**Vejledning til fortegnelse over behandlingsaktiviteter**

Efter den 25. maj 2018 skal alle virksomheder føre en intern fortegnelse over deres behandling af personoplysninger. Det er virksomheden, der har ansvaret for, at reglerne om behandling af personoplysninger overholdes, og virksomheden skal kunne vise, at de overholder reglerne. Derfor har AutoBranchen Danmark lavet et udkast til fortegnelser over behandlingsaktiviteter, som virksomheden foretager. Fortegnelserne skal være tilgængelig skriftlig og elektronisk og kan kræves udleveret af Datatilsynet.

**Ansvarsfraskrivelse:**

Fortegnelserne er kun et udkast og er ikke fyldestgørende. De kan bruges til inspiration, men kræver konkret tilpasning.

**Fortegnelserne skal indeholde følgende:**

1) Navn og kontaktoplysninger på virksomheden selv, evt. repræsentant og databeskyttelsesrådgiver

2) Formålene med behandlingen

* Samtlige formål med behandlingsaktiviteten skal fremgå af fortegnelsen
* I visse tilfælde kan flere behandlingsaktiviteter samles i én fortegnelse

3) Kategorier af registrerede

* De registrerede er de personer, som der behandles personoplysninger omkring, fx. kunder, medarbejdere, leverandører og samarbejdspartnere

4) Kategorier af personoplysninger

* Her skal det angives, om det er almindelige eller følsomme personoplysninger der behandles
* Følsomme oplysninger er: CPR-nummer, race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, genetiske data, biometriske data med henblik på entydigt at identificere en fysisk person, helbredsoplysninger, seksuelle forhold/ orientering

5) Kategorier af modtagere som oplysningerne er eller vil blive videregivet til

* Her skal kortlægges, om der sker eller vil ske en videregivelse af personoplysninger
* Kun de overførsler, der er regelmæssige, skal anføres i fortegnelsen

6) Overførsler af personoplysninger til tredjelande og/eller internationale organisationer

* Oplyse om overførsler af personoplysninger til et tredjeland eller en international organisation
* Et tredjeland er et land uden for EU / EØS (fx USA, Kina, Indien)
* Der er flere måder overførslen kan se på:
  + 1. overførslen sker til et sikkert tredjeland
    2. overførslen sker via EU-kommissionens standardkontrakter
    3. overførslen sker via Binding Corporate Rules
* Vedlægge dokumentation for passende garantier
* Angive modtagere i fortegnelsen

7) Forventede slettefrister af de forskellige kategorier af oplysninger (hvis det er muligt at angive disse)

* Fortegnelsen skal oplyse de forventede tidsfrister for sletning
* Det skal konkret overvejes, hvor længe det er nødvendigt at have personoplysningerne (hvis de ikke er nødvendige, så skal de slettes)
* Slettefrister skal angives for de forskellige kategorier af oplysninger
* Der skal ikke angives sletning for hele behandlingen
* Det forudsættes, at der er procedurer som sikrer, at der sker sletning i overensstemmelse med de fastsatte frister
* Bogføringsreglerne: 5 år + løbende kalenderår efter regnskabsårets afslutning
* Retskrav: 3 år efter afslutningen af opgaven
* Stamdata fra kunden bør ikke slettes før efter 5 år fra kundeforholdets ophør, så der er overensstemmelse med bogføringsreglerne
* E-mails kan typisk gemmes i 5 år afhængig af indhold

8) Hvis det er muligt en generel beskrivelse af tekniske og organisatoriske foranstaltninger

* Der skal i fortegnelsen være en beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger
* Eksempler kan være:
  + Arbejdsbetinget adgang
  + Al datatransmission og lagring af data sker krypteret
  + Kun de X personer, der aktuelt er sikkerhedsgodkendt, har adgang til de elektronisk registrerede oplysninger
  + Elektronisk registrerede oplysninger er lagret på en server, hvorpå der er installeret aktive virusscannere
  + Der er etableret backup og genetableringsprocedure for alle servere
  + Der er alene adgang til arbejdsstationer med individuelt brugernavn og password
  + Arbejdsstationer har screensaver password, og der er installeret antivirus program
  + Adgang er baseret på bruger id og et personligt password, der er minimum X antal tegn
  + Der foretages kontrol med afviste adgangsforsøg
  + Der bruges VPN og kryptering i forbindelse med fjernarbejdspladser og andre mobile enheder
  + Medarbejdertræning og videreuddannelse
  + Certificering af medarbejdere, der arbejder med persondata
  + Etablering af procedurer og politikker for behandling og kommunikation af personoplysninger