Hvordan sikrer jeg god privatlivsbeskyttelse?

- Du skal efterleve persondataloven og den tilhørende sikkerhedsbekendtgørelse, som har til formål at beskytte borgernes personlige integritet og privatliv
- Du bør følge kravene i dansk standard for informationssikkerhed, DS 484/ISO 27001 (krav til statslige myndigheder)
- Du bør lave en PIA-screening og eventuelt en PIA på systemet
- Du bør overveje privatlivsfremmende teknologier (PETs)

Privatlivsbeskyttelse giver:

Brugerne af dit system sikkerhed og tryghed for, at systemet har respekt for deres oplysninger

Privatlivsbeskyttelse giver:

Bedre design af dit system ved, at du tænker og overvejer det en ekstra gang.

Privatlivsbeskyttelse giver:

Dig en bedre mavefornemmelse!—og du bliver fri for at skulle betale en dyr lappeløsning senere hen.

D I
ITEK

IT- og Telestyrelsen
Ministeriet for Videnskab
Teknologi og Udvikling

Privacy Impact Assessments

Hurtigt i gang!

Privacy Impact Assessments (PIA)

Denne pjece giver dig et overblik over, hvad en PIA er, hvorfor det er en god idé at udføre den, og hvilke spørgsmål man skal stille i en PIA.

PIA hvem?

Projekter, der behandler personoplysninger eller bruger nyere teknologi, giver anledning til at tænke over beskyttelsen af privatlivet.

Et system skal bruges for at være en succes. Og en forudsætning for denne brug er, at brugerne har tillid til, at systemet er sikkert og respekterer deres oplysninger.

En PIA er en proces der hjælper til at tænke privatlivsbeskyttelsen ind fra start i et projekt, og dermed sikre, at de fremtidige brugere kan være trygge og sikre ved systemet.

Processen for en PIA vurderer systemet, evaluerer designet, og fordrer, at der tænkes i muligheder og alternative designs for at fremme privatlivsbeskyttelsen endnu mere.

Undgå omkostninger

Ved at udføre en PIA tidligt i et projektforløb undgås det, at der opdages problemer på et senere stadium, når ændringer af komponenter er meget dyrere.

En fordel ved at indbygge følsomhed over for beskyttelsen af privatlivet i projektets design fra begyndelsen er, at der skabes grundlag for et fleksibelt og tilpasningsvenligt system, som nedbringer omkostningerne ved fremtidige ændringer, fremmer konkurrence og innovationsevnen, samt sikrer en længere levetid for applikationen.

Hvilke spørgsmål?

I en PIA skal du overordnet svare og evaluere på:

1. Indsamler eller behandler systemet personfølsomme oplysninger? Hvordan og hvorfor?
2. Kan indsamlingen af personoplysninger mindskes eller undgås? Hvordan / hvorfor ikke?
3. Anvender systemet en nyere teknologi, som kræver specielle overvejelser? Hvilke og hvordan? Det kunne eksempelvis være biometri, RFID tags eller lignende.
4. Hvordan er systemet designet? Hvad er de overordnede processer? Hvilke overvejelser har du gjort for at sikre personers kontrol og adgang til oplysninger?
5. Hvordan identificerer systemet personer? Bruger man f.eks. samme ID til en person (f.eks. CPR-nummer) på tværs af databaser, eller har personer forskellige ID'er i forskellige dele af systemet?
6. Anvender systemet privatlivsfremmende teknologier? Hvilke og hvordan? F.eks. i form af pseudonymisering og anonymisering.
7. Omfatter projektet flere forskellige organisationer, det være sig private virksomheder eller offentlige myndigheder? Hvis ja, hvem er ansvarlig for hvad?
8. Betyder projektet, at man kommer til samle flere data ind om personer end før? Hvorfor?
9. Hvordan er oplysninger opbevaret og sikret?
10. Har du udarbejdet procedurer og politikker for medarbejdere, der har adgang til personfølsomme data og genrel information om systemet ? Hvilke og hvem er ansvarlig?

Når du har besvaret og analyseret disse spørgsmål, har du en ide om niveauet for privatlivsbeskyttelsen i dit projekt. Nu kan du så begynde at overveje, om du bør kigge efter alternative løsninger.

Vil du vide mere?

På IT– og Telestyrelsens hjemmeside kan du finde vejledninger til, hvordan du udfører en PIA-screening og en PIA-analyse.

http://www.itst.dk/publikationer