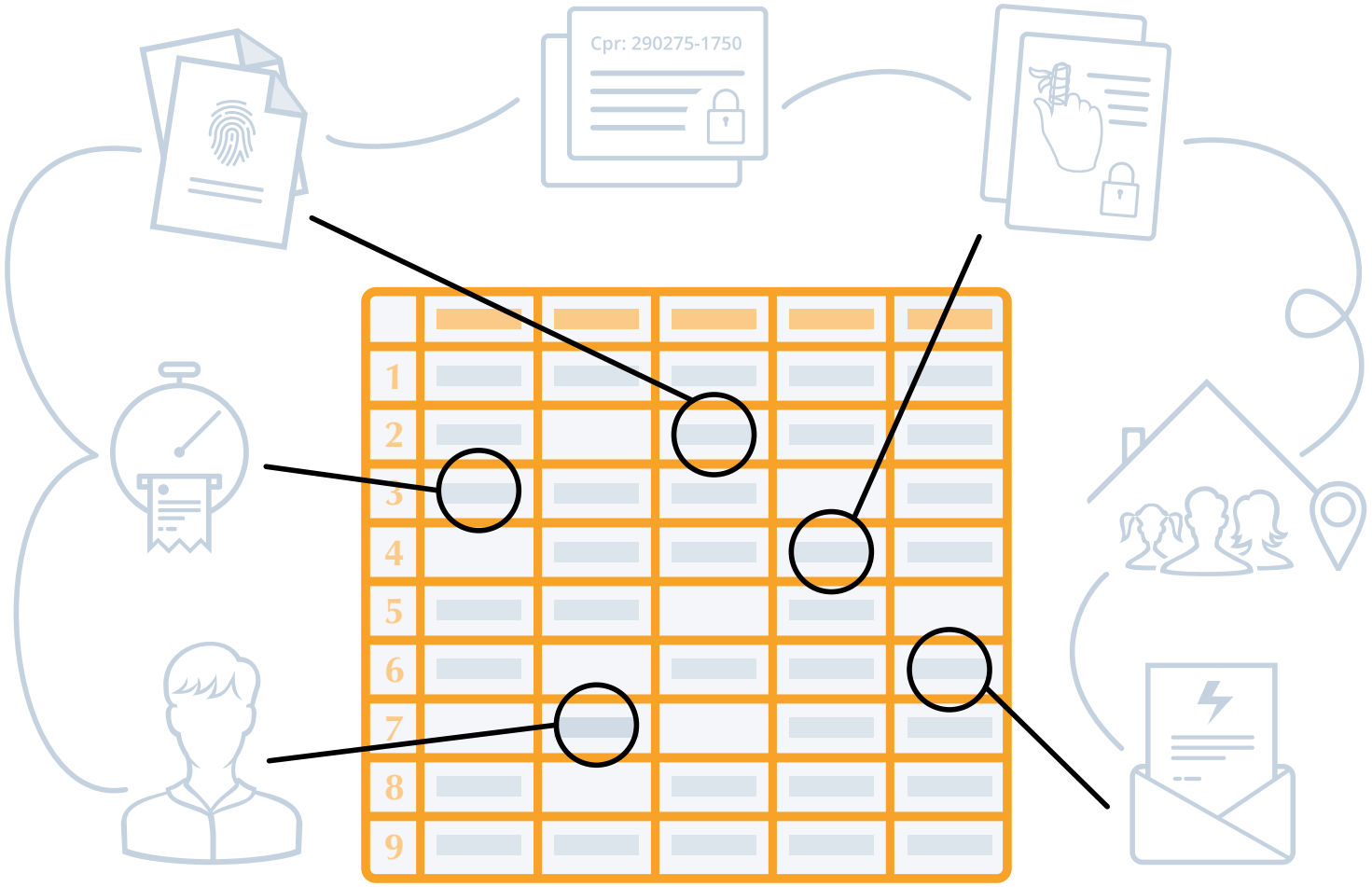

Tjekliste til GDPR-fortegnelsen:

Få overblik over de persondata, I behandler

Med en fortegnelse slår I to fluer med ét smæk. I opfylder jeres GDPR-pligt – og ikke mindst gør I resten af jeres GDPR-liv nemmere. For fortegnelsen giver jer overblik. Når I først har den grundlæggende fortegnelse på plads, kan I langt lettere opfylde andre krav, GDPR stiller til jer, blandt andet at føre en hændelseslog. Det er noget, som Datatilsynet interesserer sig for.

VISMA | DataLøn

Hvad, hvorfor og hvordan?

Hvad er en fortegnelse?
Se det som en slags aktuel, beskrivende lagerbeholdning. Fortegnelsen er jeres hvem, hvad, hvor over de persondata, I behandler og opbevarer på den ene, anden eller tredje måde.

Hvorfor en fortegnelse?
Selvfølgelig ikke bare fordi I skal, men fordi en kortlægning af, hvilke persondata I behandler i jeres virksomhed, vil få jer til at opdage, hvis og hvor der er huller i osten. Hvis man ikke ved, at der er noget galt, er det som bekendt svært at gøre noget ved det. Den køber Datatilsynet bare ikke, hvis de skulle komme forbi.

Hvordan ser en fortegnelse ud?
Der er frit slag, men en god måde at skabe overblik er at stille det op i en matrix. Det gør det også nemt at supplere med nye informationer. I skal tænke på fortegnelsen som et levende dokument.

