DATABEHANDLERAFTALER

MELLEM

HØRSHOLM KOMMUNE OG [LEVERANDØR]

version 4.0 af 19. august 2020

Standardkontraktsbestemmelser

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

mellem

Hørsholm Kommune
CVR 70960516
Slotsmarken 13
2970 Hørsholm
Danmark

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

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 fritvalgsindsatser indenfor praktisk hjælp og personlig pleje 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 bestemmelser 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.

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 generel skriftlig godkendelse fra den dataansvarlige. Underdatabehandlere skal findes inden for EU.

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 6 ugers 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 databe-

skyttelsesforpligtelser 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 tilbagelevere alle personoplysningerne og slette eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

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

a. Ingen, partnerne bekendt.

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 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.

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	Dorte Dahl
Stilling	Centerchef, Sundhed og Omsorg
Telefonnummer	4849 3660
E-mail	dda@horsholm.dk
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	Malene Frost
Stilling	Systemadministrator
Telefonnummer	4849 3666
E-mail	mafr@horsholm.dk

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

Bilag A Oplysninger om behandlingen

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

Formålet med behandlingen af personoplysninger er at databehandler kan yde service til udvalgte borgere i Hørsholm Kommune, hvor der er behov for personlig pleje og praktisk hjælp.

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

Behandling af persondata til planlægning og koordinering af borgerbesøg, at læse borgerens informationer med henblik på, at give den korrekte ydelse til den korrekte borger, samt opdatering af borgerens journal med udførte ydelser/pleje samt plejeinformationer om borgeren.

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

☒ Almindelige personoplysninger:

Navn, adresse, telefonnummer, kontaktpersoner, pårørende, sygedage, familieforhold, bolig, bil, stilling, arbejdsområde, arbejdstelefon, fødselsdato.

Følsomme personoplysninger om (jf. Databeskyttelsesforordningens artikel 9):

☒ Race eller etnisk oprindelse
☐ Politisk overbevisning
☒ Religiøs overbevisning
☐ Filosofisk overbevisning
☐ Fagforeningsmæssigt tilhørsforhold
☐ Genetiske data
☐ Biometriske data
☒ Helbredsoplysninger, herunder misbrug af medicin, narkotika, alkohol, sygdomshistorik, medicinhistorik, plejebehov, diagnoser m.v.
☒ En fysisk persons seksuelle forhold eller seksuelle orientering

Personoplysninger om straffedomme og lovovertrædelser (jf. Databeskyttelses-forordningens artikel 10):

☒ Straffedomme
☒ Lovovertrædelser

Oplysninger om CPR-nummer (jf. Databeskyttelseslovens § 11)

☒ CPR-numre

A.4. Behandlingen omfatter følgende kategorier af registrerede

A) Børn der er visiteret til pleje
B) Voksne der er visiteret til pleje
C) Udenbysborgere i ældreboliger
D) Kontaktpersoner/nærmeste pårørende
E) Oplysninger om kontaktpersoner internt og eksternt

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

Behandlingen er ikke tidsbegrænset og varer så længe, det er relevant for databehandlerens udførelse af de aftalte opgaver og efterlevelse af forpligtelser over for den dataansvarlige i Hovedaftalen.

Bilag B Underdatabehandlere

Med nærværende kontrakt er bestemmelsen mellem Kommunen og Leverandøren, at Leverandøren ikke må benytte underleverandører, jævnfør kontrakten afsnit 9. Derfor vil der i dette samarbejde ikke forekomme underdatabehandlere.
I tilfælde af at denne bestemmelse ændres, vil det være nedenstående retningslinjer, der skal følges.

Ved bestemmelsernes ikrafttræden skal databehandleren havde godkendt underdatabehandlere af dataansvarlige, inden samarbejdet med underdatabehandleren kan opstarte.
Godkendelsen skal ske ved udfyldelse af nedenstående skema.

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.
Varsel for godkendelse af underdatabehandlere er 6 ugers varsel.

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:

Alle Databehandlerens medarbejdere, der leverer ydelser hos udvalgte borgere i Kommunen, skal kunne tilgå Kommunens omsorgssystem Nexus i forbindelse med planlægning og udførelse af indsatser. Omsorgssystemet tilgås via PC på Databehandlerens adresse såvel som via en app på mobiltelefon eller tablet, således at der kan slås op og dokumenteres ude hos borgeren eller på ruten.

