SOLRØD KOMMUNE

CENTER FOR HR, POLITIK
OG DIGITALISERING

# DATABEHANDLERAFTALE

I henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen) med henblik på databehandlerens behandling af personoplysninger

Mellem

Solrød Kommune
Solrød Center 1
2680 Solrød Strand
CVR. nr.: 68534917
(herefter "den dataansvarlige")

Og

[Databehandlerens navn]
[adresse]
[postnr. og by]
CVR. nr.: [XXXX]
(herefter "databehandleren")

der hver især er en "part" og sammen udgør "parterne"
Parterne har aftalt følgende standardkontraktsbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder:

**1. Præambel**

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.

2. Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).

3. I forbindelse med leveringen af [tjeneste/system] behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.

5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.

6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.

7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.

8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.

9. Bilag D indeholder en beskrivelse af databehandlerkæden.

10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.

11. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

**Kommenteret [MRS1]:** Bilag D er ændret fra at indeholde bestemmelser vedrørende andre aktiviteter, som ikke er omfattet af bestemmelserne, til at indeholde en beskrivelse af databehandlerkæden.

**2. Den dataansvarliges rettigheder og forpligtelser**

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes[1] nationale ret og disse Bestemmelser.

2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.

3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

**3. Databehandleren handler efter instruks**

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.

2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

**4. Fortrolighed**

1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.

2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

1 Henvisninger til "medlemsstat" i disse bestemmelse skal forstås som en henvisning til "EØS medlemsstater".

**5. Behandlingssikkerhed**

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

   Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

   a. Pseudonymisering og kryptering af personoplysninger

   b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

   c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

   d. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.

3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

   Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

**6. Anvendelse af underdatabehandlere**

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).

2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige.

3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedr. tilføjelse eller udskiftning af underdatabehandlere med mindst 60 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B. I forbindelse med tilføjelse eller udskiftning af underdatabehandlere skal databehandleren ajourføre og fremsende et opdateret bilag B og D til den dataansvarlige.

4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

   Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

6. Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

**Kommenterede [MRS2]:** Tilføjelse til Datatilsynets standard skabelon

7. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

**7. Overførsel til tredjelande eller internationale organisationer**

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.

2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:

   - overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
   - overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
   - behandle personoplysningerne i et tredjeland

4. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.5.

5. Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

**8. Bistand til den dataansvarlige**

1. Databehandlerens bistand til den dataansvarlige inden for rammerne af denne aftale er lovpligtig, jf. artikel 28, stk. 3, litra f. og dermed påregnelig. Nedenstående og lignende ydelser er således omkostningsfrie for den dataansvarlige.

**Kommenterede [MRS3]:** Tilføjelse til Datatilsynets standard skabelon

2. Databehandleren bistår, under hensyntagen til behandlingens karakter, den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III.

   Dette indebærer, at databehandleren skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

   - oplysningspligten ved indsamling af personoplysninger hos den registrerede
   - oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
   - indsigtsretten
   - retten til berigtigelse
   - retten til sletning ("retten til at blive glemt")
   - retten til begrænsning af behandling
   - underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
   - retten til dataportabilitet
   - retten til indsigelse
   - retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

3. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:

   - den dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

   - den dataansvarliges forpligtelse til uden unødig forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder

   - den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)

   - den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at

behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

4. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 8.1. og 8.2.

**9. Underretning om brud på persondatasikkerheden**

1. Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

2. Databehandlerens underretning til den dataansvarlige skal om muligt ske straks efter, og senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.

3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:

   - karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger

   - de sandsynlige konsekvenser af bruddet på persondatasikkerheden

   - de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

4. Parterne skal i bilag C angive yderligere information, som ikke fremgår ovenfor, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

**10. Sletning og returnering af oplysninger**

1. Den dataansvarlige ejer til hver tid data, og træffer beslutning om, hvorvidt der skal ske sletning eller tilbagelevering af personoplysningerne efter, at behandlingen af personoplysningerne er ophørt i medfør af Hovedaftalen. Hvis den dataansvarlige ikke meddeler databehandleren inden Hovedaftalens ophør, hvorvidt data skal slettes eller tilbageleveres, forventes det i overensstemmelse

med forordningens bestemmelser, at data slettes hos databehandleren og dennes eventuelle underdatabehandlere når opbevaringen ikke længere er nødvendig iht. formålet.

