Vejledning

|  |
| --- |
| 14. august 2020 |

**Fortegnelse vedrørende personaleadministration**

**Indhold**

[1. Krav om fortegnelse 1](#_Toc49424174)

[2. I elektronisk form 1](#_Toc49424175)

[3. Fortegnelsens indhold 2](#_Toc49424176)

[1. Navn og kontaktoplysninger for den dataansvarlige 2](#_Toc49424177)

[2. Formålene med behandlingen af oplysningerne 2](#_Toc49424178)

[3. Kategorier af registrerede og kategorier af personoplysninger 2](#_Toc49424179)

[4. Kategorier af modtagere ved videregivelse 3](#_Toc49424180)

[5. Overførsler til tredjelande og internationale organisationer 3](#_Toc49424181)

[6. Sletning, herunder slettefrister 3](#_Toc49424182)

[7. Tekniske og organisatoriske sikkerhedsforanstaltninger 4](#_Toc49424183)

[Bilag: Eksempel på en fortegnelse over personaleadministration i en privat virksomhed 6](#_Toc49424184)

# 1. Krav om fortegnelse

Langt de fleste virksomheder skal have en *intern* fortegnelse over deres be­handling af personoplysninger. En virksomhed skal ifølge Datatilsynet typisk have en sådan fortegnelse vedrørende sin personaleadministration.

Fortegnelsen kan hjælpe virksomheden med at sikre og påvise, at databeskyttelsesreglerne overholdes.

I denne vejledning gennemgås kravene til fortegnelsen med fokus på personaleadministrationen. I bilaget er et eksempel på, hvordan fortegnelsen kan se ud. Da der netop er tale om et eksempel, er det vigtigt, at I tilpasser fortegnelsen til jeres virksomheds konkrete forhold.

Datatilsynet har udgivet en generel ”*Vejledning om fortegnelse”*, der også indeholder eksempler, der vedrører personaleadministrationen. Du kan finde denne vejledning på Datatilsynets hjemmeside <https://www.datatilsynet.dk/vejledninger/vejledninger-databeskyttelsesforordningen/>.[[1]](#footnote-1)

# 2. I elektronisk form

Fortegnelsen skal være *skriftlig* og *elektronisk*. Det er altså ikke tilstrækkeligt, at virksomheden kun har fortegnelsen i et fysisk dokument. Fortegnelsen kan f.eks. laves i et skema (f.eks. i Excel), eller i et almindeligt tekstbehandlingsdokument (f.eks. i Word).

Selvom fortegnelsen er intern, skal virksomheden stille den til rådighed for Datatilsynet, hvis Datatil­synet beder om at se den.

# 3. Fortegnelsens indhold

Fortegnelsen skal omfatte *al virksomhedens behandling af personoplysninger* ved personaleadmi­nistration, herunder[[2]](#footnote-2):

Almindelige oplysninger, der alene er omfattet af artikel 6 i databeskyttelsesforordningen.

Særlige kategorier af oplysninger, der også er omfattet af artikel 9 (særligt følsomme personoplysninger):

* race eller etnisk oprindelse
* politisk, religiøs eller filosofisk overbevisning
* fagforeningsmæssige tilhørsforhold
* genetiske data
* biometrisk data med henblik på entydigt at identificere en fysisk person
* helbredsoplysninger
* seksuelle forhold eller seksuel orientering

Oplysninger om strafbare forhold, der er omfattet af artikel 10 og databeskyttelseslovens § 8. Oplysninger om CPR-nummer, der er omfattet af databeskyttelseslovens § 11.

Fortegnelsen skal mindst indeholde følgende *7 punkter*:

## 1. Navn og kontaktoplysninger for den dataansvarlige

* 1. Virksomheden er dataansvarlig for behandlingen af oplysningerne om virksomhedens medarbejdere mv. i forbindelse med personaleadministrationen. Virksomheden kan her oplyse virksomhedens navn, CVR-nummer samt kontaktoplysninger som adresse, hjemmeside, telefonnummer samt e-mail.

Når det er relevant, skal der også angives navn- og kontaktoplysninger på en fælles dataansvarlig, den dataansvarliges repræsentant[[3]](#footnote-3) og/eller databeskyttelsesrådgiveren.

