generelt, principperne for databeskyttelse og fortolkningen af principperne. Dette er ikke en anbefaling i dette appendiks, men et krav ifølge lovgivningen.

Overensstemmelseskontrol

Virksomheden må vurdere projektprocessen og det resulterende design for at sikre sig, at den overholder persondataloven. I modsætning til en PIA, der bedst påbegyndes på et tidligt tidspunkt i projektforløbet, foretages overensstemmelseskontrollen normalt senere, når designet er nået så langt som til detailstadiet eller umiddelbart før implementeringen.

Hver deltagende virksomhed må vurdere de aktiviteter, den vil foretage som en del af det resulterende system eller koncept, med henblik på at sikre, at den overholder persondataloven.

Udsættelse af gennemførelse og tilpasning af design

I den udstrækning, designet ikke overholder bestemmelserne, vil det være ulovligt at idriftsætte det nye eller tilpassede system eller koncept. Det vil være nødvendigt at ændre designet før ibrugtagningen, så der opnås overensstemmelse.