Databehandlerens medarbejdere skal planlægge deres besøg på en digital planlægningstavle og i borgerens kalender i omsorgssystemet. Desuden skal databehandlerens medarbejderne i borgerens journal via notater dokumentere det udførte arbejde og informationer fra besøget, som kan være relevante for den videre indsats hos borgeren.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Ud over almindelige personoplysninger (art. 6) omfatter behandlingen også en større mængde personoplysninger, som er opfattet af Databeskyttelsesforordningens art. 9 om "Særlige kategorier af personoplysninger", og der skal derfor etableres et højt sikkerhedsniveau.

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

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

1. Pseudonymisering og kryptering
Pseudonymisering af personoplysningerne er ikke nødvendigt, da data opbevares i Kommunes system.

2. Awareness og opdatering af sikkerhedspolitik
Databehandlerens medarbejdere, der arbejder med Kommunens data, skal have vejledning og instruktion i, hvordan persondata behandles så sikkert som muligt.

Databehandler skal hele tiden holde sig opdateret om gældende persondatalovgivning.

3. Adgang til oplysningerne
Data må ikke komme til uvedkommendes kendskab i henhold til gældende sikkerhedskrav, jf. Databeskyttelsesforordningen.

Kun personer, der har et sagligt behov må få adgang til kommunens oplysninger. Medarbejdere, der behandler persondata, skal bruge en unik brugeridentifikation med et unikt, personligt og fortroligt password for at få adgang og login må ikke deles.

Medarbejdere, der behandler persondata, må ikke have adgang til mere, end de har behov for, for at udføre opgaven.

Overlades en it-arbejdsplads til en anden, skal der først logges af, og kollegaen skal logge på med eget brugernavn og adgangskode.

Hvis en medarbejder stopper eller får en anden funktion i virksomheden, skal medarbejderens adgang til at behandle persondata straks lukkes.

Mindst hvert halve år skal der foretages kontrol af, om medarbejdernes adgange stadig er korrekte. Kontrollen skal dokumenteres.

Det er ikke tilladt at foretage usaglige, herunder private, opslag i persondata

4. Tavshedspligt
Som databehandler har du tavshedspligt, jf. forvaltningsloven samt sundhedsloven - kapitel 9 om tavshedspligt, videregivelse og indhentning af helbredsoplysninger, vejledning om sundhedspersoners tavshedspligt dialog og samarbejde med patienters pårørende, bekendtgørelse om information og samtykke i forbindelse med behandling og ved videregivelse og indhentning af helbredsoplysninger m.v. samt vejledning om information og samtykke og om videregivelse af helbredsoplysninger mv.
Alle oplysninger, som du får adgang til – både virksomhedsdata og personoplysninger– er fortrolige og må ikke videregives til andre. Det gælder også efter samarbejdets ophør.

5.Adgangskode
Til enhver tid skal den dataansvarliges retningslinjer følges. Adgang til it-udstyr sker via den dataansvarliges sikkerhedssystem.
Der skal kræves adgangskode for at logge på it-udstyr (herunder mobile enheder) og it-systemer som bruges til behandling af persondata. Adgangskoden skal opfylde følgende krav:

- Være på mindst 8 tegn – gerne flere
- Være en kombination af store og små bogstaver, tal og specieltegn
- Må højst løbe 90 dage
- Adgangskoden må ikke skrives ned
- En god adgangskode skal være svær at gætte for andre.

Adgangskoden er strengt personlig og må ikke videregives til andre. Ved mistanke om at andre kender adgangskoden, skal den ændres!

6. Pauseskærm
Aktivér pauseskærm med adgangskode, inden arbejdspladsen forlades - også selvom det kun er kortvarigt. Eksempelvis med 'Windows + L'.

Pauseskærmen skal indstilles til automatisk aktivering efter 10 minutter.

Mobiltelefoner bliver automatisk låst og logget ud af systemer, når telefonen ikke er aktiv via den dataansvarliges mdm-system.

7. Sikkerhed mod virus, hacking og spam
Kommunen kræver at databehandlerens computere er forsynet med passende sikkerhedsforanstaltninger mod virus, hacking og spam. Disse sikkerhedsforanstaltninger skal mindst indeholde følgende:

- Et moderne og tidssvarende antivirusprogram med mailscanning
- En firewall

Sikkerhedspakken skal opdateres jævnligt, og der skal ligeledes jævnligt laves en totalscanning af harddisken.

Computeren skal sættes til at opdatere styresystem og software automatisk, eksempelvis sikkerhedspakker fra Microsoft, Adobe mv.

