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 [titel/navn og dato på aftalen/ydelsen] 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 nærmere oplysninger om brud og håndtering af brud hos databehandleren eller dennes underdatabehandlere.

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.

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 specifik skriftlig godkendelse fra den dataansvarlige.

3. Databehandleren må kun gøre brug af underdatabehandlere med den dataansvarliges forudgående specifikke skriftlige godkendelse. Databehandleren skal indgive anmodningen om en specifik godkendelse mindst 60 dage inden anvendelsen af den pågældende underdatabehandler. 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.

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. Denne databehandleraftale skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og databehandleraftalen kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

8. Bistand til den dataansvarlige

1. 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

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:

   - 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.

3. Parterne kan 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 kan 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.

3. Databehandleren fremsender dokumentation for, at den påkrævede sletning er foretaget hvis den dataansvarlige anmoder herom.

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

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	Lise Bernhardt
Stilling	Sekretariats- og digitaliseringschef
E-mail	lbe@solrod.dk
Underskrift	

   På vegne af databehandleren

   Navn
   Stilling
   Telefonnummer
   E-mail
   Underskrift

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.

Navn	Martin Rynkeby Sinding
Stilling	Digitaliseringskonsulent
Telefonnummer	56 18 20 03
E-mail	mrsi@solrod.dk

   Navn
   Stilling
   Telefonnummer
   E-mail

Bilag A Oplysninger om behandlingen

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

Behandling af den dataansvarliges oplysninger sker i henhold til formålet i Hovedaftalen.
Databehandleren må ikke anvende oplysningerne til andre formål.
Oplysningerne må ikke behandles efter instruks fra andre end den dataansvarlige.

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

[Her beskriver databehandleren udførligt de typer af behandling, som databehandleren udfører i henhold til formålet i Hovedaftalen, herunder processer, varigheden og karakteren af behandlingen.]

A.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede
Almindelige personoplysninger (Databeskyttelsesforordningens artikel 6)

☐ Almindelige personoplysninger

[*Databehandleren angiver her typen/typerne af personoplysninger; fx stamoplysninger som navn, adresse, fødselsdato, tlf. nummer, e-mail m.v.*]

Følsomme personoplysninger (Databeskyttelsesforordningens artikel 9):
☐ Racemæssig eller etnisk baggrund
☐ Politisk overbevisning
☐ Religiøs overbevisning
☐ Filosofisk overbevisning
☐ Fagforeningsmæssige tilhørsforhold
☐ Helbredsforhold, herunder misbrug af medicin, narkotika, alkohol m.v.
☐ Seksuelle forhold

Oplysninger om enkeltpersoners rent private forhold
☐ Strafbare forhold
☐ Væsentlige sociale problemer
☐ Andre rent private forhold, som ikke er nævnt ovenfor:

[*Databehandleren angiver personoplysninger om private forhold, hvis dette er relevant]*

Oplysninger om cpr-nummer (Databeskyttelsesforordningens artikel 87)
☐ CPR-numre

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

A) [*Indsæt kategori af personer*]

B) [*Indsæt kategori af personer*]

C) [*Indsæt kategori af personer*]

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

[Indsæt evt. varighed]

A.6 Indsamlingen/modtagelsen eller overførslen af personoplysningerne foretages på følgende måde

[Databehandleren beskriver metoden]

A.7 Databehandleren har udarbejdet en databeskyttelsespolitik

☐ Ja ☐ Nej

A.8 Databehandleren har udarbejdet en fortegnelse over alle behandlingsaktiviteter, som til enhver tid kan fremvises, hvis det er relevant

☐ Ja ☐ Nej

A.9 Databehandleren har udarbejdet og implementeret politikker og procedurer vedrørende opbevaring af personoplysninger og sikker bortskaffelse af udstyr, medier, dokumenter, og kan fremvise disse politikker

☐ Ja ☐ Nej

A.10 Databehandleren har sikret, at den dataansvarliges data er tilstrækkelig adskilt fra andre data

☐ Ja ☐ Nej

A.11 Databehandleren har foretaget risikovurdering af behandlingsaktiviteten og den kan efter aftale udleveres til den dataansvarlige

☐ Ja ☐ Nej

A.12 Data slettes automatisk i løsningen. Hvis ja beskrives det nedenfor hvordan

☐ Ja ☐ Nej
[Databehandleren udfylder]

A.13 Der er fritekstfelter i løsningen herunder, men ikke begrænset til: tekstfelter til besvarelse af spørgsmål, beskedfunktioner i løsningen, mulighed for at lave profiltekster, muligheder for beskrivelse af billeder, objekter mv.

☐ Ja ☐ Nej

A.14 Det er muligt at bruge løsningen til at kontakte personer via for eksempel mails, SMS'er mv.

☐ Ja ☐ Nej

Bilag B Underdatabehandlere

B.1 Databehandleren angiver de foranstaltninger som gennemføres af databehandleren, for at kontrollere om underdatabehandlernes overholder gældende databeskyttelseslovgivning, herunder om underdatabehandleren har et tilstrækkeligt sikkerhedsniveau.