2. Den dataansvarlige kan inden Hovedaftalens ophør skriftligt meddele databehandleren, hvorvidt alle personoplysningerne skal tilbageleveres til den dataansvarlige. I de tilfælde, hvor personoplysningerne tilbageleveres til den dataansvarlige, skal databehandleren ligeledes slette eventuelle kopier. Databehandleren skal sikre, at eventuelle underdatabehandlere ligeledes efterlever den dataansvarliges meddelelse.

**Kommenterede [MRS4]:** Ændret iht. Datatilsynets standard skabelon

**11. Revision, herunder inspektion**

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.

2. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmeret angivet i Bilag C.7. og C.8.

3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

**12. Parternes aftale om andre forhold**

1. Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

**13. Ikrafttræden og ophør**

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.

2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.

3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.

4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 10.1, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.

5. Underskrift

På vegne af den dataansvarlige

| | |
|---|---|
| Navn | Martin Green Jensen |
| Stilling | Centerchef for HR, Politik og Digitalisering |
| Telefonnummer | 56182355 |
| E-mail | mgj@solrod.dk |
| Dato | [DATO] Underskrift: |

**Kommenterede [MRS5]:** Ændret iht. Datatilsynets standard skabelon. Datofelt tilføjet iht. pkt. 13.1.

På vegne af databehandleren

| | |
|---|---|
| Navn | [NAVN] |
| Stilling | [STILLING] |
| Telefonnummer | [TELEFONNUMMER] |
| E-mail | [E-MAIL] |
| Dato | [DATO] Underskrift: |

**Kommenterede [MRS6]:** Ændret iht. Datatilsynets standard skabelon. Datofelt tilføjet iht. pkt. 13.1.

**14. Kontaktpersoner hos den dataansvarlige og databehandleren**

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

Kontaktperson hos den dataansvarlige:

| | |
|---|---|
| Navn | Digitalisering |
| Telefonnummer | 56182000 |
| E-mail | digitalisering@solrod.dk |

Ved underretning om sikkerhedsbrud, jf. pkt. 10.1, skal følgende mailadresse altid anvendes:
sikkerhedsbrud@solrod.dk

**Kommenteredе [MRS7]:** Tilføjelse iht. Datatilsynets standard skabelon.

Kontaktperson hos databehandleren:

Navn
Stilling
Telefonnummer
E-mail

## Bilag A Oplysninger om behandlingen

[BEMÆRK: I TILFÆLDE AF FLERE BEHANDLINGSAKTIVITETER, SKAL DISSE OPLYSNINGER FREMGÅ FOR HVER ENKELT BEHANDLINGSAKTIVITET]

**A.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige**

[BESKRIV FORMÅLET MED BEHANDLINGEN]

**A.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)**

[BESKRIV KARAKTEREN AF BEHANDLINGEN]

**A.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede**

**Almindelige personoplysninger** (Databeskyttelsesforordningens artikel 6)

[BESKRIV TYPEN AF PERSONOPLYSNINGER DER BEHANDLES I NEDENSTÅENDE SKEMA. SLET ELLER TILFØJ KOLONNER ALT AFHÆNGIG AF, HVOR MANGE FORSKELLIGE TYPER REGISTRERERE DER BEHANDLES OPLYSNINGER OM]

