Databehandleraftale – baseret på Datatilsynets skabelon

Standardkontraktsbestemmelser

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

mellem

[Navn] Kommune
CVR [CVR-NR]
[Adresse]
"[Postnummer og by]"
[Land]

herefter "den dataansvarlige"

og

[Navn]
CVR [CVR-NR]
[Adresse]
"[Postnummer og by]"
[Land]

herefter "databehandleren"

der hver især er en "part" og sammen udgør "parterne"

HAR AFTALT følgende standardkontraktsbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder

Indhold

1. Præambel

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 drift og vedligeholdelse af et pladsanvisningssystem reguleret i "Hovedaftalen", behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.

5. Der hører tre bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.

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

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

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

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

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

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 blandt andet ansvarlig for 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.

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

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

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 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 3 måneders varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere var″I tilfælde hvor databehandleren eller underdatabehandlere er ophørt, eller er gået konkurs, skal personoplysningerne slettes, og evt. tilbageleveres jf. bestemmelse 11.1."sel 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. 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 under-

lagt, 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.

8. 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.

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 senest 48 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.

10. 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 dataansvarlige, at oplysningerne er slettet, 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. Arkivloven

   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 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.

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 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]

   Dato / Underskrift

   På vegne af databehandleren

Navn	[Navn]
Stilling	[Stilling]
Telefonnummer	[Telefonnummer]
E-mail	[E-mail]

   Dato / 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.

   Dataansvarlig:

   Særligt ved sikkerhedsbrud jf. afsnit 9 og bilag C.3:

E-mail	[E-mail]

Navn	[Navn]
Stilling	[Stilling]
Telefonnummer	[Telefonnummer]
E-mail	[E-mail]

Databehandler:

Navn	[Navn]
Stilling	[Stilling]
Telefonnummer	[Telefonnummer]
E-mail	[E-mail]

Bilag A Oplysninger om behandlingen

A.1. Formålet med den dataansvarliges behandling af personoplysninger, hvormed databehandleren skal behandle dem

Databehandleren stiller nedenstående system til rådighed for den dataansvarlige. Systemet fungerer som pladsanvisningssystem med henblik på at den dataansvarlige kan levere lovpligtige ydelser til borgerne inden for dagtilbudsloven.

Systemet stilles til rådighed for den dataansvarlige via SaaS-løsninger.

Databehandler bistår bl.a. den dataansvarlige på følgende områder:

- Drift og vedligeholdelse af systemet
- Support og fejlhåndtering, således at den dataansvarlige har anvendelige data for arbejdet med borgerne. Data skal kunne understøtte den dataansvarliges arbejde inden for pladsanvisning.
- Rapportering af den dataansvarliges data

Leverandøren må ikke anvende oplysningerne til andre formål.

Oplysningerne må ikke behandles efter instruks fra andre end den dataansvarlige.

Systemnavn	Formål
	Pladsanvisningens fagsystem til varetagelse af pladsanvisning efter dagtilbudsloven. Behandling af personoplysninger sker med henblik på at registrere børns optagelse i dag-, fritids- og klubtilbud, herunder tilskud, fripladstilskud, egenbetaling, madordning, sikkerhed (tilskadekomst/erstatning), hygiejne, børnemiljøvurderinger samt sprogmiljøvurderinger

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

Databehandleren behandler personoplysningerne med henblik på opsætning, opbevaring, hosting, drift, support, samt vedligehold af produktet beskrevet i ovenstående tabel (A.1), for hvilket der er indgået aftale mellem den dataansvarlige og databehandler.

Personoplysninger importeres via systemer og eksporteres via de integrationer, der evt. er aftalt i Hovedaftalen og evt. tillæg.

Da der behandles større mængder af følsomme og fortrolige oplysninger primært om børn, er databehandleren forpligtiget til at etablere passende sikkerhedsforanstaltninger, som svarer til typen af behandlingen og i overensstemmelse med databeskyttelsesforordningens artikel 32. Instruks fremgår af bilag C.