## 2. Formålene med behandlingen af oplysningerne

I en fortegnelse over personaleadministration vil det være nok at angive, at formålet er ”personaleadministration”.

## 3. Kategorier af registrerede og kategorier af personoplysninger

Kategorier af registrerede vil f.eks. være:

* jobansøgere
* nuværende medarbejdere
* tidligere medarbejdere
* pårørende

For at overholde kravet om en beskrivelse af kategorier af personoplysninger vurderer Datatilsynet, at virksomheden som minimum skal angive, om de personoplysninger, der behandles alene er omfattet af artikel 6, eller om oplysningerne - foruden at være omfattet af artikel 6 – også er omfattet af artikel 9 eller artikel 10, jf. ovenfor i pkt.3.:

1. almindelige oplysninger (art. 6),
2. særlige kategorier af oplysninger (særligt følsomme personoplysninger) (også art. 9) og/eller
3. oplysninger om strafbare forhold (art. 10).

For så vidt angår de særlige kategorier af oplysninger i artikel 9 skal der specificeres hvilke kategorier af oplysninger virksomheden behandler. Hvis virksomheden f.eks. alene behandler helbredsoplysninger, skrives ”helbredsoplysninger” i fortegnelsen. Det er også muligt at opliste alle kategorier og så afkrydse de relevante.

Herudover kan du vælge at tydeliggøre, hvilke oplysninger der er tale om, f.eks. medarbejderens identifikationsoplysninger, oplysninger om løn, ferie og andet fravær mv. Se også eksemplet sidst i vejledningen.

## 4. Kategorier af modtagere ved videregivelse

Hvis virksomheden videregiver eller vil videregive personoplysninger ved personaleadministrationen, skal du oplyse kategorier af modtagere i fortegnelsen.

Kun de overførsler, der er *regelmæssige*, skal anføres i fortegnelsen, f.eks.

* Offentlige myndigheder, fx SKAT
* Pensionsselskaber
* BS - med henblik på betalingsformidling

Det skal fremgå af fortegnelsen, hvilke kategorier af personoplysninger, der bliver eller vil blive videregivet til den pågældende modtager. I tilknytning hertil skal det fremgå, hvilke kategorier af registrerede, de pågældende oplysninger vedrører. Se et eksempel i bilaget.

## 5. Overførsler til tredjelande og internationale organisationer

Virksomheden skal klarlægge, om personoplysninger vil blive overført til tredjelande eller internationale organisationer. Dette skal i så fald fremgå af fortegnelsen.

Hvis dette punkt er relevant for jeres virksomhed, kan du læse mere om overførsler til tredjelande og internationale organisationer i Datatilsynets ”Vejledning om fortegnelse”. Her finder du også en nærmere gennemgang af begreberne ”tredjelande” og ”internationale organisationer”. [[4]](#footnote-4)

## 6. Sletning, herunder slettefrister

Hvis det er muligt, skal du oplyse de forventede tidsfrister for sletning. Slettefristerne skal angives for de forskellige kategorier af oplysninger om de forskellige kategorier af registrerede, som virksomheden behandler i forbindelse med personaleadministrationen.

Databeskyttelsesreglerne indeholder et generelt krav om, at en virksomhed ikke må opbevare oplysninger på en måde, der giver mulighed for at identificere den registrerede i længere tid end det, der er nødvendigt til behandlingsformålet. Virksomheden skal derfor løbende overveje, om det er nødvendigt at opbevare en oplysning – og ellers slette den. Har virksomheden fastsat generelle slettefrister, følger det dog af Datatilsynets nuværende praksis, at virksomheden ikke har pligt til løbende at gennemgå samtlige sager, dokumenter mv. med henblik på at sikre, at der ikke behandles oplysninger i strid hermed. Det forudsætter dog, at virksomheden har procedurer som sikrer, at det sker sletning i overensstemmelse med de fastsatte frister.[[5]](#footnote-5)