Tjekliste til at opbygge jeres fortegnelse

Helt overordnet skal virksomhedens kontaktoplysninger fremgå – gerne med en specifik kontaktperson. Dertil skal følgende informationer med, og stiller I det op i en matrix, går I i gang med rækker og kolonner:

Hvis og hvilke persondata behandler I?

De fleste virksomheder vil her have ***flere overordnede kategorier, for eksempel "kunder" og "medarbejdere"****. Under hver af disse kategorier bør I udpensle præcis hvilke data, det drejer sig om.

Under "medarbejdere" kunne det være navn, adresse, cpr-nummer, lønoplysninger, testresultater, fagforeningsmedlemskab, log over adgangskort eller over mails.

Under "kunder" kunne det være e-mailadresser, mailkorrespondance, telefon-logs eller cookie-information fra hjemmesiden.

Gå jeres processer igennem med en tættekam for at få alle oplysningerne med.

Hvor dyr eller følsom er den enkelte oplysning?

Det vil sige, er personoplysningen almindelig (for eksempel navn), fortrolig (for eksempel CPR-nummer) eller følsom (for eksempel fagforeningsmedlemskab)? Det fortæller jer noget om, hvor godt I skal passe på den.

Hvor har I hver enkelt personoplysning fra?

Notér det ud for hver oplysning. Er det kunden eller medarbejderen selv, der har afgivet informationen? Eller er det jer som arbejdsgiver, der har indsamlet den?

***Bonustip:**
Laver I fortegnelsen i et regneark, kan I med fordel lave en fane for hver overordnede kategori.

Hvad er formålet med at have oplysningen?

Formålet med at opbevare en kundes e-mailadresse vil typisk være at kunne "administrere kundeforholdet", mens formålet med at opbevare medarbejdernes løn- og skatteoplysninger vil være at kunne udbetale korrekt løn.

Dette punkt i fortegnelsen er vigtigt, fordi GDPR stiller krav om, at formålet med hver enkelt oplysning skal være klart, tydeligt afgrænset og specifikt formuleret.

Hvad er jeres grundlag for at behandle oplysningen?

I skal altid have jeres hjemmel – jeres behandlingsgrundlag – på plads. For eksempel: Det er for at kunne leve op til en indgået kontrakt, at I behandler medarbejderens lønoplysninger. Eller: Det er på baggrund af indhentet samtykke, at I sender nyhedsbreve til jeres kunder.

Hvis I har problemer med at udfylde dette punkt i jeres fortegnelse, bør I overveje situationen nøje.

Hvornår og hvor ofte sletter I den givne persondata?

Notér i jeres fortegnelse, hvornår I sletter de enkelte persondata. For eksempel at videoovervågning slettes dagligt, eller at kontaktinformation på kunder slettes x måneder efter afsluttet opgave.

Husk, at I kun må opbevare persondata så længe det er relevant i forhold til jeres specifikke formål.

Og at I skal opstille klare regler for jeres sletteprocedurer og -frister. De regler kan I først beskrive, når I har overblik over alle de persondata, I behandler. Med andre ord når I har lavet jeres fortegnelse…

Hvor opbevarer I personoplysningerne?

På papir og/eller digitalt? Ligger digitale data eksternt, skal I sørge for at have databehandleraftaler på plads, og have styr på hvor deres datacentre befinder sig. Det er vigtigt at vide og notere, om det er inden eller uden for EU, da der er skrappe regler for, hvilke data der overhovedet må ligge uden for EU. Retsgrundlaget skal stå helt klart – og skrives ind i fortegnelsen.

Hvem videregiver I personoplysninger til?

Persondata skal generelt ikke deles med eksterne parter. Men når det er nødvendigt – for eksempel når man indberetter lønoplysninger til SKAT – skal det skrives ind i fortegnelsen, og lovgrundlaget skal noteres.

Sikkerhedsforanstaltninger

Hvad gør I aktivt for at sikre personoplysningerne? For eksempel elektronisk adgangsstyring og logning af brug, kryptering, fysisk sikkerhed som adgangskort og lås og slå. Hvis I har nedskrevne politikker og regler på dette område, kan I henvise til disse dokumenter.

Sådan kunne en enkelt række på medarbejderdata i en fortegnelse se ud. Det er et tænkt eksempel, der alene tjener til illustration af princippet.

Personoplysning	Kilde	Formål	Behandlingsgrundlag	Følsomhed	Sletning	Lagring	Videregivelse	Foranstaltninger
Logs fra adgangskort	Indsamles når adgangskort bruges i bygning	• Adgangskontrol • Sikkerhed (fx v. brand)	Legitim interesse	Almindelig	30 dage	Kortfirma A/S i Andeby, Andeland	Ingen. Dog til myndighed hvis del af en efterforskning	• Adgangsbegrænset til HR og nærmeste leder • Kryptering under transport

Har du brug for starthjælp?
Visma DataLøns jurister, der er specialister på det ansættelsesretlige område og GDPR, kan hjælpe dig med at komme videre med din virksomheds fortegnelse. Find ud af, hvor du ender og begynder med en indledende snak: Ring 72 27 90 16.

Du finder en række fokuserede GDPR-webinarer på dataløn.dk/gdpr-webinar