Vejledning i brug af databehandleraftaleskabelonen:

I nedenstående skabelon til databehandleraftale anvendes gule og lilla overstregninger indeholdende eksempler på tekst, der kan anvendes.

De gule overstregninger stammer fra Datatilsynets skabelon. De lilla overstregninger er Erhvervsstyrelsens forslag. Det bemærkes, at der er tale om forslag/eksempler, og at der derfor altid skal foretages en konkret vurdering af, om forslagene passer til netop den databehandleraftale, du skal indgå.

De anførte kantede parenteser skal naturligvis slettes fra det endelige dokument. I de tilfælde, hvor det giver mening, skal indholdet af de kantede parenteser ligeledes slettes.

Al den tekst, der ikke er overstreget med en farve, er standardtekst/-bestemmelser og må ikke slettes.

UDKAST

Standardkontraktsbestemmelser

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

mellem

Erhvervsstyrelsen
CVR-nummer 10150817
Langelinie Allé 17
2100 København Ø
Danmark

herefter "den dataansvarlige"

og

[NAVN]
CVR-nummer [CVR-NR]
[ADRESSE]
[POSTNUMMER OG BY]
[LAND]

herefter "databehandleren"

der hver især er en "part" og sammen udgør "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. Indhold

2. 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] 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 bestemmelser vedrørende andre aktiviteter, som ikke af omfattet af Bestemmelserne.

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.

3. 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.

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

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.

4. 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.

   [NOTE: PARTERNE BØR FORUDSE OG OVERVEJE KONSEKVENSERNE, DER KAN FØLGE AF EN POTENTIELT ULOVLIG INSTUKS, SOM DEN DATAANSVARLIGE HAR GIVET OG REGULERE DETTE I EN AFTALE MELLEM PARTERNE.]

   Eksempel på tekst (evt. som selvstændigt punkt): Er den dataansvarliges instruks i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret, jf. Bestemmelse 9.2, foretager den dataansvarlige en vurdering af risikoen for den registrerede forbundet med den ulovlige instruks. Er der som følge af den ulovlige instruks sket et sikkerhedsbrud hos databehandleren, jf. databeskyttelsesforordningens art. 33, bistår den dataansvarlige databehandleren med anmeldelse til Datatilsynet på samme måde, som det fremgår af Bestemmelse 10.3 og 10.4 for databehandleren.

5. 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.

6. 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.

7. 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 [VALG 1] specifik skriftlig godkendelse fra den dataansvarlige [VALG 2] generel skriftlig godkendelse.

3. [VALG 1 FORUDGÅENDE SPECIFIK GODKENDELSE] Databehandleren må kun gøre brug af underdatabehandlere med den dataansvarliges forudgående specifikke skriftlige godkendelse. Databehandleren skal indgive anmodningen om en specifik godkendelse mindst 3 måneder inden anvendelsen af den pågældende underdatabehandler. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

   [[VALG 2 FORUDGÅENDE GENEREL GODKENDELSE] Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst [ANGIV TIDSPERIODE] 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.]

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.

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.

8. 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:

    a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
    b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
    c. 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.6.

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.

9. Bistand til den dataansvarlige

1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt 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 så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

    a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
    b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
    c. indsigtsretten
    d. retten til berigtigelse
    e. retten til sletning (”retten til at blive glemt”)
    f. retten til begrænsning af behandling
    g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
    h. retten til dataportabilitet
    i. retten til indsigelse

j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

2. 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:

   a. 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

   b. 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

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

   d. 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.

3. 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 9.1. og 9.2.

10. 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 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:

   a. 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

b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden

c. 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 den information, 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.

11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at [VALG 1] slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlig, at oplysningerne er slettet [[VALG 2] tilbagelevere alle personoplysningerne og slette eksisterende kopier], medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

2. [HVIS RELEVANT] Følgende regler i EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne efter ophør af tjenesterne vedrørende behandling af personoplysninger:

   a. […]

   Databehandleren forpligter sig til alene at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som disse regler foreskriver.

12. 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.

13. 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.

14. 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 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftligt varsel af begge parter.