**Kommenterede [MRS8]:** Ændret iht. Datatilsynets standard skabelon. Tabel tilføjet.

| REGISTRERERE / PERSON-OPLYSNINGER | [BESKRIV TYPEN AF REGISTRERERE] | [BESKRIV TYPEN AF REGISTRERERE] |
|---|---|---|
| **Almindelige personoplysninger: (art. 6)** | ☐ Navn<br>☐ Adresse<br>☐ E-mail<br>☐ Telefonnummer<br>☐ Fødselsdato<br>☐ Medarbejder ID<br>☐ Billeder<br>☐ Andre almindelige personoplysninger: [beskriv hvilke] | ☐ Navn<br>☐ Adresse<br>☐ E-mail<br>☐ Telefonnummer<br>☐ Fødselsdato<br>☐ Medarbejder ID<br>☐ Billeder<br>☐ Andre almindelige personoplysninger: [beskriv hvilke] |
| **Følsomme personoplysninger: (art. 9)** | ☐ Race eller etnisk oprindelse<br>☐ Politisk, religiøs eller filosofisk overbevisning<br>☐ Fagforeningsmæssige tilhørsforhold<br>☐ Genetisk data<br>☐ Biometrisk data<br>☐ Helbredsoplysninger<br>☐ Seksuelle forhold eller orientering | ☐ Race eller etnisk oprindelse<br>☐ Politisk, religiøs eller filosofisk overbevisning<br>☐ Fagforeningsmæssige tilhørsforhold<br>☐ Genetisk data<br>☐ Biometrisk data<br>☐ Helbredsoplysninger<br>☐ Seksuelle forhold eller orientering |

| | | |
|---|---|---|
| **Straffedomme og lovovertrædelser (§10)** | ☐ Straffedomme og lovovertrædelser | ☐ Straffedomme og lovovertrædelser |
| **CPR-nummer (§11)** | ☐ CPR-nummer | ☐ CPR-nummer |
| **Andre fortrolige personoplysninger** | ☐ Væsentlige sociale forhold<br>☐ Væsentlige økonomiske forhold<br>☐ Bankoplysninger<br>☐ Ansøgninger og CV<br>☐ Andre fortrolige oplysninger: [beskriv hvilke] | ☐ Væsentlige sociale forhold<br>☐ Væsentlige økonomiske forhold<br>☐ Bankoplysninger<br>☐ Ansøgninger og CV<br>☐ Andre fortrolige oplysninger: [beskriv hvilke] |

**A.4. Behandlingen omfatter følgende kategorier af registrerede (f.eks. borgere, elever, kontanthjælpsmodtagere m.m.):**

[BESKRIV KATEGORIERNE AF REGISTRERERE, HVIS IKKE TABELLEN I A.3 ANVENDES]

**Kommenterede [MRS9]:** Ændret iht. Datatilsynets standard skabelon. Jf. tabel i A.3.

**A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed**

[BESKRIV VARIGHEDEN AF BEHANDLINGEN]

## Bilag B Underdatabehandlere

### B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere:

| NAVN | CVR | ADRESSE | BESKRIVELSE AF BE-HANDLING |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden at følge den aftalte procedure for tilføjelse eller udskiftning af underdatabehandlere jf. pkt. 6 – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

**Kommenterede [MRS10]:** Ændret iht. Datatilsynets standard skabelon.

### B.2. Varsel for godkendelse af underdatabehandlere

Jf. pkt. 6.3.

## Bilag C Instruks vedrørende behandling af personoplysninger

**C.1 Behandlingens genstand/instruks**
Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

[BESKRIV BEHANDLINGEN, SOM DATABEHANDLEREN INSTRUERES I AT FORETAGE]

**C.2 Behandlingssikkerhed**
Sikkerhedsniveauet skal afspejle:

[BESKRIV – UNDER HENSYNTAGEN TIL BEHANDLINGENS KARAKTER, OMFANG, SAMMENHÆNG OG FORMÅL SAMT RISICIENE AF VARIERENDE SANDSYNLIGHED OG ALVOR FOR FYSISKE PERSONERS RETTIGHEDER OG FRIHEDSRETTIGHEDER – ELEMENTERNE, SOM ER AFGØRENDE FOR SIKKERHEDSNIVEAUET]

[EKSEMPELVIS]:

"BEHANDLINGEN OMFATTER EN STØRRE MÆNGDE PERSONOPLYSNINGER OMFATTET AF DATABESKYTTELSESFORORDNINGENS ARTIKEL 9 OM "SÆRLIGE KATEGORIER AF PERSONOPLYSNINGER", HVORFOR DER SKAL ETABLERES ET "HØJT" SIKKERHEDSNIVEAU."]