Det er Dansk Erhvervs vurdering, at en virksomhed som udgangspunkt må have mulighed for at opbevare en personalesag 5 år efter medarbejderens fratræden som følge af den almindelige 5-årige forældelsesfrist i ansættelsesretlige sager. Virksomheden skal også overholde bogføringslovens regler, herunder opbevaring af relevante oplysninger i denne sammenhæng i 5 år efter et regnskabsårs afslutning. Samtidig kan der være eksempler, hvor særlige forhold gør længerevarende opbevaringsperiode relevant, f.eks. verserende arbejdsskadesager, uafsluttede retssager eller arbejdsretlige tvister mellem medarbejderen og virksomhed, pensionsforpligtelser, dagpengerefusion og udbetaling af tilgodehavender.

## 7. Tekniske og organisatoriske sikkerhedsforanstaltninger

Det er efter databeskyttelsesreglerne et krav, at behandling af personoplysninger skal ske med tilstrækkelig sikkerhed. Hvis det er muligt, skal fortegnelsen indeholde en generel beskrivelse af de tekniske og organisatori­ske sikkerhedsforanstaltninger, der er reguleret i forordningens generelle afsnit om behandlingssikker­hed.

Når virksomheden fastlægger det tekniske og organisatoriske sikkerhedsniveau, skal der tages højde for:

* det aktuelle tekniske niveau
* implementeringsomkostningerne
* behandlingens karakter, omfang, sammenhæng og formål samt
* risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsret­tigheder.

Datatilsynet har givet følgende eksempler på foranstaltninger i ”*Vejledningen om fortegnelse”*:

|  |
| --- |
| **Tekniske foranstaltninger** |
| * Arbejdsbetinget adgang. * Al datatransmission og lagring af data sker krypteret. * Kun de X personer, der aktuelt er sikkerhedsgodkendt i henhold til sikkerhedscirkulæret XX, har adgang til de elektronisk registrerede oplysninger. * De elektronisk registrerede oplysninger er lagret på en server, hvor der er installeret aktive virusscannere med henblik på løbende automatisk virustjek mv. * Der er etableret backup og genetableringsprocedure for alle servere. * Der er alene adgang til arbejdsstationer med individuelt brugernavn og password * Arbejdsstationer har screensaverpassword, og der er installeret antivirusprogram * 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 devices. |
| **Organisatoriske foranstaltninger** |
| * Medarbejdertræning og videreuddannelse. * Certificering af medarbejdere, der arbejder med persondata. * Etablering af procedurer og politikker for behandling og kommunikation af personoplysninger. |

Dansk Erhverv har udarbejdet en selvstændig ”*Vejledning om sikkerhedspolitik i forbindelse med personaleadministration*”. Læs mere i denne vejledning, der indeholder et eksempel på en sådan sikkerhedspolitik.

Datatilsynet har udgivet en vejledning om behandlingssikkerhed og databeskyttelse gennem design og standardindstillinger, hvor sikkerhedskravene er beskrevet.[[6]](#footnote-6)

# Bilag: Eksempel på en fortegnelse over personaleadministration i en privat virk­somhed

|  |
| --- |
| **Fortegnelse over behandling af personoplysninger ved personaleadministration hos [virksomhed]**  [dato] |

|  |
| --- |
| **1. Dataansvarlig** |

**Navn og kontaktoplysninger:**

Virksomhedens navn, CVR-nummer samt kontaktoplysninger (adresse, hjemmeside, telefonnummer og e-mail).

*Hvis relevant*: Virksomhedens databeskyttelsesrådgiver (DPO) samt dennes kontaktoplysninger - navn, adresse, hjemmeside, telefonnummer og e-mail.

*Hvis relevant*: Den fælles dataansvarlige samt dennes kontaktoplysninger (adresse, hjemmeside, telefonnummer og e-mail.

