VEJLEDNING

FORTEGNELSE OVER BEHANDLINGSAKTIVITETER

**Fortegnelse over behandlingsaktiviteter:**

Databeskyttelsesforordningen kræver, at dataansvarlige og databehandlere skal føre fortegnelse over deres behandlinger af personoplysninger.

Fortegnelsespligten er som udgangspunkt en forpligtigelse overfor den dataansvarlige selv, altså en intern forpligtigelse for virksomheden eller organisationen. Men hvis Datatilsynet anmoder om fortegnelsen, skal denne kunne fremvises til enhver tid.

Formålet med at føre fortegnelse omhandler Databeskyttelsesforordningens krav til ansvarlighed. Det betyder, at det er den dataansvarlige, der har ansvaret for at forordningens krav overholdes. Samtidig skal dette kunne påvises/dokumenteres.

En fortegnelse vil uomtvisteligt give et overblik for den dataansvarlige, og på denne måde medvirke til, at forordningens krav til databeskyttelse overholdes. Herudover vil fortegnelser gøre det muligt at påvise, at disse krav overholdes.

**Formkrav:**

Det er et krav, at fortegnelsen skal foreligge både skriftligt og elektronisk. Dette betyder, at det ikke er nok blot at have fortegnelsen i et fysisk dokument. Dataansvarlige og databehandlere skal begge overholde formkravet.

**Undtagelse til fortegnelseskravet:**

Som udgangspunkt er små virksomheder eller organisationer med under 250 ansatte undtaget fra at føre en fortegnelse over behandlingsaktiviteter.

Dette udgangspunkt gælder dog ikke altid. Hvis en virksomhed eller en organisation foretager behandlingsaktiviteter, som er omfattet af én af nedenstående tre situationer, vil virksomheden altid være forpligtiget til at føre en fortegnelse:

Risiko for den registreredes rettigheder:

Hvis der foretages behandlingsaktiviteter, der sandsynligvis vil medføre en risiko for den registreredes rettigheder, skal der stadig føres en fortegnelse selvom virksomheden eller organisationen har under 250 ansatte.

Behandlingen af personoplysninger sker oftere end ”lejlighedsvist”:

Hvis behandlingen af personoplysninger sker oftere end ”lejlighedsvist”, er virksomheden eller organisationen forpligtet til at føre en fortegnelse, selvom denne har under 250 ansatte.

Personaleadministration, der indeholder behandling af personoplysninger, vil f.eks. ikke være lejlighedsvis behandling af personoplysninger.

*Denne undtagelse medfører, at udgangspunktet om, at virksomheder og organisationer med under 250 ansatte ikke skal føre en fortegnelse, bliver et meget indskrænket udgangspunkt. Det er dermed i praksis sjældent, at en virksomhed eller en organisation kan undlade at udarbejde og føre en fortegnelse over behandlingsaktiviteter.*

Der behandles følsomme personoplysninger eller oplysninger om strafbare forhold:

Hvis en behandling af personoplysninger indebærer en behandling af følsomme oplysninger eller personoplysninger om lovovertrædelser eller straffedomme, skal der føres en fortegnelse, selvom virksomheden eller organisationen har under 250 ansatte.

**Indholdskrav:**

Indholdskravene til fortegnelsen afhænger af, om man er dataansvarlig eller databehandler.

Krav til den dataansvarliges fortegnelse

Den dataansvarlige skal føre fortegnelse over de behandlingsaktiviteter, som denne er ansvarlig for. Fortegnelserne skal indeholde al databehandlingsaktivitet.

Fortegnelsen skal som minimum indeholde:

* Den dataansvarliges navn og kontaktoplysninger.

Hvis det findes relevant, skal også andre aktørers navne og kontaktoplysninger oplyses. Dette kan f.eks. være en databeskyttelsesrådgiver, en repræsentant for den dataansvarlige eller en fælles dataansvarlig.

* Formålene med hver enkelt behandling.

Hvis én bestemt behandling tjener flere formål, skal alle formål med behandlingen angives.

I nogle tilfælde vil der kunne samles flere behandlingsaktiviteter i samme fortegnelse. Dette forudsætter, at disse behandlingsaktiviteter kan formuleres og samles under ét formål. Dette betyder, at der kan føres en fortegnelse over behandlinger, der har samme formål – f.eks. kan *”personaleadministration”* fremgå som ét samlet formål for flere forskellige behandlinger med samme formål.

* Kategorierne af de registrerede og af personoplysningerne underlagt behandling.