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etablere det nødvendige (og aftalte) sikkerhedsniveau.

Databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

[BESKRIV KRAVENE TIL PSEUDONYMISERING OG KRYPTERING AF PERSONOPLYSNINGER]
Databehandler foretager pseudonymisering af persondata, hvor den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers grundlæggende rettigheder og frihedsrettigheder tilsiger det.

Databehandler foretager kryptering af persondata, hvor den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers grundlæggende rettigheder og frihedsrettigheder tilsiger det.

Der anvendes altid kryptering af personoplysninger ved enhver transmission af fortrolige og følsomme personoplysninger via eksterne kommunikationsforbindelser.

**Kommenterede [MRS11]:** Beskriv i øvrigt hvordan dekrypteringsnøgler gemmes og kontrolleres, hvis dette er relevant.

[BESKRIV KRAVENE VEDRØRENDE EVNEN TIL AT SIKRE VEDVARENDE FORTROLIGHED, INTEGRITET, TILGÆNGELIGHED OG ROBUSTHED AF BEHANDLINGSSYSTEMER OG –TJENESTER]
Databehandler foretager mindst én gang årligt en risikovurdering for hver af de behandlingssystemer og tjenester, hvori den Dataansvarliges personoplysninger behandles. Databehandler foretager loyalt og professionelt mitigerende foranstaltninger baseret på risikovurderingens resultater.
Databehandler foretager løbende mitigerende foranstaltninger af teknisk og organisatorisk karakter, når dette viser sig påkrævet.

Databehandler sikrer desuden, at:

- adgang til de personoplysninger, som aftalen vedrører, er begrænset til personer, der har et sagligt formål.
- der er tekniske og/eller organisatoriske foranstaltninger, som sikrer, at alene disse autoriserede personer, har adgang. Autorisationen omfatter også personer, som udfører konsulentopgaver eller nødvendige revisions- drifts- og systemtekniske opgaver.
- der løbende foretages kontrol af, om brugerne er tildelt de adgange og autorisationer, som de bør have.
- ansatte og eventuelle samarbejdspartnere skal være bekendt med og have tilstrækkelig uddannelse og instruktion om databehandlingens formål, politikker, arbejdsgange og om deres tavshedspligt.

[BESKRIV KRAVENE VEDRØRENDE EVNEN TIL RETTIDIGT AT GENOPRETTE TILGÆNGELIGHEDEN AF OG ADGANGEN TIL PERSONOPLYSNINGER I TILFÆLDE AF EN FYSISK ELLER TEKNISK HÆNDELSE]
Databehandler sikrer at:

- have opdaterede og effektive beredskabsplaner og -procedurer, der sikrer genetablering af personoplysninger og adgange inden for rimelig tid i tilfælde af driftsafbrydelser.
- der foretages regelmæssig backup af personoplysninger, der er omfattet af aftalen samt med passende mellemrum foretage restore tests.
- effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed gennem afholdelse af it-beredskabsøvelser regelmæssigt afprøves og evalueres. Den dataansvarlige kan anmode om at få dokumentation for gennemførelsen stillet til rådighed.

[BESKRIV KRAVENE VEDRØRENDE PROCEDURER FOR REGELMÆSSIG AFPRØVNING, VURDERING OG EVALUERING AF EFFEKTIVITETEN AF DE TEKNISKE OG ORGANISATORISKE FORANSTALTNINGER TIL SIKRING AF BEHANDLINGSSIKKERHEDEN]
Databehandleren skal sikre, at der foreligger procedurer, som sikrer, at der sker regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.

