Tjekliste til implementering af persondataforordningen

1. Skabe over blik over:

- Hvilke data behandler man
- Hvor ligger data gemt (IT-systemer, fysiske journaler mv.)
- Hvem har adgang
- Hvem udveksler man data med. Hvem modtager man data fra
- Hvem sender man data til (andre dataansvarlige eller databehandlere)
- Få afklaret hvornår man er dataansvarlig og hvilke databehandlere man anvender (se punkt 6 og 7)
- Hvordan er data beskyttet/sikkerhed

2. Hvordan informerer man de personer, hvis data man behandler?

- Udarbejde persondatapolitiker omkring behandlingen af data, som indeholder de informationer, som i henhold til persondataforordningens, skal gives til de registrerede.
- Udarbejde persondatapolitik for medarbejderdata
- Persondatapolitik for behandling af kundedata
- Persondatapolitik for behandling af eventuelle andre typer data end kunde- og medarbejderdata.
- Få afdækket, hvordan man bedst får informeret de registrerede om/henvist til de forskellige persondatapolitikker

3. Udarbejde "Fortegnelser" over de forskellige behandlinger af persondata, som man foretager, jf. forordningens art. 30

- Fortegnelse for behandling af medarbejderdata
- Fortegnelse for behandling af kundedata
- Fortegnelser over eventuel behandling af andre data-typer

4. Juridiske krav – Lovlig behandling

- Gennemgå om de forskellige databehandlinger opfylder de juridiske krav, dvs. er der den fornødne saglighed, har man den fornødne hjemmel. Sammenfatte dette på skrift og evt. indarbejde det i de ovennævnte fortegnelser. Hvis ikke man har de fornødne hjemler, f.eks. manglende samtykker, sikre at dette sker.
- Sikre at data ikke gemmes længere end de må og/eller skal – Dvs. sikre at der sker sletning/anonymisering af data, som man ikke længere har et sagligt behov for og/eller hjemmel til gemme, eller som man ikke længere er forpligtede til at gemme. Der kan ikke fastsættes et bestemt antal år eller måneder for, hvor længe man må gemme f.eks. kundedata.
- Det vil bero på en konkret vurdering af, om man har et sagligt formål med at gemme disse oplysninger. Fsva. medarbejderdata vil disse kunne gemmes i 5 år, bl.a. med den begrundelse, at der kan opstå efterbetalingssager i op til 5 år efter at en medarbejder har ophørt med sit ansættelsesforhold.

- Foretage en grundig oprydning i eksisterende/gamle data både i IT-systemer. mailsystem og i fysisk materiale

5. Håndtering af de registreredes rettigheder

- Gøre sig klart, om man kan – og hvordan man skal – håndtere de registreredes krav på indsigt, sletning, berigtigelse, mv. Hvilke procedurer går i gang, hvis en registreret anmoder om berigtigelse, indsigt eller sletning.

6. Brug af databehandlere

- Få afdækket brugen af databehandlere
- Udarbejde eller efterspørge databehandleraftaler

7. Videregivelse af oplysninger til andre dataansvarlige

- Få afdækket om man videregiver data til andre selvstændige dataansvarlige, dvs. virksomheder eller personer som anvender de pågældende personoplysninger til deres egen selvstændige behandling og udarbejde en aftale med disse.
- Hvordan sender man disse oplysninger – sikkerhed, evt. kryptering mv.

8. Sikkerhed

- IT-sikkerhed? Sikring mod hacking. Kryptering ved forsendelse af personfølsomme oplysninger, evt. anonymisering af personoplysninger.
- Adgangssikkerhed – begrænse adgang til persondata til de personer, som har behov for data
- Fysisk sikkerhed. Makulering, evt. aflåste kontorer, nøgle til kopieringsmaskiner, adgang til huset, etc.
- Både fysisk og IT-mæssig sikkerhed og de tiltag der iværksættes skal afvejes i forhold til den risiko, der er forbundet med at de pågældende data går tabt/lækkes. Personfølsomme oplysninger, CPR-numre og straffeoplysninger skal altid underlægges større sikkerhedsforanstaltninger end alm. oplysninger, som navn, adresse, e-mail mv.
- Sikre, at der sker løbende sletning og/eller anonymisering af data med bestemte intervaller – se ovenfor under pkt. 4
- Hvordan håndterer man et evt. databrud?
- Sikre at man ved evt. databrud kan give Datatilsynet besked indenfor 72 timer
- Afdække om man evt. ved et databrud også skal underrette de registrerede

9. Information/undervisning af medarbejdere

- Sikre at medarbejdere er bekendt med persondatareglerne og har en adfærd, der sikrer overholdelse af reglerne
- Evt. udarbejde en "adfærdsguide" til medarbejderne
- Evt. uddanne medarbejderen via E-learning

Marts 2018