Hvis virksomheden har mere end 5 computere/enheder, anbefales det, at der installeres en central sikkerhedsløsning som indeholder antivirus og opdatering af systemet.

Databehandlerens mobile enheder sikres med en MDM-løsning af kommunen. MDM-løsningen sikrer at de mobile enheder kun har installeret de apps, som er nødvendige for databehandleren.

8. Internet

Hvis databehandleren anvender trådløst netværk, skal stærk kryptering være slået til, så andre ikke kan bruge netværket. Der bør vælges en lang og kompleks krypteringsnøgle.

Ved brug af internet skal det sikres, at uvedkommende trafik ikke kan få adgang fra det åbne net til databehandlerens interne net.

Systemet skal være indstillet sådan, at personlige oplysninger altid slettes, når en browser lukkes ned.

Browseren skal indstilles sådan, at brugeren altid bliver spurgt, inden filer, informationer, programmer m.v. bliver overført til computeren.

9. Installation og opdatering af programmer

Databehandleren skal sørge for, at styresystem og andre programmer hele tiden er opdateret, og at der ikke anvendes programmer, der ikke er så gamle, at Databehandleren ikke længere kan yde support til dem.

10. Sikker mail og digital post

Fortrolige eller følsomme personoplysninger skal sendes sikkert, dvs. via digital post eller krypteret, hvis de sendes via e-mail, f.eks. via Virk.dk.

Mails med Persondata må ikke gemmes i Outlook (eller lignende systemer), men skal slettes løbende og senest efter 30 dage. Mails, der skal fungere som dokumentation, skal lægges på borgerens sag i omsorgssystemet.

11. Opbevaring af data

Databehandleren må alene behandle og opbevare data vedrørende Kommunen og borgere (dataansvarliges data) i Kommunens it-systemer. Data må ikke behandles i andre systemer.

Bærbare pc'er og andre mobile enheder, der har adgang til Kommunens data, skal opbevares aflåst, når disse ikke anvendes. Bærbare enheder må ikke efterlades i fx en bil, selvom denne er aflåst.

12. Papirmateriale

Papirmateriale, der indeholder personoplysninger af fortrolig eller følsom karakter, skal opbevares i et aflåst skab, skuffe eller lokale, når det ikke anvendes.

Når materialet anvendes, skal Databehandleren opbevare materialet sikkert og under opsyn. Printere skal placeres så uvedkommende ikke kan få adgang. Udskifter med personoplysninger skal hentes straks efter de er printet.

Papirmateriale med personoplysninger skal bortskaffet sikkert umiddelbart efter anvendelse.

13. Reparation eller kassation af udstyr
Hvis computere eller andet dataudstyr skal repareres eller til service, skal det sikres, at reparations- eller servicepersonalet behandler oplysninger, som de evt. måtte få viden om gennem deres arbejde, som fortroligt materiale, der ikke må anvendes eller videregives. Hvis det er muligt, skal oplysningerne på udstyret slettes inden reparation eller service.

Hvis dataudstyr eller medier, der indeholder Kommunens data, skal kasseres, skal dette destrueres eller afmagnetiseres på en sådan måde, at man ikke længere kan læse indholdet.

Kommunen fraråder Databehandleren at sælge eller bortgive udstyr, som har været anvendt til behandling af personoplysninger. Harddiske eller lagringsmedier bør i stedet destrueres fysisk, medmindre der kan garanteres en fuldstændig sikkerhedsletning.

14. Fysisk sikring af datalokationer
De lokationer, hvor oplysningerne behandles, skal sikres, så uvedkommende ikke kan få adgang til oplysningerne, dvs., at lokaler skal aflåses forsvarligt, der skal evt. være etableret et alarmsystem, adgang til et eventuelt serverrum skal være begrænset, og skærme og printere skal placeres sikkert, og så uvedkommende ikke kan få adgang til dem. Ved arbejdstids ophør skal døre og vinduer lukkes.

15. Hjemme-/fjernarbejdspladser
Kommunens data må kun behandles på Databehandlerens hovedlokation samt Databehandlerens mobile enheder. Hjemmearbejdspladser accepteres ikke.

16. Logning
Kommunen foretager maskinel registrering (logning) i omsorgssystemet.

Loggen indeholder oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrører eller det anvendte søgekriterium.

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:

- Udarbejde retningslinjer, herunder passende databeskyttelsespolitikker, for bistand i forbindelse med den dataansvarliges overholdelse af de registreredes rettigheder. Disse retningslinjer skal udleveres til den dataansvarlige på dennes anmodning.

