

Besvarelsen af interviewskemaet danner grundlag for virksomhedens vurdering i GAP-analysen.

1. Hvilke almindelige ikke-følsomme personoplysninger behandles?

Eksempler på almindelige ikke-følsomme personoplysninger:

- Generelle kontaktoplysninger, såsom navn, adresse, telefonnummer og fødselsdato.
- Oplysninger vedr. en persons økonomi, skattemæssige forhold og gældsforhold.
- Bankinformationer, såsom kontonumre.
- Uddannelsesrelaterede oplysninger, CV-relaterede oplysninger og generelle kvalifikationer.
- Generelle oplysninger vedr. familiære forhold.
- Stillingsbetegnelse, arbejdsområde, specialer, personlige produktions- og salgstal.

Vær opmærksom på, at der gælder særlige regler for behandling af CPR-numre. Du kan læse mere om dette på Datatilsynets hjemmeside.

2. Med hvilken lovhjemmel behandles ikke-følsomme almindelige personoplysninger?

- *Samtykke*: Personoplysninger behandles på baggrund af den registreredes skriftlige samtykke.
- *Opfyldelse af kontrakt*: Personoplysninger behandles med henblik på at opfylde en kontrakt - eksempelvis en ansættelseskontrakt eller købskontrakt.
- *Overholdelse af retlig forpligtelse*: Personoplysninger behandles for at overholde en retlig forpligtelse - eksempelvis i forbindelse med indberetning til SKAT eller opbevaring af personoplysninger for at leve op til bogføringslovens krav.
- *Beskyttelse af den registreredes vitale interesser*: Personoplysninger kan behandles på baggrund af denne lovhjemmel i tilfælde, hvor den registrerede eksempelvis pga. sygdom, bortrejse m.v. ikke er i stand til at meddele samtykke. Anvendes primært af offentlige myndigheder.
- *Beskyttelse af en anden fysisk persons vitale interesser*: som ovenstående med udgangspunkt i en anden impliceret person end den registrerede.
- *Udførelse af en opgave i samfundets interesse*: Personoplysninger behandles i forbindelse med opgaver af almen interesse - eksempelvis i statistisk, historisk eller videnskabeligt øjemed. Anvendes primært af offentlige myndigheder.
- *Som led i offentlig myndighedsudøvelse*: Anvendes af offentlige myndigheder.
- *På baggrund af interesseafvejning*: Personoplysninger behandles på baggrund af den dataansvarliges berettigede forretningsmæssige interesser, hvor den registreredes interesser og rettigheder ikke står i vejen for dette. Der er tale om en konkret afvejning, og du bør ved tvivl kontakte din rådgiver.

3. Med hvilket formål behandles oplysningerne?

Behandling af personoplysninger må kun ske til udtrykkeligt angivne og saglige formål.

Behandlingen skal ske med udgangspunkt i principperne om lovlighed, rimelighed og gennemsigtighed, og en senere behandling må ikke ske til formål, som er uforenelige med

de oprindelige formål. Et eksempel på et formål er HR- og administrationsrelaterede formål såsom rekruttering og ansættelse af nye medarbejdere eller salgs- og marketingrelaterede formål såsom opfyldelse af kontrakt mellem kunde og virksomhed.

4. Hvilke følsomme personoplysninger behandles?

Eksempler på følsomme personoplysninger er:

- Racemæssig eller etnisk oprindelse.
- Politisk, religiøs eller filosofisk overbevisning.
- Fagforeningsmæssige tilhørsforhold.
- Genetiske data.
- Væsentlige sociale problemer.
- Biometriske data.
- Helbredsoplysninger.
- Seksuelle forhold eller seksuel orientering.

Vær opmærksom på at personoplysninger vedrørende straffedomme og lovovertrædelser anses for en særlig kategori af personoplysninger, hvortil der kræves en særlig lovhjemmel for at behandling. Du bør kontakte din rådgiver for konkret rådgivning vedr. behandling af for eksempel straffeattester.

5. Med hvilken lovhjemmel behandles de følsomme personoplysninger?

- *Udtrykkeligt samtykke*: Personoplysninger behandles på baggrund af den registreredes aktivt, bekræftende samtykke.
- *Nødvendig til opfyldelse af forpligtelser og udøvelse af rettigheder vedrørende ansættelsesretlige forhold og lovgivning om social sikring og beskyttelse*: Oplysninger behandles med henblik på at opfylde virksomhedens forpligtelser vedr. eksempelvis overenskomstaftaler.
- *Beskyttelse af den registreredes vitale interesse, hvor den pågældende ikke fysisk eller juridisk er i stand til at give sit samtykke*: Personoplysninger kan fx behandles på baggrund af denne lovhjemmel i tilfælde, hvor den registrerede pga. sygdom, bortrejse m.v. ikke er i stand til at meddele samtykke. Anvendes primært af offentlige myndigheder.
- *Beskyttelse af en anden fysisk persons vitale interesse, hvor den pågældende ikke fysisk eller juridisk er i stand til at give sit samtykke*: Som ovenstående med udgangspunkt i en anden impliceret person end den registrerede.
- *Personoplysninger, som tydeligvis er blevet offentliggjort af den registrerede person selv*: Behandling af oplysninger, som den registrerede selv har offentliggjort.

Hvis du behandler følsomme personoplysninger, bør du kontakte din rådgiver, da det er vigtigt at have en lovhjemmel for behandling og opbevaring af følsomme personoplysninger.

6. Med hvilke(t) formål behandles oplysningerne?

Behandling af følsomme personoplysninger skal ligesom almindelige ikke-følsomme personoplysninger ske til udtrykkeligt angivne og saglige formål og må ikke behandles til andre formål end de oprindeligt angivne formål (se spørgsmål 3).

