Hvorfor arbejde med persondatasikkerhed?

- √ Du får en viden om, hvad du skal/må/ikke må i forhold til gældende love og regler
- √ Din virksomhed viser respekt for såvel medarbejdernes som kundernes persondata
- √ Du er bedre forberedt i tilfælde af brud på sikkerheden
- √ Med PIA-analyserne*) får virksomhedens ledere et bedre beslutningsgrundlag
- √ Nedskrevne politikker, retningslinjer og instrukser giver mere trygge medarbejdere
- √ Du får afdækket risiko-områderne, og kan agere herpå inden det måtte gå galt
- √ Brug på persondatasikkerheden = tab/udgifter p.g.a oprydningsomkostninger og måske tabt omsætning
- √ En generel opmærksomhed på persondatasikkerhed i virksomheden vil mindske risiciene for brud på datasikkerheden

TD Consult er certificeret indenfor Persondatabeskyttelse og kan hjælpe med:

- ⇒ Udarbejdelse af databeskyttelses-politikker og –instrukser
- ⇒ Virksomheds-seminar om persondatabeskyttelse
- ⇒ Træning af medarbejdere
- ⇒ PIA-analyse *) af organisationens arbejdsgange

*) Privacy Impact Assessment (Indvirkning på persondata)

TD Consult
v/Tove A. Dahlmann
Skårupøre Strandvej 123, 5881 Skårup
Tlf: 40 25 46 26
Mail: Tove@tdconsult.dk
Web: www.tdconsult.dk
Cvr: 25 51 76 01

december 2016

Fleksibel freelance assistance

En træningstjekliste vedr. medarbejderviden om Persondatasikkerhed for små og mellemstore organisationer

Denne tjekliste skitserer nogle af de praktiske konsekvenser af loven, og er tænkt som en almen ramme for den nødvendige grundlæggende viden hos kontor-personale i små og mellemstore organisationer. Under hver overskrift er en ikke-udtømmende guide til de punkter, der bør være omfattet i enhver uddannelse. Medarbejdere med opgaver såsom markedsføring, edb-sikkerhed og styring af databaser kan have behov for specialiseret uddannelse for at gøre dem opmærksomme på særlige krav til databeskyttelse i deres arbejdsområde.

TD Consult
v/Tove A. Dahlmann
Skårupøre Strandvej 123, 5881 Skårup
Tlf: 40 25 46 26
Mail: Tove@tdconsult.dk
Web: www.tdconsult.dk

Fleksibel freelance assistance

1. Sikker håndtering af personlige oplysninger

Ved dine medarbejdere:

◊ At de skal håndtere adgangskoder sikkert – skifte dem regelmæssigt, og ikke dele dem med andre?

◊ At de skal sørge for at for at låse / logge af computere, når de er væk fra deres skriveborde?

◊ At de skal sørge for at bortskaffe fortroligt papiraffald sikkert ved makulering?

◊ At de skal sørge for at forhindre virusangreb ved at være på vagt, når de åbner e-mails og vedhæftede filer eller besøger nye hjemmesider?

◊ At de bør arbejde på et "clear-desk" -grundlag - ved at lagre personlige oplysninger i papir-form sikkert, når det ikke bliver brugt?

◊ At besøgende bør ledsages på områder, der normalt er forbeholdt ansatte?

◊ At de skal positionere computerskærme væk fra vinduer for at forhindre utilsigtet videre-givelse af personoplysninger?

◊ At de skal kryptere personlige oplysninger, der bliver medtaget udenfor kontoret, hvis det vil forårsage ulempe for eller skade de registrerede, i tilfælde af at oplysningerne skulle gå tabt eller blive stjålet?

◊ At de skal sørge for at tage back-ups af personoplysninger? Og at disse backups skal håndteres lige så sikkert som de øvrige personoplysninger?

2. Imødegåelse af de rimelige forventninger hos kunder og medarbejdere

Ved dine medarbejdere:

◊ At de kun må indsamle de person-oplysninger, de har brug for til et specifikt formål?
◊ At de skal forklare nye eller ændrede forretningsmæssige formål for kunder og medarbejdere, og sørge for at opnå samtykke eller give en opt-out-mulighed?
◊ At de skal sørge for at opdatere oplysninger omgående - for eksempel adresseændringer, marketing præferencer?
◊ At de skal slette person-oplysninger, som der ikke længere er grundlag for at beholde?
◊ At de overtræder loven, hvis de videregiver kunde- eller medarbejder-persondata uden samtykke?
◊ Om der i virksomheden finder overvågning sted?

3. Udlevering af personlige oplysninger

Ved dine medarbejdere:

◊ At de skal være opmærksomme på, at der er mennesker, der vil forsøge at narre dem til at videregive personlige oplysninger?
◊ At de skal foretage identitetskontrol, før de videregiver personlige oplysninger?

4. Håndtering af anmodninger fra enkeltpersoner om indsigt i deres personlige oplysninger

Ved dine medarbejdere:

◊ At den/de registrerede har ret til at få en kopi af de personlige oplysninger, virksomheden har i sine systemer/arkiver?
◊ Hvordan de identificerer en anmodning om indsigt?
◊ Hvem de skal videregive det til, hvis det ikke er deres ansvar at svare?
◊ At virksomheden har et maksimum på 4 uger til at reagere?
◊ At det maksimale gebyr, der kan opkræves for skriftlig besvarelse af en anmodning om indsigt, er kr. 10 pr. side og i alt max kr. 200?
◊ At det er nødvendigt at kontrollere identiteten af rekvirenten?
◊ Hvad man gør, hvis andre personers oplysninger er indeholdt i det foreslåede svar?

Definitionen på Personlige oplysninger (Persondata)

PersonDataLovens §3 nr. 1: "*Enhver form for information om en identificerbar fysisk person*"

Med andre ord, almindelige oplysninger som

Navn,
Postadresse,
Mailadresse,
Telefonnummer,
Medlemsnummer i en forening

kategoriseres som Persondata.
Datatilsynets definition inkluderer endog også billede, stemme, registreringsnr, genetiske kendetegn og fingeraftryk,
den nye Persondataforordning/Databeskyttelsesforordning medtager tillige lokaliserings-data og online-identifikatorer.

Denne tjekliste er inspireret af en lignende publikation fra ICO Information Commissioners Office (det engelske datatilsyn), publikationen kan findes på https://www.ioc.org.uk/