5. Underskrift

   På vegne af den dataansvarlige

Navn	[NAVN]
Stilling	[STILLING]
Telefonnummer	[TELEFONNUMMER]
E-mail	[E-MAIL]

   Underskrift

   På vegne af databehandleren

Navn	[NAVN]
Stilling	[STILLING]
Telefonnummer	[TELEFONNUMMER]
E-mail	[E-MAIL]

   Underskrift

15. 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.

Navn	[NAVN]
Stilling	[STILLING]
Telefonnummer	[TELEFONNUMMER]
E-mail	[E-MAIL]

Navn	[NAVN]
Stilling	[STILLING]
Telefonnummer	[TELEFONNUMMER]
E-mail	[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

[BESKRIV TYPEN AF PERSONOPLYSNINGER DER BEHANDLES]

[EKSEMPELVIS]

"Navn, e-mailadresse, telefonnummer, adresse, personnummer, betalingskortoplysninger, medlemsnummer, type af medlemskab, fremmøde i fitnesscenter og tilmelding til konkrete fitnesshold."

[BEMÆRK: BESKRIVELSEN BØR VÆRE SÅ SPECIFIK SOM MULIGT, OG UNDER ALLE OMSTÆNDIGHEDER, SKAL TYPEN AF PERSONOPLYSNINGER PRÆCISERES YDERLIGERE END BLOT "PERSONOPLYSNINGER SOM DEFINERET I DATABESKYTTELSESFORORDNINGENS ARTIKEL 4, NR. 1" ELLER HVILKEN KATEGORI AF OPLYSNINGER ("ARTIKEL 6, 9 ELLER 10") DER BEHANDLES.]

A.4. Behandlingen omfatter følgende kategorier af registrerede

[BESKRIV KATEGORIERNE AF REGISTREREDE]

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]

Eksempel på tekst: Behandlingen er ikke tidsbegrænset og varer indtil hovedaftalen ophører.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden den dataansvarliges skriftlige godkendelse – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

[Der bør også indsættes en liste over underdatabehandleres eventuelle underdatabehandlere etc.]

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING

B.2. Varsel for godkendelse af underdatabehandlere [Skal stemme med afsnit 7, hvis der indsættes noget] [VALGFRIT] [HVIS RELEVANT, BESKRIV VARSLINGSPERIODEN FOR GODKENDELSE AF UNDERDATABEHANDLER]

Eksempel på tekst: Databehandleren har den dataansvarliges godkendelse til at gøre brug af ovennævnte underdatabehandlere.

Databehandleren må kun tilføje eller erstatte underdatabehandlere på ovenstående liste med den dataansvarliges forudgående specifikke skriftlige godkendelse. Databehandleren skal indgive anmodningen om en specifik godkendelse mindst 3 måneder inden anvendelsen af den pågældende underdatabehandler.

Såfremt den dataansvarlige har indsigelser mod ændringerne, skal den dataansvarlige give meddelelse herom til databehandleren inden 14 dage efter modtagelsen af underretningen. Den dataansvarlige kan alene gøre indsigelse, såfremt den dataansvarlige har rimelige, konkrete årsager hertil.]

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, SAMMEHÆNG OG FORMÅL SAMT RISICIENE AF VARIERENDE SANDDSYNLIGHED 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.” eller fx:

Behandlingen omfatter en større mængde personoplysninger af ikke-fortrolig eller følsom karakter, jf. databeskyttelsesforordningens art. 6.]

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]

[BESKRIV KRAVENE VEDRØRENDE EVNEN TIL AT SIKRE VEDVARENDE FORTROLIGHED, INTEGRITET, TILGÆNGELIGHED OG ROBUSTHED AF BEHANDLINGSSYSTEMER OG –TJENESTER]

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

[BESKRIV KRAVENE VEDRØRENDE PROCEDURER FOR REGELMÆSSIG AFPRØVNING, VURDERING OG EVALUERING AF EFFEKTIVITETEN AF DE TEKNISKE OG ORGANISATORISKE FORANSTALTNINGER TIL SIKRING AF BEHANDLINGSSIKKERHEDEN]

[BESKRIV KRAVENE VEDRØRENDE ADGANG TIL OPLYSNINGERNE VIA INTERNETTET]

[BESKRIV KRAVENE VEDRØRENDE BESKYTTELSE AF OPLYSNINGER UNDER TRANSMISSION]

[BESKRIV KRAVENE VEDRØRENDE BESKYTTELSE AF OPLYSNINGER UNDER OPBEVARING]

[BESKRIV KRAVENE VEDRØRENDE FYSISK SIKRING AF LOKALITETER, HVOR DER BEHANDLES OPLYSNINGER]

[BESKRIV KRAVENE VEDRØRENDE ANVENDELSE AF HJEMME-/FJERNARBEJDSPLADSER]

[BESKRIV KRAVENE VEDRØRENDE LOGNING]

Eksempel på tekst: Databehandleren skal sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og –tjenester.

