Standardkontraktbestemmelser

(Databehandleraftale)

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

mellem

Brønderslev Kommune
CVR 29189501
Ny Rådhusplads 1
9700 Brønderslev
DK

herefter ”den dataansvarlige”

og

[NAVN]
CVR [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

Indhold

[1. Præambel 3](#_Toc120113570)

[2. Den dataansvarliges rettigheder og forpligtelser 4](#_Toc120113571)

[3. Databehandleren handler efter instruks 4](#_Toc120113572)

[4. Fortrolighed 4](#_Toc120113573)

[5. Behandlingssikkerhed 5](#_Toc120113574)

[6. Anvendelse af underdatabehandlere 5](#_Toc120113575)

[7. Overførsel til tredjelande eller internationale organisationer 7](#_Toc120113576)

[8. Bistand til den dataansvarlige 7](#_Toc120113577)

[9. Underretning om brud på persondatasikkerheden 8](#_Toc120113578)

[10. Sletning og returnering af oplysninger 9](#_Toc120113579)

[11. Revision, herunder inspektion 9](#_Toc120113580)

[12. Parternes aftale om andre forhold 10](#_Toc120113581)

[13. Ikrafttræden og ophør 10](#_Toc120113582)

[14. Kontaktpersoner hos den dataansvarlige og databehandleren 11](#_Toc120113583)

[Bilag A: Oplysninger om behandlingen 12](#_Toc120113584)

[Bilag B: Underdatabehandlere 14](#_Toc120113585)

[Bilag C: Instruks vedrørende behandling af personoplysninger 15](#_Toc120113586)

## 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 tre 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. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
10. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

## 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 (henvisninger til ”medlemsstat” i disse bestemmelser skal forstås som en henvisning til ”EØS-medlemsstater”) 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.

## 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.

## 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.

## 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:

1. Pseudonymisering og kryptering af personoplysninger
2. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
3. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
4. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.
5. 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.
6. 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.

## 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 vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 7 dage 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.

1. 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.
2. 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.
3. 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.

## 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:
4. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
5. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
6. behandle personoplysningerne i et tredjeland
7. 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.
8. 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.

## 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:

1. oplysningspligten ved indsamling af personoplysninger hos den registrerede
2. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
3. indsigtsretten
4. retten til berigtigelse
5. retten til sletning (”retten til at blive glemt”)
6. retten til begrænsning af behandling
7. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
8. retten til dataportabilitet
9. retten til indsigelse
10. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering
11. 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:
12. 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
13. 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
14. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)
15. 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.
16. 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.

## 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. Underretningen skal ske til mail-adressen: dpo@99454545.dk.
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:
4. 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
5. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
6. 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.
7. 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.

## Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at tilbagelevere alle personoplysningerne og slette eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

## 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 nærmere 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.

## 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.

## 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: Mads Hurley
Stilling: Chef Digitalisering og IT
Telefon: 99454582

Underskrift

På vegne af databehandleren

Navn: [NAVN]
Stilling: [STILLING]
Telefon: [TELEFONNUMMER]
E-mail: [E-MAIL]

Underskrift

## 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.

Dataansvarlig

Navn: Mikkel Baltersersen
Stilling: DPO
Telefon: 99455455
E-mail: DPO@99454545.dk

Underskrift

Databehandler

Navn: [NAVN]
Stilling: [STILLING]
Telefon: [TELEFONNUMMER]
E-mail: [E-MAIL]

Underskrift

## Bilag A: Oplysninger om behandlingen

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

Behandlingen af den dataansvarliges personoplysninger sker i henhold til formålet i Hovedaftalen, dvs. til brug for levering, herunder support, af ”tjeneste, projektnavn, opgave eller ydelse”.

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

Databehandleren foretager følgende former for behandling af personoplysninger: indsamling, registrering, organisering, systematisering, opbevaring, genfinding, søgning, brug, videregivelse ved transmission, formidling og sletning.