[Databehandleren udfylder]

B.2. 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 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.

B.3. Varsel for godkendelse af underdatabehandlere
Databehandleren skal indgive anmodningen om en specifik godkendelse mindst 60 dage inden anvendelsen af den pågældende underdatabehandler.

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 udfylder]

C.2 Behandlingssikkerhed
Databehandleren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de aftalte behandlinger, og som dermed opfylder Databeskyttelsesforordningens artikel 32.

Foranstaltningerne fastlægges ud fra overvejelser om:

- 1. Hvad der kan lade sig gøre rent teknisk
- 2. Implementeringsomkostningerne
- 3. Den pågældende behandlings karakter, omfang, sammenhæng og formål
- 4. Konsekvenserne for borgerne ved et sikkerhedsbrud
- 5. Den risiko, der er forbundet med behandlingerne, herunder risikoen for:

    a) tilintetgørelse af oplysningerne

    b) tab af oplysningerne

    c) ændring af oplysningerne

    d) uautoriseret videregivelse af oplysningerne

    e) uautoriseret adgang til oplysningerne

[Databehandler udfylder]

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

C.2.1 Sikkerhedscertificeringer
Databehandleren har sikkerhedscertificeringer, fx ISO27001, som kan udleveres ved anmodning

☐ Ja ☐ Nej

C.2.2 Pseudonymisering og kryptering
Databehandleren er forpligtet til at pseudonymisere og kryptere data, når dette er relevant og muligt.
Dekrypteringsnøgler gemmes og kontrolleres på følgende måde:

[Databehandler udfylder]

C.2.3 Fysisk eller teknisk hændelse
Databehandleren skal hurtigst muligt genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.

C.2.4 Funktionsadskillelse
Databehandleren er forpligtet til at have logisk og fysisk funktionsadskillelse for så vidt det er muligt.

C.2.5 Fortrolighed
Databehandleren har pligt til at instruere de ansatte, der har adgang til eller på anden måde varetager behandling af den dataansvarliges personoplysninger, om databehandlerens forpligtelser, herunder bestemmelserne om tavshedspligt og fortrolighed samt fortrolighedserklæringer.

C.2.6 Uddannelse mm.
Databehandleren har pligt til at sikre, at de ansatte har den nødvendige bevidsthed og uddannelse i databeskyttelse og datasikkerhed.

C.2.7 Transmission af oplysninger over internettet
Ved tilslutning til internet eller andre åbne net skal der træffes foranstaltninger, som sikrer imod, at uvedkommende får adgang til databehandlerens interne net.
Ved transmission af personoplysninger over det åbne internet (fx e-mail) skal databehandleren efterleve følgende minimumskrav:

- Transmission af følsomme personoplysninger, CPR-nummer og oplysninger om strafbare forhold, skal ske ved forsvarlig kryptering.
- Sikkerhed for afsenderes og modtagers identitet (autencitet) skal sikres i fornødent omfang ved anvendelse af fx digital signatur eller individuelle fortrolige adgangskoder

C.2.8 Adgangsstyring
Kun de personer hos databehandleren, som er autoriseret hertil, må have adgang til personoplysningerne, og der er etableret en adgangsstyringspolitik.
Der må ikke gives adgangsrettigheder til personoplysninger i videre omfang, end de pågældende har behov for i deres jobfunktion.

Medarbejdernes adgangskoder skal være tilstrækkelig komplekse.
Der skal føres kontrol med afviste adgangsforsøg, og der skal blokeres for yderligere forsøg efter flere afviste adgangsforsøg.

Der føres kontrol med afviste adgangsforsøg på følgende måde:

[Databehandler udfylder]

C.2.9 Anti-virus, antimalware og firewall
Databehandleren skal anvende anerkendte Anti-virus, antimalware og firewall programmer med henblik på at beskytte personoplysninger bedst muligt.

C.2.10 Sikkerhedsopdateringer
Databehandleren er forpligtet til løbende at foretage sikkerhedsopdateringer af styresystemer og andre relevante systemer med henblik på at beskytte personoplysningerne.

C.2.11 Backup
Databehandleren er forpligtet til at tage backup af personoplysningerne og med jævne mellemrum foretage restore tests af backup.
Databehandleren skal kunne dokumentere, at der foretages backup og restore tests af backup.

C.2.12 Logning
Alle transaktioner med følsomme personoplysninger, cpr-numre og oplysninger om strafbare forhold skal logges og loggen skal indeholde oplysninger om:

- Tidspunkt
- Bruger
- Type af anvendelse
- Angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium.

Loggen opbevares i [*Databehandleren udfylder*] måneder, hvorefter den slettes.

C.2.13 Fysisk sikkerhed
Der skal træffes sikkerhedsforanstaltninger til hindring af uvedkommendes adgang til personoplysninger, som databehandleren behandler i medfør af aftalen.