Databehandleren skal efterleve ISO27001-standarden eller tilsvarende standard og efterleve relevante kontroller.

Den dataansvarlige stiller krav om, at databehandleren har et passende beredskab i tilfælde af en utilsigtet fysisk eller teknisk hændelse. Databehandleren skal derved rettidigt kunne genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en utilsigtet fysisk eller teknisk hændelse.

Den dataansvarlige stiller krav om, at oplysningerne er beskyttede under transmission og opbevaring ud fra en betragtning af ovenstående hensyn vedr. sikkerhedsniveauet.

Den dataansvarlige stiller krav om, at databehandleren har foretaget passende sikring af de lokaliteter, hvor oplysningerne behandles, fx ved hjælp af tyverialarmer og videoovervågning.

Databehandleren skal sikre, at hændelseslogning til registrering af brugeraktivitet, undtagelser, fejl og informationssikkerhedshændelser opbevares og gennemgås. Databehandleren skal beskytte logningsfaciliteter og logoplysninger mod manipulation og uautoriseret adgang. Databehandleren skal sikre, at der foretages maskinel registrering (logning) af alle anvendelser af personoplysninger. Registreringen skal mindst indeholdeoplysning om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium. Loggen skal opbevares i 6 måneder, hvorefter den skal slettes. Databehandleren skal sikre, at aktiviteter udført af systemadministratorer og systemoperatører logges, og databehandleren skal benytte disse logs og gennemgå disse regelmæssigt. Denne log skal ligeledes opbevares i 6 måneder, hvorefter den skal slettes.

Den dataansvarlige forestår konstruktionen af testdata og herunder anonymisering eller pseudonymisering af disse. Databehandleren implementerer de af den dataansvarlige til rådighed stillede testdata i de relevante systemer og løsninger.

Den dataansvarlige stiller krav om, at anvendelse af hjemme-/fjernarbejdspladser foregår via sikrede forbindelser.

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

Såfremt databehandleren bliver opmærksom på, herunder som led i sin løbende risikovurdering, at de af den dataansvarlige krævede foranstaltninger ikke er tilstrækkelige eller pas-

sende, skal databehandleren straks efter databehandlerens kendskab hertil skriftligt underrette den dataansvarlige herom samt bistå den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger. Databehandleren er derfor forpligtiget til løbende at vurdere, hvor vidt sikkerhedsniveauet er passende og om nødvendigt justere behandlingen derefter. Bistand i relation hertil afregnes efter medgået tid, jf. Bilag D, under forudsætning af, at der er indgået skriftlig aftale om den konkrete bistands indhold og omfang.

Databehandleren skal på den dataansvarliges anmodning give denne tilstrækkelige informationer til, at denne kan påse og dokumentere, at databehandleren har truffet de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger, jf. Bilag C.6 om tilsyn.

C.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

[BESKRIV OMFANG OG UDSTRÆKNING AF BISTANDEN SOM SKAL YDES AF DATABEHANDLEREN]

[BESKRIV DE SPECIFIKKE TEKNISKE OG ORGANISATORISKE FORANSTALTNINGER SOM DATABEHANDLEREN SKAL GENNEMFØRE MED HENBLIK PÅ AT BISTÅ DEN DATAANSVARLIGE]

Eksempel på tekst: Databehandleren skal videresende anmodninger mv. vedr. de registreredes rettigheder fra de registrerede til den dataansvarlige, såfremt disse ved en fejl er sendt til databehandleren. Videresendelsen skal ske til den i Bestemmelse 15 anførte kontaktperson.

Underretninger om sikkerhedsbrud og bistand i den forbindelse, jf. Bestemmelse 9.2, stiles til styrelsens IT-sikkerhedskoordinator via erst@erst.dk, Att.: IT-sikkerhedskoordinatoren.