Databehandler har til enhver tid tidssvarende procedurer for gennemførelse af:

- regelmæssig kontrol, vurdering, tilpasning og forbedring af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger, som Databehandleren er underlagt efter den til enhver tid gældende lovgivning, retspraksis, Datatilsynets afgørelser, anbefalinger og retningslinjer samt vilkårene i nærværende databehandleraftale.

- kontrol af, at sikkerhedsforanstaltningerne faktisk efterleves i forhold til den til enhver tid værende risiko for de registreredes rettigheder og frihedsrettigheder.
- kontrol af brugeradgang for medarbejdere eller andre autoriserede.
- kontrol af at backuppen er læsbar, skrivebeskyttet, har det rette omfang og kan reetableres.
- kontrol af at der sker korrekt kryptering, herunder at krypteringsnøglen opbevares sikkert.
- kontrol med at sikkerhedsloggene er tilstrækkelige og relevante.
- kontrol med at det fysiske sikkerhedsniveau er afstemt med det til enhver tid værende trusselsbillede.
- databehandleren har formelle procedurer for ændringshåndtering med henblik på at sikre, at enhver ændring er behørigt autoriseret, testet og godkendt inden implementering.
- for kritiske sikkerhedsopdateringer skal Databehandleren have procedurer, der sikrer, at disse kan gennemføres uden unødig forsinkelse.
- at der føres ekstraordinære kontroller ved større ændringer af systemteknisk set-up og efter brud på persondatabeskyttelsen.

[BESKRIV KRAVENE VEDRØRENDE ADGANG TIL OPLYSNINGERNE VIA INTERNETTET]
Når der tilgås systemer indeholdende personoplysninger over internettet, så skal autentifikationen af brugeren ske ved multifaktorautentificering(MFA). Der må kun oprettes forbindelse til personoplysninger omfattet af disse bestemmelser igennem sikre krypterede forbindelser.

[BESKRIV KRAVENE VEDRØRENDE BESKYTTELSE AF OPLYSNINGER UNDER TRANSMISSION]
Der skal anvendes tilstrækkelige sikkerhedsforanstaltninger i forbindelse med transmission af personoplysninger. Sikkerhedsforanstaltningerne skal leve op til de til enhver tid anerkendte og gældende branchestandarder for behandling af personoplysninger.

Databehandler sikrer i denne forbindelse, at personoplysninger er krypteret i forbindelse med transmissionen. Krypteringen skal løbende holdes opdateret, og følge den til enhver tid værende anerkendte og gældende branchestandard.

[BESKRIV KRAVENE VEDRØRENDE BESKYTTELSE AF OPLYSNINGER UNDER OPBEVARING]
Under opbevaring af personoplysninger skal der etableres tilstrækkelige sikkerhedsforanstaltninger under hensyntagen til karakteren af de behandlede personoplysninger, og risikoen for de registreredes rettigheder.

Databehandler sikrer, at personoplysningerne er krypteret under opbevaring. Krypteringen skal løbende holdes opdateret, og følge den til enhver tid værende anerkendte og gældende branchestandard.

[BESKRIV KRAVENE VEDRØRENDE FYSISK SIKRING AF LOKALITETER, HVOR DER BEHANDLES OPLYSNINGER]
Databehandler sikrer, at der er passende sikkerhedsforanstaltninger mod enhver uautoriseret adgang til lokationer, hvor den dataansvarliges data behandles. Sikkerhedsforanstaltningerne skal være afstemt med det aktuelle trusselsbillede i henhold til følsomhed og omfanget af personoplysninger. Behandlingen foregår fra lokationer, som er beskyttet mod skader forårsaget af fysiske forhold som f.eks., - men ikke begrænset til - brand, overophedning, vandskade, magnetisme, forsyningssvigt, tyveri eller hærværk. Databehandleren skal sikre, at alt anvendt udstyr, der anvendes i forbindelse med behandlingen af personoplysninger, er underlagt passende tekniske foranstaltninger.