Fortegnelsen skal inkludere en skildring af, hvilke kategorier af registrerede og personoplysninger, der behandles.

Angivelsen af kategorier vedrører hvilken gruppe af registrerede, der behandles oplysninger om. Dette kan f.eks. være ”patienter”, ”kunder”, ”børn”, ”ansøgere”, ”ansatte” og lignende.

Kategorien af personoplysninger vedrører hvilke personoplysninger, der behandles. Som minimum skal det belyses, hvorvidt der behandles almindelige personoplysninger, følsomme personoplysninger eller oplysninger om strafbare forhold (*for vejledning til denne kategorisering se Enkel-GDPRs vejledning om Personoplysninger og behandling heraf i step 1*). I forbindelse med kategoriseringen af de følsomme oplysninger, skal det specificeres hvilke følsomme oplysninger, der behandles. Det kan eksempelvis være følsomme oplysninger vedrørende religiøs overbevisning, helbredsoplysninger eller strafbare forhold.

* Modtagere ved videregivelse

Hvis/når personoplysninger videregives til andre, skal fortegnelsen inkludere oplysninger om disse modtagere. Det skal altså kunne klarlægges, om der sker videregivelse og i givet fald, hvem denne videregivelse sker til. Det er dog kun de videregivelser, der er regelmæssige, som skal anføres i fortegnelsen. Under samme punkt, skal fortegnelsen inkludere oplysninger om hvilke kategorier af personoplysninger, der bliver eller vil blive videregivet til den pågældende modtager. Hertil skal det fremgå, hvilke kategorier af registrerede, de pågældende personoplysninger vedrører.

* Overførelser til tredjelande eller internationale organisationer.

Hvis virksomheden på den ene eller den anden måde videregiver personoplysninger til tredjelande eller internationale organisationer, skal dette angives i fortegnelsen.

Sker en sådan overførelse på baggrund af fornødne garantier, skal dokumentation for disse garantier vedlægges fortegnelsen (*læs om disse garantier i Enkel-GDPRs vejledning om overførelse til tredjelande i step 5*).

* Angivelse af slettefrister

Som dataansvarlig skal du så vidt muligt angive de forventede slettefrister for sletning af personoplysninger. Slettefristerne skal angives for hver af de forskellige kategorier af personoplysninger, som du behandler.

Dette krav skal ses i forlængelse af, at det efter forordningen ikke er tilladt at opbevare eller behandle personoplysninger i et længere tidsrum, end hvad der vurderes som værende nødvendigt for behandlingsformålet. Dette betyder samtidig, at personoplysningerne skal slettes så snart behandlingen ikke længere stemmer overens med formålet.

* Angivelse af tekniske og organisatoriske foranstaltninger

Fortegnelsen skal indeholde en overordnet og generel beskrivelse af hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, som virksomheden/organisationen gennemfører for behandling af personoplysninger (*læs om gennemførelse af tekniske og organisatoriske sikkerhedsforanstaltninger i Enkel-GDPRs vejledning herom i step 8*).

Krav til databehandlerens fortegnelse

Med forordningen følger også et krav om, at databehandleren skal føre en fortegnelse over behandlinger.

Denne fortegnelse skal som minimum indeholde:

* Navn og kontaktoplysninger

Fortegnelsen skal indeholde angivelse af navn og kontaktoplysninger både på databehandleren, eller databehandlerne (hvis der er flere), samt på den dataansvarlige. Hvis det findes relevant, skal også andre relevante aktørers navne og kontaktoplysninger oplyses. Dette vil f.eks. være en databeskyttelsesrådgiver, en repræsentant for databehandleren, eller en repræsentant for den dataansvarlige.

* Kategorierne af behandlinger

Fortegnelsen skal indeholde de forskellige kategorier af behandlinger, som databehandleren behandler på vegne af den dataansvarlige.

* Angivelse af om der sker overførelse til et tredjeland eller en international organisation

Hvis databehandleren overfører personoplysninger til et tredjeland eller en international organisation, skal dette angives i fortegnelsen. Sker en sådan overførelse på baggrund af fornødne garantier, skal dokumentation for disse garantier vedlægges fortegnelsen (*læs om disse garantier i Enkel-GDPRs vejledning om overførelse til tredjelande i step 5*).

* Tekniske og organisatoriske foranstaltninger

Så vidt det er muligt, skal fortegnelsen indeholde en beskrivelse af de tekniske og organisatoriske foranstaltninger, som databehandleren foretager for behandlingen af personoplysninger.