C.4 Opbevaringsperiode/sletterutine

[BESKRIV EVENTUEL OPBEVARINGSPERIODE/SLETTERUTINE FOR DATABEHANDLEREN]

[EKSEMPELVIS] *"Personoplysninger opbevares i [ANGIV TIDSPERIODE], hvorefter de slettes hos databehandleren.*

Eksempel på tekst: Personoplysningerne opbevares indtil hovedaftalen ophører.

- Anmodning om sletning af oplysninger er underlagt Service Level Agreement for hovedaftalen.

- Ved anmodning om sletning af oplysninger skal databehandleren dokumentere, at sletningen er udført.

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret den dataansvarlige oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

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 følgende:

[ANGIV, HVOR BEHANDLINGEN FINDER STED] [ANGIV, HVILKEN DATABEHANDLER EL LER UNDERDATABEHANDLER, DER ANVENDER ADRESSEN]

Eksempel på tekst: Erhvervsstyrelsen, Langelinie Allé 17, 2100 København Ø. Brug af den dataansvarliges netværk gennem en af den dataansvarlige til rådighed stillet stærkt krypteret VPN-adgang anses for at ske fra nærværende lokation uanset brugerens faktiske geografiske placering.

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 DATABESKYTTELSES-FORORDNINGENS KAPITEL V]

Eksempel på tekst: Der vil ikke ske en overførsel af personoplysninger til tredjelande.

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

[BESKRIV PROCEDURERNE FOR DEN DATAANSVARLIGES REVISIONER, HERUNDER INSPEKTIONER, MED BEHANDLINGEN AF PERSONOPLYSNINGER, SOM ER OVERLADT TIL DATABEHANDLEREN]

[EKSEMPELVIS]

Databehandleren skal en gang årligt 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 og ISAE 3402.

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.

[ELLER]

"Den dataansvarlige eller en repræsentant for den dataansvarlige foretager [ANGIV TIDSPERIODE] en fysisk inspektion af lokaliteterne, hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen, med henblik på at fastslå databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Ud over det planlagte tilsyn, kan den dataansvarlige gennemføre en inspektion hos databehandleren, når den dataansvarlige finder det nødvendigt."

[OG, HVIS RELEVANT]

"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 [HVIS RELEVANT] Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere
[BESKRIV PROCEDURERNE FOR DATABEHANDLERENS REVISIONER, HERUNDER INSPEKTIONER, MED BEHANDLINGEN AF PERSONOPLYSNINGER, SOM ER OVERLADT TIL UNDERDATABEHANDLEREN]

[EKSEMPELVIS]

Databehandleren skal en gang årligt 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 og ISAE 3402.

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.

[ELLER]

"Databehandleren eller en repræsentant for databehandleren foretager [ANGIV TIDSPERIODE] en fysisk inspektion af lokaliteterne, hvorfra underdatabehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen, med henblik på at fastslå underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Ud over det planlagte tilsyn, kan databehandleren gennemføre en inspektion med underdatabehandleren, 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.

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

[OG, HVIS RELEVANT]

"Den dataansvarlige kan – hvis det findes nødvendigt – vælge at initiere og deltage på en fysisk inspektion hos underdatabehandleren. Dette kan blive aktuelt, hvis den dataansvarlige vurderer, at databehandlerens inspektion hos underdatabehandleren ikke har givet den dataansvarlige tilstrækkelig sikkerhed for, at behandlingen hos underdatabehandleren sker I overensstemmelse med databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarliges eventuelle deltagelse i en inspektion hos underdatabehandleren ændrer ikke ved, at databehandleren også herefter har det fulde ansvar for underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser."

[OG, HVIS RELEVANT]

"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."

Bilag D Parternes regulering af andre forhold

Eksempel på tekst:

Vederlag for særskilt bistand

I den udstrækning databehandleren bistår den dataansvarlige med sidstnævntes overholdelse af databeskyttelsesforordningen, jf. databehandleraftalens punkt 9, eller med vurdering af den dataansvarliges behandlingssikkerhed, jf. databehandleraftalens Bilag C.2, afregnes der efter medgået tid med den følgende timesats: xxx kr.

Såfremt der fremgår en anden timepris af parternes "hovedaftale", jf. databehandleraftalens punkt 2.3, har denne forrang.