Mobile lagringsmedier
Mobile lagringsmedier med personoplysninger skal være mærket og skal opbevares med tilstrækkelig stærk kryptering under opsyn eller under lås, når de ikke benyttes.

Mobile lagringsmedier med personoplysninger må kun udleveres til autoriserede personer med henblik på revision eller drifts- og systemtekniske opgaver. Der skal føres en fortegnelse over, hvilke mobile lagringsmedier der benyttes i forbindelse med databehandlingen.

Der skal udarbejdes skriftlige instrukser for anvendelse og opbevaring af mobile lagringsmedier.

Reparation, service og kassation af udstyr
I forbindelse med reparation og service af udstyr, der indeholder personoplysninger, samt ved salg og kassation af anvendte datamedier skal der træffes fornødne foranstaltninger for at sikre, at personoplysningerne ikke hændeligt eller bevidst tilintetgøres, fortabes eller forringes eller, at personoplysningerne kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med gældende lov.

Ved kassation af udstyr og lagringsmedier, der indeholder personoplysninger, skal lagringsmedier destrueres eller renses, så der sker effektiv sletning af personoplysningerne. Dokumentation for, at kassation er foretaget i overensstemmelse med ovenstående, skal opbevares i den periode, databehandlingen foregår og forevises på den dataansvarliges anmodning.

[BESKRIV KRAVENE VEDRØRENDE ANVENDELSE AF HJEMME-/FJERNARBEJDSPLADSER]
Hjemme-/fjernarbejdspladser skal være sikret med tekniske kontroller, der sikrer, at behandlingen af personoplysninger sker i overensstemmelse med gældende lovgivning og den dataansvarliges og databehandlerens retningslinjer.
Det skal sikres, at uvedkommende ikke får adgang til personoplysninger, der behandles ved hjemmearbejdspladser, ligesom de enkelte medarbejdere skal instrueres i, hvordan uvedkommende ikke får adgang.

Databehandler sikrer, at der anvendes kryptering af kommunikationsforbindelser. Fjernadgange skal være sikret af en VPN-løsning eller anden sikkerhedsteknologi, så det kun er autoriserede personer, som kan få adgang til personoplysninger.

Autentifikation af personer, som får adgang til personoplysninger, skal være baseret på multifaktorautentifikation (MFA) eller tilsvarende sikkerhedsforanstaltninger.

[BESKRIV KRAVENE VEDRØRENDE LOGNING]
Der skal foretages maskinel registrering (logning) ved al behandling af personoplysninger.
Loggen skal som minimum indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte eller det anvendte søgekriterium.

Loggen skal opbevares i seks måneder, hvorefter den skal slettes, medmindre der i overensstemmelse med loggens formål fastsættes en længere opbevaringsperiode af hensyn til at kunne anvende den som værktøj til brug ved efterforskning.

Databehandleren fører løbende kontrol med, at loggen indeholder de nødvendige oplysninger, som fremgår af disse bestemmelser.

Databehandleren skal ved mistanke om misbrug eller brud på persondatasikkerheden vederlagsfrit udlevere en log over brugeraktivitet. Databehandleren skal sikre, at loggen er forståelig og indeholder de relevante aktiviteter.

[BESKRIV KRAVENE VEDRØRENDE ADGANGSSTYRING]
Det skal sikres, at det kun er medarbejdere hos databehandleren, som er autoriseret hertil, der har adgang til personoplysningerne. Dette kan fx have sit afsæt i en etableret adgangsstyringspolitik.

Det skal sikres, at adgangskoder for databehandlerens medarbejdere er tiltrækkeligt komplekse og at de følger Center for Cybersikkerheds anbefalinger vedr. passwordsikkerhed. Desuden skal der føres kontrol med afviste adgangsforsøg, og der skal blokeres for yderligere forsøg efter flere afviste adgangsforsøg.