Overførsler af personoplysninger til andre systemer

- Personoplysninger eksporteres via de integrationer, der evt. er aftalt i Hovedaftalen.
- Leverandøren skal vise en oversigt (flow) over, hvorledes datastrømmene er fra systemet og til systemet. Eksempelvis at der hentes oplysninger fra CPR og e-indkomst. Tilsvarende vises et flow for sammenhæng til andre systemer, som systemet sender persondata til.

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

Typer af personoplysninger	Borgere	Børn, umyndiggjorte eller andre sårbare datasubjekter	Medarbejdere	[Hvis relevant, angiv andre typer af registrerede]
Almindelige personoplysninger:	Identifikationsoplysninger, CPR-numre, familierelationer, sagsoplysninger, kontaktoplysninger (arbejdspladsinfo o.l.) samt løn og skatteoplysninger	Identifikationsoplysninger, CPR-numre, familierelationer, sagsoplysninger	Identifikationsoplysninger, CPR-numre, sagsoplysninger, ansættelsesforhold	
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.		**x**		
En fysisk persons seksuelle forhold eller seksuelle orientering				
Strafbare forhold (fx straffedomme, lovovertrædelser etc.)				
CPR-nr.	**x**	**x**	**x**	

Andre fortrolige oplysninger [Angiv hvilke fortrolige oplysninger. Eksempelvis: væsentlige sociale forhold, indtægts- og formueforhold, arbejds-, uddannelses- og ansættelsesmæssige forhold]	**x**	**x**		

A.4. Behandlingen omfatter følgende kategorier af registrerede

Se A.3

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

Er bestemt af Hovedaftalens aftalte periode.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING	DIREKTE UNDER-DATABEHANDLER	OVERFØRSELS-GRUNDLAG	SIKKERHEDSFOR-ANSTALTNINGER

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 underretning om planlagte ændringer vedrørende tilføjelse eller udskiftning samt godkendelse af underdatabehandlere, den dataansvarliges indsigelsesmulighed og behandling af sådan indsigelse

Databehandleren skal pr. e-mail eller anden skriftlig vis til kontaktpersonen/kontaktpunktet anført i Databehandleraftalens punkt 14 underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer.

En sådan underretning skal være den dataansvarlige i hænde minimum 3 måneder før anvendelsen eller ændringen skal træde i kraft.

Hvis den dataansvarlige har indsigelser mod ændringerne, skal den dataansvarlige give meddelelse herom til databehandleren inden 30 dage efter modtagelsen af underretningen.

Den dataansvarlige kan alene gøre indsigelse, hvis den dataansvarlige har rimelige, konkrete årsager hertil.

Hvis den dataansvarlige afgiver en rimelig og konkret indsigelse mod anvendelse af en underdatabehandler inden for den anførte frist, er databehandleren forpligtet til at tage indsigelsen i betragtning. Hvis databehandleren vælger ikke at imødekomme indsigelsen, eller hvis databehandleren ikke er i stand til at imødekomme indsigelsen inden for en rimelig frist, er den dataansvarlige berettiget til med 1 måneds skriftligt varsel at opsige den del af Hovedaftalen dækkende netop den ydelse, hvor underdatabehandleren ellers ville få adgang til persondata. Den øvrige del af Hovedaftalen løber fortsat i henhold til bestemmelserne i Hovedaftalen.

Ved antagelse af nye underdatabehandlere i Databehandleraftalens løbetid, skal databehandleren iagttage de aftalte vilkår i punkt C.5 om lokalitet for behandling samt punkt C.6 om instruks vedrørende overførsel af personoplysninger til tredjelande.

