Databeskyttelse gennem design

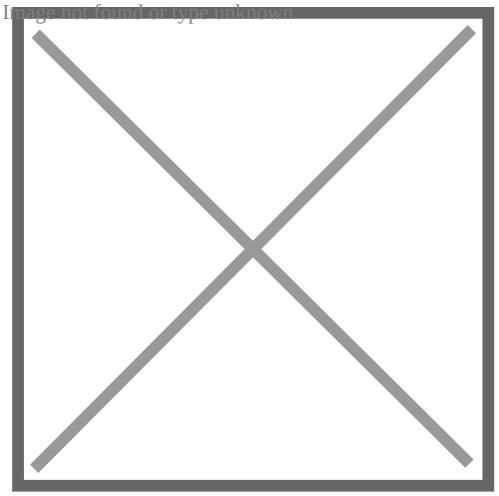
12. november 2018

Databeskyttelse er en kontinuerlig proces. Er du færdig med at implementere den nye persondataforordning, herunder de organisatoriske og tekniske sikkerhedsforanstaltninger? Nej, vel.

Persondataforordningen stiller krav til at implementere databeskyttelse gennem design, hvorpå man skal sikre persondata i hele ens virksomhed.

Så svaret er nok, at du aldrig bliver helt færdig med at overholde persondataforordningen, da det er en kontinuerlig proces i en digital verden, hvor det er nødvendigt at både vedligeholde og opdatere beskyttelsen af persondata i IT-systemer. Dette kan illustreres således:

Image not found or type unknown



Kilde: Det norske datatilsyn

For at opnå den rette databeskyttelse er det vigtigt, at du hele tiden overvejer dine IT-systemer og dine processer.

IT-systemer og medarbejdere skal kunne håndtere persondata

Men hvordan opfylder du så rent faktisk persondataforordningens krav om databeskyttelse gennem design? Alle virksomheder bestræber sig på at digitalisere, men hvilke tekniske og organisatoriske foranstaltninger der er passende varierer fra virksomhed til virksomhed.

Det er i den forbindelse værd at efterleve følgende syv designprincipper:

Designprincipperne	Beskrivelse	JA/NEJ
Proaktiv, ikke reaktiv:	Foranstaltninger iværksættes, inden risici forekommer.	
Privacy som standardindstilling:	Den registrerede behøver ikke selv foretage sig noget for at beskytte sine oplysninger.	
Privacy skal være indlejret i systemet:	Foranstaltningerne designes ind i IT-systemer fra starten og tilføjes ikke efterfølgende, herunder automatisk.	
Der skal være fuld funktionalitet:	Man får ikke fuld funktionalitet uden sikkerhed og databeskyttelse.	
Beskyttelse i hele livscyklussen:	Beskyttelsen indbygges i designfasen, inden IT-systemet sættes i drift og er aktivt i hele systemets levetid.	
Transparens:	Forretningsmodeller og teknologier skal have gennemsigtighed.	
Brugeren i centrum:	De registreredes interesser er i fokus, så de er i kontrol.	

Kilde: Dr. Ann Cavoukian

Og følgende syv Privacy Enhansing Technologies (PET):

PET'erne	Beskrivelse	JA/NEJ
Begrænse data:	Du indsamler kun de data, der er relevante og begrænset til formålet.	
Adgangsbarrierer:	Det er kun dem, der har et formål med at behandle den pågældende persondata, som har adgang.	
Anonymisering:	Når du ikke længere har et formål med at bruge de pågældende persondata, anonymiseres eller slettes de som en sikkerhedsforanstaltning.	
Pseudonymisering:	En god måde at systematisere ens persondata på uden at være linkbar. Personoplysningerne bliver delt op med tal i stedet for de faktiske oplysninger, og kan dermed gemmes, uden at de henføres til en fysisk person.	
Kryptering:	Dette er en sikkerhedsforanstaltning, som giver troværdighed og fortrolighed. Det er en god og sikker måde at dele personoplysninger på.	
Biometrics:	I stedet for adgangskoder kan f.eks. fingeraftryk bruges som sikkerhedsforanstaltning.	
Auditability:	Logning af alle ens aktiviteter som en sikkerhedsforanstaltning der skaber troværdighed i forbindelse med Datatilsynets kontrol.	

Kilde: Handbook of Privacy and Privacy-Enhancing Technologies

Ovenstående syv designprincipper og syv PET'er skal tilsammen efterleves i form af en kontinuerlig proces, for at du har et IT-system og nogle medarbejdere, der kan håndtere persondata korrekt, så du derved er på forkant og undgår sanktioner.

Ring til Roesgaard og hør nærmere om databeskyttelse gennem design.

Skrevet af:

Frederikke Schlitterlau
Cand. Merc. Jur.
23 45 00 14 · fs@roesgaard.dk