- Databehandleren skal påse overholdelsen af de interne retningslinjer. Retningslinjerne skal revideres mindst én gang årligt for at sikre deres fortsatte relevans og tilstrækkelighed.

- Databehandleren etablerer procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden.

C.4 Opbevaringsperiode/sletterutine

Personoplysninger opbevares i kommunens omsorgssystem. Eventuelle personoplysninger opbevaret hos databehandleren skal slettes efter endt brug og senest efter 14 dage.

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 dataansvarliges 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:

Personoplysninger behandles hos:
[Leverandørnavn]
[Adresse]
[Postnummer og by]

samt i borgerens hjem.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Databehandler må ikke overføre personoplysninger til tredjelande og skal sikre, at underdatabehandler heller ikke overfører personoplysninger til tredjelande.

En overførsel kan f.eks. bestå i en overførsel af personoplysninger via internettet, via en USB-nøgle eller i at personer i et tredjeland får adgang til at se personoplysninger, der fysisk befinder sig i EU.

Ved tredjeland skal forstås som et land, der ikke er medlem af EU eller EØS (Island, Liechtenstein og Norge).

Personoplysninger skal opbevares i EU.

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

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

Der er enighed mellem parterne om, at erklæringen skal udarbejdes i overensstemmelse med gældende anerkendte branchestandard svarende til ISAE 3000.

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

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

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

Bilag D Parternes regulering af andre forhold

D.1 Kommunikation om databrud

Leverandøren må ikke hverken offentligt eller til tredjeparter kommunikere om brud på persondatasikkerheden, uden forudgående skriftlig aftale med Kommunen om indholdet af en sådan kommunikation.

D.2 Erstatning

1. Databehandleren skal skadesløsholde den Dataansvarlige, såfremt den Dataansvarlige bliver mødt med krav fra tredjemand som følge af, at Databehandleren i sin rolle eller Databehandlerens eventuelle underleverandører i deres rolle som underleverandør har overtrådt den til enhver tid gældende dataretlige lovgivning. Databehandleren hæfter kun for skader, hvis Databehandleren eller dennes eventuelle underleverandører ikke har opfyldt sine forpligtelser som og/eller underdatabehandlere, som det følger af den til enhver tid gældende lovgivning, eller hvis Databehandleren som eller dennes eventuelle underleverandører som underdatabehandlere har undladt at følge eller handlet i strid med den Dataansvarliges lovlige instruks. Forpligtelsen til at skadesløsholde den Dataansvarlige er ikke omfattet af en eventuel aftalt erstatningsmaksimering i Kontrakten. Leverandørens forpligtelse til at skadesløsholde den Dataansvarlige efter nærværende afsnit gælder ikke for bøder pålagt den Dataansvarlige i medfør af databeskyttelsesforordningens artikel 83 eller sanktioner fastlagt i Danmark i overensstemmelse med databeskyttelsesforordningens artikel 84.

2. Databehandleren indestår - uden tidsbegrænsning - for, at det leverede ikke krænker tredjemands, herunder Databehandlerens underleverandørers, rettigheder. Rejses der et krav mod den Dataansvarlige, giver den Dataansvarlige Databehandleren skriftlig meddelelse herom, og Databehandleren overtager herefter sagen og samtlige hermed forbundne omkostninger. Databehandleren er i enhver henseende pligtig til at skadesløsholde den Dataansvarlige for enhver omkostning i forbindelse med sagen, herunder omkostninger til advokat m.v. samt sagsomkostninger, som måtte blive tilkendt den registrerede.

Databehandleren skal skadesløsholde den Dataansvarlige for ethvert krav, som måtte gøres gældende overfor den Dataansvarlige eller enhver indirekte eller direkte omkostning og tab, som den Dataansvarlige måtte blive påført som følge af, at det leverede krænker tredjemands rettigheder, herunder afholde alle omkostninger, der er nødvendige for, at [f.eks. systemet] kan anvendes som forudsat i Databehandleraftalen. [Husk at undersøge om der allerede er taget stilling til ansvarsbegrænsning/ansvarsfraskrivelse i hovedaftalen]

Databehandleren skal straks give den Dataansvarlige skriftlig meddelelse, såfremt Databehandleren bliver opmærksom på eventuelle rettighedskrænkelser og bistå den Dataansvarlige under sagen i fornødent omfang.