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 skal forestå opsætning, hosting, drift, support, vedligehold og videreudvikling af produkter på dagtilbudsområdet. Databehandleren stiller en løsning til rådighed for den dataansvarlige, der anvender løsningen som led i at yde lovpligtige ydelser til borgere på dagtilbudsområdet. Behandling af personoplysninger sker med henblik på at registrere børns optagelse i dag-, fritids- og klubtilbud, herunder tilskud, fripladstilskud, egenbetaling, madordning, sikkerhed (tilskadekomst/erstatning), hygiejne, børnemiljøvurderinger samt sprogmiljøvurderinger mv. I den forbindelse opbevarer databehandleren oplysninger og sørger for visning, back-up, fejlfinding og sammenstilling af den dataansvarliges data.

Dette bilag beskriver de generelle sikkerhedsforanstaltninger, som databehandleren skal implementere for løsningen.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Behandlingen omfatter persondata (herunder persondata omfattet af databeskyttelsesforordningens artikel 9 om "særlige kategorier af personoplysninger og strafbare forhold mv.) og der skal derfor etableres et højt sikkerhedsniveau.

Databehandleren skal løbende identificere og dokumentere risici gennem risikovurderinger og revisionserklæringer.

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:

- Have retningslinjer for styring af informationssikkerhed, herunder for intern organisering i relation roller og ansvarsområder mv. samt for mobilt udstyr og fjernarbejdspladser.

- Som led i informationssikkerheden have fokus på at teste, anskaffe, udvikle og vedligeholde de relevante systemer.

- Sørge for, at sikkerhedsforanstaltninger justeres løbende baseret på en risikovurdering, som indbefatter aktuelle trusler, den anvendte teknologiske platform samt organisatoriske forhold.

- Sørge for, at ansatte hos databehandleren, der er beskæftiget med behandling af personoplysninger under databehandleraftalen, er underlagt lovmæssig tavshedspligt i udførelsen af opgaver for offentlige myndigheder, jf. straffelovens §§ 152 og 152a. Alle ansatte hos databehandleren skal gøres opmærksom på denne tavshedspligt.

- Sørge for, at alene personale, som autoriseres hertil, har adgang til de personoplysninger, der behandles under databehandleraftalen. Såfremt det følger af databehandleraftalen, at særlige sikkerhedsgodkendelser er påkrævet for personale, der er beskæftiget med behandling af den dataansvarliges personoplysninger, skal databehandleren sikre, at disse godkendelser tilvejebringes.

- Sikre, at databehandlerens medarbejdere modtager tilstrækkelig uddannelse og instruktioner, samt at der udføres løbende sikkerheds bevidstheds aktiviteter for relevante medarbejder.

- Have restriktioner for fysisk adgang, således at områder, hvor der sker behandling af personoplysninger - hvad enten dette er manuelt eller elektronisk – ved adgangskontrolmekanismer adskilles fra områder, hvortil der er generel adgang. Sådanne adgangskontrolmekanismer kan eksempelvis omfatte systemer til fysisk adgangskontrol, låse, personsluser, sikkerhedspersonale og overvågningsudstyr.

- Have begrænsninger på adgangsrettigheder til personoplysninger og et system til adgangskontrol. Adgang til personoplysninger skal være begrænset til medarbejdere, og hvor det er relevant, andre leverandører, med et arbejdsbetinget behov og tildeles efter forudgående godkendelse fra databehandleren. Adgang skal tilbagekaldes, når brugeren ikke længere opfylder kriterierne for at have adgang. Databehandleren skal varetage autorisation for databehandlerens medarbejdere og - i det omfang det er særskilt aftalt i databehandleraftalen eller i Hovedaftalen - for den dataansvarliges medarbejdere.

- Sikre, at adgangsrettigheder gennemgås minimum halvårligt.

- Arbejde med styring af aktiver, herunder ansvar, klassifikation og mediehåndtering

- Anvender passende logiske autentifikationsmekanismer, eksempelvis adgangskoder, biometri eller lignende. De anvendte autentifikationsmekanismer skal leve op til, hvad der opfattes som god skik på området (eksempelvis krav til adgangskoders længde og kompleksitet).

- Have passende tekniske foranstaltninger til at begrænse risikoen for uautoriseret adgang og/eller installering af skadelig kode. Sådanne foranstaltninger kan omfatte firewalls, antivirus software og malware-beskyttelse. Databehandleren skal have formelle procedurer til sikring af, at sikkerhedssystemerne holdes opdaterede.