C.2.14 Sikring af udstyr
I forbindelse med reparation, service eller destruktion af udstyr og medier, som indeholder personoplysninger omfattet af aftalen, skal det sikres, at uvedkommende ikke får adgang til personoplysningerne.

C.2.15 Hjemmearbejdspladser/fjernarbejdspladser
Databehandlerens behandling af personoplysninger sker helt eller delvist ved anvendelse af hjemmearbejdspladser/fjernarbejdspladser [*Databehandleren udfylder*]

☐ Ja ☐ Nej

- Den dataansvarlige skal godkende brugen af hjemme – eller fjernarbejdspladser
- Der skal anvendes 2-faktor-autentifikation.
- Der må kun etableres eksterne IT-kommunikationsforbindelser, hvis der efter godkendelse og efter nærmere aftale herom træffes foranstaltninger, som sikrer, at uvedkommende ikke gennem disse forbindelser får adgang til personoplysninger.
- Der skal foretages foranstaltninger, der sikrer, at personoplysninger, der transmitteres over åbne net, som fx internettet, ikke fortabes, ændres eller kommer til uvedkommendes kendskab under transmissionen. Dette sker ved krypteret forbindelse.
- Ved anvendelse af bærbare pc'er og hjemme-pc'er gælder principielt de samme retningslinjer som for databehandlerens almindelige IT-arbejdspladser.
- Den enkelte bruger og databehandler skal sikre, at der opretholdes en sikkerhed, der som minimum er på højde med den sikkerhed, som gælder i den dataansvarliges vante rammer. Al behandling af data, der kan klassificeres som følsomt eller fortroligt bør foregå på arbejdspladsen, men i særlige tilfælde kan det forekomme nødvendigt andre steder. I disse tilfælde må det ikke ske i det offentlige rum (tog, lugthavne o.lign.). Arbejdet skal i givet fald ske i diskrete rammer og altid via en sikret forbindelse (VPN/MPLS).
- Udskrivning af følsomt og/eller fortroligt materiale accepteres kun ved skriftlig aftale.
- Brug af fjernarbejdspladser skal aftales skriftligt med den dataansvarliges IT-sikkerhedsorganisation.

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

C.4 Opbevaringssted
Opbevaring af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse opbevares/hostes andre steder end følgende:

[Databehandler udfylder]

C.5 Overførsel af personoplysninger til tredjelande
Databehandleren overfører personoplysninger til tredjelande:

☐ Ja ☐ Nej

Overførselsgrundlaget er baseret på *[Databehandleren udfylder]*

Hvis der *ikke* overføres personoplysninger til tredjelande, kan dette til enhver tid dokumenteres:

☐ Ja ☐ Nej

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.

C.6 Tilsyn med underdatabehandlere
Databehandleren fører tilsyn med eventuelle underdatabehandlere, og kan dokumentere tilsynet hvis kommunen anmoder herom. Eventuelle udgifter i forbindelse med tilsyn af underdatabehandlere afholdes af databehandleren.

C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren eller dennes underdatabehandler
Databehandleren skal hvert år for egen regning indhente en revisionsrapport/inspektionsrapport fra en uafhængig tredjepart vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Revisionserklæringen fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Erklæringen skal udarbejdes i overensstemmelse med "gældende, anerkendte branchestandarder på området", og skal omfatte både databehandlerens og eventuelle underdatabehandleres databehandling. Den dataansvarlige kan anfægte rammerne for og/eller metoden 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 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 Datarettigheder

C.8.1 Udlevering af personoplysninger
Databehandleren og dennes eventuelle underdatabehandlere udleverer hurtigst muligt oplysninger til brug for den registreredes indsigtsret, hvis den dataansvarlige anmoder om oplysningerne.

C.8.2 Passende format

Databehandleren og dennes eventuelle underdatabehandlere udleverer oplysningerne i et passende format i overensstemmelse med relevant lovgivning, hvis den dataansvarlige anmoder herom.

C8.3 Sletning
Databehandleren og dennes eventuelle underdatabehandlere sletter oplysninger, hvis den dataansvarlige anmoder herom.

Bilag D Oplysninger vedrørende databrud

D.1 Databehandleren beskriver de nærmere forhold, hvis der har været et databrud hos databehandleres eller underdatabehandleren inden for de seneste 3 år, eller har været genstand for undersøgelse hos en databeskyttelsestilsynsmyndighed eller en kundetvist

[Databehandler udfylder]

D.2 Databehandleren har en dokumenteret beredskabsplan/hændelsesstyringsproces, som følges i tilfælde af persondatasikkerhedsbrud, og denne kan fremvises ved anmodning

☐ Ja ☐ Nej

D.3 Databehandleren har procedurer for it-beredskab

☐ Ja ☐ Nej

D.4 Kontaktpersoner vedrørende brud

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

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

Solrød Kommune:

Navn: Mille Ellund
Stilling: GDPR-konsulent
Telefonnummer: 29 47 73 60
E-mail: Sikkerhedsbrud@solrod.dk

Databehandler:

Navn:
Stilling:
Telefonnummer:
E-mail: