UDKAST

Standardkontraktsbestemmelser

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

mellem

Frederiksberg Kommune
CVR 11259979
Smallegade 1
2000 Frederiksberg
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 Madservice til hjemmeboende borgere i Frederiksberg Kommune (herefter "Rammeaftalen") 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 4 bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.

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

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

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

9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke af omfattet af Bestemmelserne.

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

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

3. Den dataansvarliges rettigheder og forpligtelser

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

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

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

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

4. Databehandleren handler efter instruks

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

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

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.

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 30 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

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 hvis muligt 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 slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlig, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

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

På vegne af databehandleren

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

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

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

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

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

Bilag A Oplysninger om behandlingen

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

Levering af madservice til hjemmeboende borgere i henhold til Rammeaftalen om levering af madservice.

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

Levering af madservice til hjemmeboende borgere med tilhørende afregning af kommune og borgere for egenbetaling.

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

☒ Almindelige personoplysninger.

Navn, adresse, visiteret kostform og ydelsesfrekvens.

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 m.v.
☐ En fysisk persons seksuelle forhold eller seksuelle orientering

Oplysninger om borgers funktionsniveau af betydning for ydelsesleveringen.

Eksempel: ”Borger er dårligt gående”, ”vent på borger åbner døren”, Eller: ”Borger er dårligt hørende, ring på 3 gange. Derudover er der tillige oplysninger om borgerens kostvalg.

Personoplysninger om straffedomme og lovovertrædelser (jf. Databeskyttelsesforordningens artikel 10):
☐ Straffedomme
☐ Lovovertrædelser

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

☐ Andre fortrolige oplysninger, som defineret i dansk lovgivning.
Udbyd, fx væsentlige private forhold, tvangsfjernelser: prosatekst

A.4. Behandlingen omfatter følgende kategorier af registrerede

Hjemmeboende borgere visiteret til madserviceordning i henhold til Servicelovens §83.

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

Databehandleren behandler personoplysninger, så længe hovedaftalen mellem parterne består og i øvrigt i overensstemmelse med afsnit 11 i nærværende aftale samt gældende lovgivning.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

[Skemaet nedenfor udfyldes af databehandleren forud for indgåelse af databehandleraftalen og godkendes først af den dataansvarlige ved underskrift af aftalen.

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.

B.2. Varsel for godkendelse af underdatabehandlere

Vi henviser til pkt. 7.3, hvor varselsfrist er sat til 30 dage

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:

Levering af madservice til kommunens hjemmeboende borgere jf. Rammeaftalen

Databehandleren er forpligtet til at kommunikere med Frederiksberg Kommune via det til enhver tid gældende IT- og omsorgssystem i kommunen (på nuværende tidspunkt CURA)

Databehandleren modtager ved opstart af en ny borger oplysninger via kommunens omsorgssystem CURA, om borgers bopæl, hvilken kostform borger er visiteret til, hvorledes borgers egenbetaling skal opkræves, og om der er særlige forhold, der skal tages hensyn til i forbindelse med leveringen.

Databehandleren tager kontakt til borger og aftaler leveringstidspunkter og om der er individuelle behov eller ønsker, der skal tages hensyn til.

I forhold til den daglige drift skal databehandleren oplyse borger om, hvilke madserviceydelser der tilbydes, normalt ved at der udsendes en menuplan med de tilbudte valgmuligheder for den kommende måned.

Databehandleren skal registrere, hvilke ydelser borger bestiller og ønsker leveret. Derudover skal ændringer i ydelsesleveringen, herunder midlertidig og permanente ophør i ordningen, registreres.

Databehandleren skal hver dag tjekke i CURA, om der er borgere, der er indlagt eller på anden vis fraværende, for herved at undgå forgæves gang. Hvis informationerne ikke er tilgængelige i CURA, kontaktes databehandleren af Visitation- og Hjælpemidler.

Databehandleren vil blive kontaktet af Visitation- og Hjælpemidler via CURA, når borgeren igen er udskrevet og skal genindtræde i ordningen.

I forhold til opkrævning af kommunen skal databehandleren udover standardoplysninger vedlægge et bilag som beskriver, hvilke borgere der har fået leveret hvad og hvornår.
Oplysningerne er nærmere beskrevet i Kravspecifikation punkt 16.

Borgerens egenbetaling for madservice håndteres af databehandleren på vegne af ordregiver via leverandøren af kommunens Pensionssystem og foregår som et træk i borgerens pension.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle behandlingens karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder – elementerne, som er afgørende for sikkerhedsniveauet.

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.

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

I. Politik og regler for informationssikkerhed

Databehandleren skal have udarbejdet en ledelsesgodkendt politik og regelsæt for informationssikkerhed i virksomheden. Databehandleren skal sikre, at medarbejdere vejledes og efterlever informationssikkerhedsreglerne.

Databehandleren skal sikre, at der er implementeret en procedure for håndtering af sikkerhedshændelser, som inkluderer rettidig orientering til den dataansvarlige, såfremt sikkerhedshændelsen omfatter personoplysninger, som behandles på dennes vegne.

II. Autorisation og adgangskontrol

Databehandleren skal udarbejde en procedure for adgangsstyring og brugeradgange, som sikrer, at det kun er relevante medarbejdere, som har adgang til personoplysninger og fortrolige data, og at adgange ophører, når medarbejdere ikke længere har brug for adgangen eller ophører i deres stilling.

Der skal anvendes individuelt login, og kodeord med passede kompleksitet.

III. Afprøvning, vurdering og evaluering

Databehandleren skal sikre, at der foreligger en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden.

IV. Ind- og uddata

Databehandleren skal sikre, at der er instruktioner og vejledning til medarbejdere hos databehandleren, som sikrer behandling, ansvar og destruktion af ind- og uddatabehandling, herunder personoplysninger som behandles i mailsystemer, support platforme, skyen mv.

Databehandleren skal sikre, at der er opsat en kommunikationskanal, fx en sikker e-mailadresse eller support platform, som den dataansvarlige kan kontakte databehandlere på, og som er opsat med passende sikkerhed, og som sikrer beskyttelse af oplysninger under transmission.

V. Fysisk sikring af lokaliteter, hvor data opbevares (servere)

Databehandleren skal sikre passende sikkerhedsforanstaltninger af fysiske lokaliteter, fx serverum eller virksomhedens kontorlokaler.

Der skal være udarbejdet en procedure, som sikrer, at der er restriktioner på fysisk adgang til serverum, og det kun er medarbejdere med et arbejdsbetinget formål, som har adgang. Databehandleren skal sikre, at der foreligger en beredskabsplan, som afprøves med passende interval.

VI. It-udstyr og opbevaring af personoplysninger

Databehandleren skal sikre, at it-udstyr, herunder mobiltelefoner, computere og tablets, som de anvender til opgaven, har den nødvendige beskyttelse og er forsynet med sikringsforanstaltninger, som beskytter data på udstyret og i de interne systemer mod skadevoldende programmer og kode samt virus. Beskyttelse af fysisk it-udstyr skal være af en sådan grad, at indholdet ikke kan kompromitteres i tilfælde af tyveri.

Der må ikke behandles personoplysninger på medarbejders private it-udstyr eller i programmer og applikationer, som ikke er godkendt af arbejdspladsen.

It-udstyr som kasseres eller på anden måde afhændes, skal sikres imod, at lagrede data efterfølgende kan genskabes. Udstyr som kan genbruges, skal slettes for indhold og nulstilles inden det videregives til en ny medarbejder.

VII. Fysiske dokumenter

Såfremt det er nødvendigt at behandle personoplysninger i form af fysiske dokumenter, skal de fysiske dokumenter opbevares med passende sikkerhed. Der må ikke opbevares fysiske dokumenter med personoplysninger, som databehandleren behandler på vegne af den dataansvarlige, i medarbejders private hjem.

Kasseret papir med fortrolige oplysninger eller information, som kan misbruges, skal opbevares i markerede beholdere på områder som er adgangskontrolsikret, og bortskaffes ved makulering.

VIII. Hjemmearbejde

Hvis databehandleren anvender hjemmearbejdspladser eller i øvrigt arbejder uden for databehandlerens egne fysiske lokaler, skal der være tekniske foranstaltninger, herunder VPN, som sikrer at medarbejdere forsat behandler og tilgår personoplysninger med passende beskyttelse. Der skal være retningslinjer, som sikrer at uvedkommende ikke kan tilgå oplysningerne (inklusiv andre i medarbejderens private husstand), og at medarbejdere kender disse retningslinjer.

IX. Backup

Databehandleren skal sikre, at der gennemføres passende backup af personoplysninger, som behandles på vegne af den dataansvarlige, som gør at data kan genskabes såfremt der skulle forekomme nedbrud. Der er etableret en procedure, som sikrer at backup ikke opbevares længere end lovgivningen for forskellige datatyper tillader.

X. Logning

It-systemer som anvendes til behandling og lagring af følsomme og fortrolige personoplysninger, er indrettet med logningsfaciliteter, som lever op til gældende logningskrav. Der skal kunne fremfindes log minimum 6 måneder tilbage.

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 mistanke om sikkerhedsbrud, skal databehandleren, jf. afsnit 9.2. snarest tage kontakt til den dataansvarlige. Hvis sikkerhedshændelsen som skyldes forhold hos databehandleren, skal databehandleren snarest og, hvis muligt, allerede sammen med underretningen, fremsende følgende oplysninger:

I. Bekræfte, at det er personoplysninger, som Frederiksberg Kommune er dataansvarlig for.
II. Oplysning om hvorvidt det er en *mistanke* om sikkerhedsbrud eller der er *konstateret* et sikkerhedsbrud
III. En beskrivelse af, i let tilgængeligt og forståeligt sprog, hvad der er gået galt, hvorfor og hvilke foranstaltninger databehandleren allerede har gjort og hvad der er i proces.
IV. Oplysninger om omfanget: hvor mange registrerede er berørt og detaljeret oplysninger om hvem, herunder CPR-nummer, hvis tilgængeligt.
V. Oplysninger om omfanget: hvor mange har haft adgang til oplysningerne.
VI. Oplysninger om hvilke typer af personoplysninger, som er omfattet.

VII. Tidspunkt for sikkerhedsbruddet – start og slut
VIII. Tidspunkt for konstatering hos databehandleren og oplysning om hvordan databehandleren opdagede det.
IX. Navn og telefonnummer på en medarbejder hos databehandleren, som den dataansvarlige kan kontakte for uddybende spørgsmål.
X. Hvilke foranstaltninger databehandlere sætter i værks for at forhindre en gentagelse.

C.4 Opbevaringsperiode/sletterutine

Databehandleren skal opbevare data tre år fra rammeaftalens ophør, i hvilken periode Ordregiver kan bede om at få udleveret data, herunder til brug for eventuel korrigering af træk fra borgers pensionsordning. De tre år er begrundet i de almindelige forældelsesfrister.

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

C.5 Lokalitet for behandling
Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end oplyst i Bilag B.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande
Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsels af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler.

C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren
Det vil med udgangspunkt i en risikovurdering kunne accepteres, at databehandleren i overensstemmelse med Datatilsynets vejledning en gang om året for egen regning stiller en skriftlig status til rådighed for Frederiksberg Kommune.

Den dataansvarlige kan fravige den aftalte tilsynsform, såfremt den dataansvarlige vurderer, at databehandleren på anden vis vil kunne dokumentere overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser med tilhørende bilag.

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.

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

Databehandleren er forpligtet til på baggrund af en vurdering af risici i forbindelse med behandlingen af personoplysninger, at føre tilsyn med eventuelle underdatabehandlere. Databehandleren dokumenterer på forlangende de udførte tilsyn for den dataansvarlige indenfor en rimelig frist.

Baseret på resultaterne af tilsynet, 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.

Bilag D Parternes regulering af andre forhold

1. Kommunikation

Databehandleren må ikke hverken offentligt eller til tredjeparter kommunikere om brud på persondatasikkerheden, uden forudgående skriftlig aftale med kommunen om indholdet af en sådan kommunikation, medmindre databehandleren har en retlig forpligtelse til sådan kommunikation.

2. Underdatabehandler

Med mindre andet aftales, og databehandleren og den dataansvarlige er enige herom, skal al kommunikation mellem Frederiksberg Kommune og underdatabehandleren ske via databehandleren.