*Hvis relevant*: Den dataansvarliges repræsentant samt dennes kontaktoplysninger - adresse, hjemmeside, telefonnummer og e-mail[[7]](#footnote-7)

|  |
| --- |
| **2. Formål med behandlingerne** |

Personaleadministration hos [virksomhed], herefter ”virksomheden”.

|  |
| --- |
| **3. Kategorier af registrerede og kategorier af oplysninger** |

Virksomheden behandler oplysninger om følgende kategorier af registrerede personer:

* Jobansøgere
* Nuværende medarbejdere
* Tidligere medarbejdere
* Pårørende

*[Nedenfor tilrettes med de relevante oplysninger, se vejledningens pkt. 2 og 3. OBS, at der altid skal være et lovligt formål for at en oplysning kan behandles.]*

**Jobansøgere**

Oplysninger, som behandles om jobansøgere:

* Identifikationsoplysninger, herunder navn, telefonoplysninger og e-mail
* Oplysninger, som indgår i jobansøgningen, herunder kompetenceprofil, stilling og arbejdssted, CV-oplysninger, uddannelse, faglige kvalifikationer og lønforhold samt begrundelser herfor.
* Helbredsoplysninger
* Personlighedstests
* […]

**Nuværende medarbejdere**

Oplysninger, som behandles om nuværende medarbejdere:

* Identifikationsoplysninger, herunder navn, adresse, telefonoplysninger og e-mail
* Stilling og arbejdssted.
* Ansættelse og beskæftigelse.
* Vagt- og tjenestetider.
* Løn- og pensionsforhold.
* Ferie og andet fravær.
* Skatteforhold.
* Løntilskud.
* Oplysninger af relevans for lønindeholdelse.
* Personalepapirer.
* Uddannelse.
* Sygefravær.
* Fradrag i lønnen (fx betaling for kantineordning eller medarbejder­-pc).
* Arbejdsskader, fleksjob, ansættelse på særlige vilkår, fx ved handicap. (NB: Se også særlige kategorier af oplysninger nedenfor).
* Udbetaling af løn, herunder lønrefusioner mv.
* Personaleadministrative oplysninger, herunder uddannelse og kvalifikationer, jobøn­sker, bedømmelser, beskæftigelse, tillidshverv, lån af diverse effekter, eventuelle ad­varsler og lignende.
* Kurser, kompetenceprofil, medarbejderudviklingssamtaler.
* Oplysning om sikkerhedsgodkendelse.
* […]

Virksomheden behandler endvidere følgende typer af særlige kategorier af oplysninger (databeskyttelsesforordningens art. 9):

* Helbredsoplysninger
* Fagforeningsmæssige tilhørsforhold
* […]

Virksomheden behandler oplysninger om strafbare forhold og lovovertrædelser (databeskyttelsesforordningens art. 10), herunder i straffeattester.

Virksomheden behandler også CPR-nummer (databeskyttelseslovens § 11).

**Tidligere medarbejdere**

Oplysninger, som behandles om tidligere medarbejdere:

[ …]

**Pårørende**

Oplysninger, som behandles om pårørende:

* Navn og kontaktoplysninger, herunder adresse, telefonoplysninger og e-mail

|  |
| --- |
| **4. Modtagere af personoplysningerne** |

Kategorier af modtagere, som oplysningerne er eller vil blive videregivet til, herunder modta­gere i tredjelande og internationale organisationer:

*[Nedenfor kan ses en række eksempler på modtagere. Modtagerne skal tilrettes de modtagere, der er relevante for virksomheden. Samtidig skal det oplyses, hvilke oplysninger, der videregives til disse modtagere. Her er et eksempel vedr. virksomhedens videregivelse af oplysninger til SKAT:*

***”SKAT***

* *Videregivelsen omfattet følgende personoplysninger om medarbejdere:*
  + *Identifikationsoplysninger, herunder navn og adresse*
  + *Stilling og arbejdssted*
  + *Lønforhold*
  + *Skatteforhold*
  + *CRP-nummer*
* *Videregivelse af følgende oplysninger om tidligere medarbejdere*
  + *[ ]*

*Der videregives ikke oplysninger om øvrige kategorier af registrerede til SKAT.”]*