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

Databehandleren behandler personoplysninger i de nedenfor afkrydsede kategorier:

[ ] Almindelige, ikke-følsomme personoplysninger, herunder cpr. nr.

Følsomme oplysninger:

[ ]  Race eller etnisk oprindelse

[ ]  Politisk overbevisning

[ ]  Religiøs eller filosofisk overbevisning

[ ]  Fagforeningsmæssige tilhørsforhold

[ ]  Genetiske data

[ ]  Biometriske data med henblik på entydig identifikation

[ ]  Helbredsoplysninger

[ ]  Seksuelle forhold eller seksuel orientering

[ ]  Oplysninger om strafbare forhold

Konkret vil der blive behandlet følgende personoplysninger: ”FX navn, e-mail, telefonnummer, adresse, etnisk baggrund og oplysninger om lidelser og/eller kroniske sygdomme, misbrug af alkohol og stoffer”.

**A.4. Behandlingen omfatter følgende kategorier af registrerede**

Databehandleren behandler oplysninger om:

1. Fx den dataansvarliges borgere
2. Andre?

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

Databehandleren behandler personoplysninger for den dataansvarlige, indtil Hovedaftalens ophør. Hvis der ikke er aftalt andet skriftligt, vil Databehandleren slette personoplysninger 5 år efter behandling af personoplysningerne er afsluttet.

## Bilag B: Underdatabehandlere

**B.1. Godkendte underdatabehandlere**

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

| Navn | CVR | Adresse | Beskrivelse af handling |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

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.

## 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:

Databehandleren leverer (i overensstemmelse med Hovedaftalen) ”tjeneste, projektnavn, opgave eller ydelse…” til den dataansvarlige. Databehandleren udfører som led i leveringen løbende support.

Her anføres eventuelt yderligere beskrivelse af Databehandlerens opgave

**C.2. Behandlingssikkerhed**

Uanset om behandlingen alene omfatter almindelige personoplysninger eller følsomme personoplysninger om fattet af databeskyttelsesforordningens artiklerne 6 og 9 ønsker den Dataansvarlige, at der skal etableres et ”højt” sikkerhedsniveau.

Databehandleren har implementeret følgende tekniske og organisatoriske sikkerhedsforanstaltninger, for at etablere det nødvendige sikkerhedsniveau jf. Databeskyttelsesforordningen:

**Kryptering af oplysninger**

Alle overførsler af følsomme personoplysninger, cpr. nr. eller oplysninger om strafbare forhold sker via krypterede forbindelser.

**Sikring af fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og tjenester**

Gennemgang af sikkerhedsprocedurer:

* Der er indført procedurer for sikker og fortrolig behandling af personoplysninger. Procedurerne er udarbejdet på baggrund af en konkret risikovurdering.
* Alle medarbejdere hos Databehandleren bliver ved ansættelse undervist i Databehandlerens IT-sikkerhedspolitikker og procedurer i forhold til behandling af personoplysninger.
* Databehandleren instruerer sine ansatte om Databehandlerens forpligtelser i henhold til Bestemmelserne.
* Databehandleren har udarbejdet en datasikkerhedsinstruks, som alle medarbejdere er underlagt.
* Databehandleren gennemgår årligt sine tekniske og organisatoriske sikkerhedsforanstaltninger for behandling af personoplysninger med henblik på at sikre, at de nødvendige foranstaltninger til stadighed er iagttaget.

Generelle sikkerhedsforanstaltninger:

* Medarbejdernes computer må ikke anvendes af andre end medarbejderen selv.
* Medarbejderne må ikke installere programmer, der ikke er godkendt af IT-ledelsen.
* Alle pc’er har kode og skærmlås på 5 minutter.

Tavshedspligt

* Medarbejdere hos Databehandleren er underlagt tavsheds- og fortrolighedsaftaler. Oplysninger, som medarbejderne får adgang til gennem samarbejdet, vil således ikke blive videregivet.

**Evnen til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse**

Databehandlerens underdatabehandlere har etableret back-up-rutiner, der sikrer, at data kan genskabes. Back-up-procedurerne er beskrevet i de enkelte underdatabehandleraftaler.

**Procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden**

* Databehandleren tilstræber løbende i muligt omfang at implementere informationssikkerhedsaktiviteter med udgangspunkt i informationssikkerhedsstandarden ISO27001:2013. Der er særligt fokus på databeskyttelsesforordningen og databeskyttelsesloven, og der er udarbejdet generel informationssikkerheds- og datafortrolighedspolitik.
* Databehandleren foretager 1 gang årligt en risikovurdering af ”tjeneste, projektnavn, opgave eller ydelse…” og processer med fokus på tilgængelighed, fortrolighed og integritet.

**Adgang til personoplysninger via internettet**

Databehandlerens medarbejdere:

* Medarbejdere hos Databehandleren har et personligt login til de systemer, som anvendes i forbindelse med ”tjeneste, projektnavn, opgave eller ydelse…”.
* Databehandlerens medarbejdere er underlagt forbud mod at skaffe sig oplysninger af enhver art, som ikke har betydning for udførelsen af den pågældendes opgaver.
* I forbindelse med ansættelsesophør er der procedurer for sletning af adgang til systemer.
* Der er etableret procedurer for brugeradgangsstyring, der sikrer, at adgang til personoplysninger er begrænset til personer, der har et arbejdsbetinget behov for at skulle tilgå oplysningerne.

Dataansvarliges medarbejdere:

* Databehandleren anmoder hvert år den dataansvarlige om at indsende daterede lister med brugere, der skal have adgang. Alle brugere, der ikke fremgår af indsendte liste, slettes.
* Databehandleren fører logbog og kontrol med supporthenvendelser.
* Den dataansvarlige kan til enhver tid give instruks til Databehandleren om at slette en bruger.

**Fysisk sikring af lokaliteter, hvor der behandles personoplysninger**

* Databehandleren har alarmsystem og dobbeltlås på døren.
* Databehandlerens underdatabehandlere har etableret fysisk sikring af lokaliteter i overensstemmelse med kravene i dataforordningen.

**Anvendelse af hjemme-/fjernarbejdspladser**

Databehandlerens medarbejdere kan anvende hjemmearbejdspladser. Retningslinjer for at tilgå systemer fra andre lokationer er beskrevet i Databehandlerens interne retningslinjer for behandling af personoplysninger.

**Logning**

Al aktivitet i systemerne logges hos underdatabehandlerne.

**C.3 Bistand til den dataansvarlige**

Komiteen 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:

Bistand i forhold til de registreredes rettigheder, jf. databeskyttelsesforordningens kapitel III:

* Databehandleren skal uden unødig forsinkelse, efter at være blevet opmærksom herpå, skriftligt underrette den dataansvarlige om enhver anmodning rettet til Databehandleren eller dennes underdatabehandlere fra en registreret om udøvelse af dennes rettigheder. Databehandleren er ikke berettiget til at besvare anmodninger fra en registreret omkring udøvelse af dennes rettigheder i henhold til gældende databeskyttelsesret.
* Databehandleren skal på opfordring fra den dataansvarlige i øvrigt hjælpe med at opfylde den dataansvarliges forpligtelser i forhold til de registreredes rettigheder i henhold til gældende databeskyttelsesret, jf. Bestemmelse 9.1.

Bistand i forhold til sikkerhedsbrud, jf. databeskyttelsesforordningens artikel 33 og 34

* Databehandleren er forpligtet til at underrette den dataansvarlige om sikkerhedsbrud inden for de tidsfrister, der er angivet i Bestemmelse 10.2.
* Databehandleren fører løbende en fortegnelse over alle sikkerhedsbrud.
* Databehandleren bistår den dataansvarlige med at tilvejebringe den information som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed, jf. Bestemmelse 10.3 samt tilgængelig information til brug for den dataansvarlige underretning af de(n) registrerede, jf. Bestemmelse 9.2.b.
* Databehandleren må ikke hverken offentligt eller til tredjeparter kommunikere om sikkerhedsbrud uden forudgående skriftlig aftale med den dataansvarlige om indholdet af en sådan kommunikation, medmindre Databehandleren har en retlig forpligtelse til sådan kommunikation.

Konsekvensanalyse, jf. databeskyttelsesforordningens artikel 35 og 36:

* Databehandleren bistår efter anmodning den dataansvarlige med de oplysninger, som er tilgængelige for Databehandleren.

Øvrig bistand:

* Databehandleren står til rådighed for besvarelse af spørgsmål fra den dataansvarlige eller den kompetente tilsynsmyndighed, Datatilsynet.
* Databehandleren underretter den dataansvarlige om:
* enhver anmodning om videregivelse af personoplysninger omfattet af Bestemmelserne fra en myndighed, medmindre orienteringen af den dataansvarlige er eksplicit forbudt ved lov, f.eks. i medfør af regler, der har til formål at sikre fortroligheden af en retshåndhævende myndigheds efterforskning
* anden manglende overholdelse af Databehandlerens samt eventuelle underdatabehandlers forpligtelser, uanset om dette sker hos Databehandleren eller hos en underdatabehandler.

De tekniske og organisatoriske sikkerhedsforanstaltninger, som skal sikre Databehandlerens bistand af den dataansvarlige i henhold til ovenstående, er nærmere beskrevet i Bestemmelse C.2.

**C.4 Opbevaringsperiode/sletterutine**

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal Databehandleren slette personoplysningerne i overensstemmelse med Bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse Bestemmelser – har ændret den dataansvarlige oprindelige valg.

**C.5 Lokalitet for behandling**

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden rettidig varsling af den dataansvarlige efter Bestemmelse 7.3, hvortil den dataansvarlige ikke har gjort indsigelse, ske på andre lokaliteter end følgende:

Data behandles hos Databehandleren på adressen ”…”, samt på medarbejdernes privatadresse i forbindelse med hjemmearbejde.

Data opbevares desuden hos de underdatabehandlere, der fremgår på den til enhver tid gældende liste over underdatabehandlere, som er vedlagt Bestemmelserne.

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

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

Databehandleren indestår for at pålægge underdatabehandlere at anfægte udlevering af personoplysninger til tredjelandes myndigheder.

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

Databehandleren skal én gang om året 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.

Erklæringen skal udarbejdes i overensstemmelse med anerkendte standarder, fx ISAE 3000 type 1.

Alternativt kan Databehandleren udfylde den dataansvarliges spørgeskema.

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. Den dataansvarlige skal i så fald bære alle udgifter i forbindelse med den nye erklæring.

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 vederlagsfrit at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion.

I det omfang den dataansvarlige måtte ønske yderligere foranstaltninger i forhold til den dataansvarliges kontrol, herunder f.eks. udlevering af logfiler, afholdes eventuelle udgifter hertil af den dataansvarlige selv.

**C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere**

Databehandleren skal føre kontrol med sine underdatabehandlere. Dette sker ved at Databehandleren én gang årligt for sin egen eller sin underdatabehandlers regning indhenter en revisionserklæring fra en uafhængig tredjepart vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser. Erklæringen, der også kan være en egen-erklæring, skal udarbejdes i overensstemmelse med anerkendte standarder, fx ISAE 3000 type 1.

Alternativt kan Databehandleren eller en repræsentant for Databehandleren foretage inspektion, evt. 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 én gang årligt.

Revisionserklæringen fremsendes til den dataansvarlige, hvis den dataansvarlige anmoder herom. 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. Den dataansvarlige skal i så fald bære alle udgifter i forbindelse med den nye erklæring.

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.

Dokumentation for inspektioner fremsendes til den dataansvarlige, hvis denne anmoder herom. 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. Den dataansvarlige skal i så fald bære alle udgifter i forbindelse med en ny inspektion.