7. Hvordan indsamles personoplysningerne?

Eksempler på hvorfra data kan indhentes:

- *Fra den registrerede selv:* fx via e-mail, ansøgninger, kontrakter, via hjemmesider m.v.
- *Fra tredjemand:* Fx via offentligt tilgængelige databaser eller fra andre virksomheder.
- *Via onlineindsamling (såsom via sociale medier):* Fx via sociale medier såsom Facebook og LinkedIn, hjemmesider m.v.
- *Internt i virksomheden:* Fx fra en anden afdeling. Denne valgmulighed er relevant i forhold til at forstå, hvordan virksomheden deler personoplysninger internt.

8. Hvordan behandles personoplysningerne?

Oplys om personoplysninger behandles og opbevares manuelt (fx i kartoteker eller ringbind), digitalt (fx som filer på computeren) eller digitalt i et system (systembehandling). Der kan også være tale om en kombination af de forskellige valgmuligheder.

9. Er den registrerede oplyst om behandlingen?

Den registrerede (se spørgsmål 13) skal til enhver tid være informeret om behandlingen af dennes personoplysninger, hvilket skal være oplyst på en tilgængelig, klar og letforståelig måde, hvilket skaber gennemsigtighed om virksomhedens behandling af personoplysninger.

10. Videregives personoplysninger?

Redegør for om personoplysninger videregives og til hvem. Du bedes angive om personoplysninger videregives til lande indenfor eller udenfor EU. Du bør i denne forbindelse være opmærksom på, at der gælder særlige regler for videregivelse af personoplysninger til lande udenfor EU. Orienter dig på datatilsynets hjemmeside eller kontakt din rådgiver.

11. Anvendes en databehandler i denne proces?

En databehandler behandler personoplysninger på vegne af den dataansvarlige og på baggrund af den dataansvarlige instruks. Personoplysninger kan fx videregives til behandling hos en databehandler i forbindelse med ekstern lønadministration. Kontakt din administrator, hvis du er i tvivl om, hvilke databehandler(e) I anvender.

12. Er der lavet en databehandleraftale?

En databehandleraftale er en kontrakt eller et andet retligt bindende dokument, som regulerer forholdet mellem den dataansvarlige og databehandleren. Databehandleraftalen fastsætter forholdet mellem den dataansvarlige og databehandleren og skal leve op til en række særlige krav. Du bør kontakte din rådgiver for at sikre dig, at dine databehandleraftaler lever op til kravene, eller at der for fremtiden udarbejdes tilstrækkelige databehandleraftaler.

13. Hvilken kategori er den registrerede?

Den eller de registrerede er den eller de personer, som den dataansvarlige behandler personoplysninger om. Eksempler på kategorier af registrerede er medarbejdere, eksterne konsulenter, samarbejdspartnere, kunder, forbrugere, borgere, ansøgere m.v.

14. Hvor lang tid opbevares personoplysningerne?

Generelt gælder det, at personoplysninger ikke bør opbevares længere end, hvad der er nødvendigt for at opfylde formålene med behandlingen af de pågældende personoplysninger. Derudover skal du være opmærksom på, at der kan gælde specifikke lovmæssige krav for opbevaring af visse personoplysninger (eksempelvis kravene i bogføringsloven).

15. Slettes data? Hvis ja, vedhæft sletteprocedure

Hvis I har en procedure for sletning af personoplysninger, bedes I uploade denne. En sletteprocedure bør blandt andet indeholde information om:

- Slettefrister for personoplysninger.
- Ansvar for sletning af personoplysninger.
- Om sletning (opbevaring) sker på baggrund lovmæssige krav.

16. Beskriv tekniske og organisatoriske sikkerhedsforanstaltninger

Beskriv de tekniske og organisatoriske sikkerhedsforanstaltninger der gælder for jeres indsamling, behandling og opbevaring af personoplysninger. I kan i denne forbindelse eksempelvis beskrive de fysiske sikkerhedsforanstaltninger, der gøres brug af, fx aflåste rum, kabinetter m.v., eller hvordan I gør brug af adgangskontrol, låste filer/mapper på computere m.v. samt IT-sikkerhed, der benyttes til ift. opbevaring af data. Det er eksempelvis adgangsbegrænsninger i systemer, IT-programmer og firewalls. Jeres tekniske og organisatoriske sikkerhedsforanstaltninger skal sikre, at der ikke sker utilsigtet tilintetgørelse, bortskaffelse eller misbrug af personoplysninger, samt at personoplysninger ikke kommer til uvedkommendes kendskab.

17. Hvilke tredjelande overføres data til?

Tredjelande er alle lande uden for EU og (EØS). Hvis der overføres personoplysninger til USA eller Indien, sker der altså en overførsel til et tredjeland.

18. Beskriv forventede tidsfrister og frekvens for sletning

Beskriv virksomhedens tidsfrister og regler for opbevaring og sletning af personoplysninger. Det er virksomheden eller organisationen selv, der er ansvarlig for at fastsætte tidsfrister for sletning, således at dette sker i overensstemmelse med reglerne.

19. Hvor opbevares data?

- *Interne servere*: Eksempelvis en filserver og IT-systemer hostet på egne servere.
- *Cloud*: Et IT-system hostet af andre, eksempelvis Dropbox, SharePoint og Microsoft 365.
- *Databehandler*: Personoplysninger, der opbevares hos konsulenter, samarbejdspartnere eller andre leverandører, der fungerer som databehandler for din virksomhed.