* Offentlige myndigheder [angiv så vidt muligt myndighedens navn, fx SKAT]
* Arbejdsmarkedets Tillægspension (ATP)
* Feriepengeinfo
* Danmarks Statistik
* Nemkonto
* Pensionskasser
* Banker [så vidt muligt navne]
* Forsikringsselskaber [så vidt muligt navne]
* [Foreninger]
* Tillidsrepræsentanter og faglige organisationer
* Arbejdsskadestyrelsen (anmeldelser om arbejdsskader)
* Arbejdsgivernes Uddannelsesbidrag (AUB)
* Arbejdsmarkedsstyrelsen (jobskabelsesordninger)
* Relevante kommuner vedr. f.eks. dagpengerefusion
* Virk.dk
* Indkomstregisteret
* DA-Barsel og/eller Barsel.dk
* Virksomhedens eksterne revision
* Virksomhedens eksterne rådgivere, herunder advokat/Dansk Erhverv
* [Øvrige]

Virksomheden kan i øvrigt overlade oplysninger til evt. databehandler(e), fx et lønbureau.

|  |
| --- |
| **5. Overførsler til tredjelande og/eller internationale organisationer** |

Nej [X]   
JA [ ]

*[Hvis JA: Angiv overførsler af personoplysninger til et tredjeland eller en international orga­nisation. Ved overførsler efter reglerne i databeskyttelsesforordningens art. 49, stk. 1, 2. af­snit angives også dokumentation for passende garantier. Læs mere herom i Datatilsynets ”Vejledning om fortegnelse”.]*

|  |
| --- |
| **6. Sletning** |

*[Hvis muligt, angives tidspunkt for sletning af oplysningerne:]*

Personoplysninger om medarbejdere og tidligere medarbejdere slettes [5 år] efter ansættelsesforholdets ophør hos virksomheden.

Oplysninger om jobansøgere, som får afslag på ansættelse, slettes senest [6 måneder] efter afslaget.

Virksomheden opbevarer endvidere oplysninger omfattet af bogføringsloven i overensstemmelse med reglerne i denne lovgivning.

Hvis der er en saglig grund til at opbevare oplysninger i længere tid, kan dette ske.

|  |
| --- |
| **7. Tekniske og organisatoriske sikkerhedsforanstaltninger** |

[Hvis det er muligt, skal der gives en generel beskrivelse af tekniske og organisatoriske sikkerhedsforanstaltninger. Punktet kan udfyldes med inspiration i afsnit 3 pkt. 7. Dansk Erhverv har også udarbejdet en ”*Vejledning om sikkerhedspolitik i forbindelse med personaleadministration*”, der indeholder et eksempel på en sikkerhedspolitik.]

1. Denne vejledning er udarbejdet i forlængelse af Datatilsynets ”Vejledning om fortegnelse” udgivet i august 2020. Alle henvisninger er således til denne version, der erstattede Datatilsynets ”Vejledning om fortegnelse” fra januar 2018. [↑](#footnote-ref-1)
2. Du kan læse mere om de forskellige typer af personoplysninger i databeskyttelsesforordningens artikel 6, 9 og 10. Se også Datatilsynets vejledning fra oktober 2017 om Databeskyttelsesforordningen (pkt. 3.0). [↑](#footnote-ref-2)
3. En repræsentant er en fysik eller juridisk person, som repræsenterer f.eks. en dataansvarlig virksomhed fsva. forpligtelser i medfør af databeskyttelsesforordningen. [↑](#footnote-ref-3)
4. Ved overførsel efter artikel 49, stk. 1, andet afsnit om ”fornødne garantier” skal dokumentation vedlægges. Læs mere i *Vejledning om overførsel af personoplysninger til tredjelande* på Datatilsynets hjemmeside. [↑](#footnote-ref-4)
5. Se Datatilsynets ”Vejledning om fortegnelse”, s. 10. [↑](#footnote-ref-5)
6. Vejledning Behandlingssikkerhed Databeskyttelse gennem design og standardindstillinger, juni 2018. [↑](#footnote-ref-6)
7. Den dataansvarliges ”repræsentant” dækker over en fysisk eller juridisk person etableret i EU, der er skriftligt udpeget af den dataansvarlige og repræsenterer denne, hvad angår den dataansvarliges forpligtelser i medfør af forordningen. Se evt. nærmere i Datatilsynets ”Vejledning om fortegnelse”. [↑](#footnote-ref-7)