Beskriv hvordan der føres kontrol med afviste adgangsforsøg:

**C.3 Bistand til den dataansvarlige**
Databehandleren skal bistå den dataansvarlige i overensstemmelse med pkt. 8.1, 8.2 og 8.3 ved at gennemføre tekniske og organisatoriske foranstaltninger.

**C.4 Opbevaringsperiode/sletterutine**
Jf. pkt. 10.1, 10.2 og A.5.

**Kommenteret [MRS12]:** Ændret iht. Datatilsynets standard skabelon.

**Kommenteret [MRS13]:** Ændret iht. Datatilsynets standard skabelon.

**C.5 Lokalitet for behandling**

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end dem, der er angivet i bilag B.

**Kommenterede [MRS14]:** Ændret iht. Datatilsynets standard skabelon.

**C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande**

[BESKRIV INSTRUKSEN VEDRØRENDE OVERFØRSEL AF PERSONOPLYSNINGER TIL TREDJELANDE ELLER INTERNATIONALE ORGANISATIONER]

[ANGIV GRUNDLAGET FOR OVERFØRSLEN SOM OMHANDLET I DATABESKYTTELSESFORORDNINGENS KAPITEL V]

Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsels af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler.

**C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren**

Databehandleren skal hvert år for egen regning indhente en revisionserklæring fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende typer af revisionserklæringer kan anvendes i overensstemmelse med disse Bestemmelser:

- ISAE 3000

Revisionserklæringen fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen og kan i sådanne tilfælde anmode om en ny revisionserklæring under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af erklæringen er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendigt.

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion.

[ELLER]

Databehandleren skal årligt for egen regning afgive en erklæring angående databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Erklæringen fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen og kan i sådanne tilfælde anmode om en ny erklæring under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af erklæringen er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendigt.

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion.

**C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere**
Databehandleren skal hvert år for egen regning indhente en revisionserklæring fra en uafhængig tredjepart vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende typer af revisionserklæringer kan anvendes i overensstemmelse med disse Bestemmelser:

- ISAE 3000

Revisionserklæringen fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen og kan i sådanne tilfælde anmode om en ny revisionserklæring under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af erklæringen er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Databehandleren eller en repræsentant for databehandleren har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra underdatabehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når databehandleren eller den dataansvarlige finder det nødvendigt.

Dokumentation for sådanne inspektioner fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden af inspektionen og kan i sådanne tilfælde anmode om gennemførelsen af en ny inspektion under andre rammer og/eller under anvendelse af anden metode.

Databehandlerens og underdatabehandlerens eventuelle udgifter i forbindelse med en fysisk inspektion af underdatabehandlerens lokaliteter er den dataansvarlige uvedkommende – uanset om den dataansvarlige har initieret og deltaget i en sådan inspektion.

[ELLER]

Databehandleren skal årligt for egen regning afgive en erklæring angående underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Erklæringen fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen og kan i sådanne tilfælde anmode om en ny erklæring under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af erklæringen er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra underdatabehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendigt.

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv. Databehandleren og/eller underdatabehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion.

## Bilag D Databehandlerkæde

[HVOR DER ANVENDES UNDERDATABEHANDLERE KAN FØLGENDE INDSÆTTES]

D.1 Databehandlerkæden

Databehandleren skal udarbejde en fuldstændig oversigt over databehandlere, som behandler den dataansvarliges personoplysninger.

Oversigten skal angive databehandlerens underdatabehandlere, og alle deres eventuelle underdatabehandlere, så hele kæden for behandling af personoplysninger er dokumenteret.

Databehandleren orienterer den dataansvarlige om enhver ændring i databehandlerkæden og ændringer af ejerskab af selskaber i databehandlerkæden.

Databehandleren udarbejder et koncerndiagram over de koncernforbundne selskaber. Databehandleren orienterer den dataansvarlige om enhver ændring af koncerndiagrammet.