- Have fysisk sikring og miljøsikring

- Foretage registrering af afviste adgangsforsøg og blokering for yderligere forsøg efter et nærmere antal på hinanden følgende afviste adgangsforsøg på systemniveau.

- Have formelle procedurer for ændringshåndtering med henblik på at sikre, at enhver ændring er behørigt autoriseret, testet og godkendt inden implementering, samt at ændringer opholder, eller styrker, sikkerheden af databehandlingen. Proceduren skal understøttes af en effektiv funktionsadskillelse og/eller ledelsesopfølgning for at sikre, at ingen enkeltpersoner kan kontrollere en ændring alene.

- Anvende relevante krypteringsteknologier for at beskytte data, der opbevares og under transmission.

- Foretage logning af brug af personoplysninger.

- I det omfang, at det følger af Hovedaftalen, foranstalte, at systemer og data sikkerhedskopieres, samt at sikkerhedskopier opbevares betryggende og i overensstemmelse med det i databehandleraftalen anførte. Backup af data skal lagres på et andet fysisk sted, end der hvor de primære systemer til behandling af persondata er placeret.

- Sikre, at produktion og evt. test foregår i adskilte miljøer. Test miljøer skal gøre brug af pseudonymiserede og/eller fiktive data jf. de aktuelle retningslinjer for anonymisering fra datatilsynet.

- Have processer for håndtering af brud på datasikkerheden og formaliserede processer for at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en teknisk eller fysisk hændelse. Disse processer skal afprøves og justeres men jævne mellemrum.

- Med jævne mellemrum udføre tekniske test af sikkerheden af systemer til behandling af persondata med henblik på at afdække svagheder og styrke risikovurderinger.

- Sikre, at behandlingen foregår i overensstemmelse med lovkrav

- Sikre, at der sker sletning af data, inden udstyr overgives til tredjepart eller i øvrigt bortskaffes. Databehandleren skal kunne dokumentere fremgangsmåden herfor.

- Sikre, at der kun etableres eksterne IT-kommunikationsforbindelser, hvis dataforbindelsen er krypteret. Der skal anvendes 2-faktor-autentifikation. Arbejdsstationer, som anvendes til fjernadgang, skal være opdateret med nyeste patch og være beskyttet af en opdateret EndPointProtection applikation.

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:

Bistand til overholdelse af de registreredes rettigheder

Løsningerne er nærmere beskrevet i Hovedaftalen.

Underretning af den dataansvarlige om anmodninger fra den registrerede

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

Bistand ved sikkerhedsbrud

Databehandler bistår den dataansvarlige i tilfælde af sikkerhedsbrud. Databehandler skal indsamle og dokumentere informationer om sikkerhedshændelser hos databehandler og underdatabehandlere, og underrette den dataansvarlige om sikkerhedsbrud, uden unødig forsinkelse og senest indenfor det antal timer som fremgår af punkt 9.2.

Databehandleren skal indberette sikkerhedsbrud og i den forbindelse sikre, at Indberettede oplysninger har et omfang og en detaljeringsgrad, som den dataansvarlige i det konkrete tilfælde finder tilstrækkeligt. Databehandler oplyser så vidt muligt følgende indenfor den angivne tidsramme i punkt 9.2.

Indberetningsoplysninger sendes til den dataansvarliges e-mail for sikkerhedsbrud, der er angivet i punkt 14.

Databehandlerens omkostninger ved bistand til den dataansvarlige

Databehandlerens bistand til den dataansvarlige er lovpligtig, jf. art. 28 stk. 3 litra e og f, og dermed påregnelig. Ovenstående og lignende ydelser honoreres ikke.

C.4 Opbevaringsperiode/sletterutine
Hvor ikke andet er aftalt, skal databehandleren opbevare de personoplysninger som databehandleren behandler på den Dataansvarliges vegne, hos databehandlerren, indtil den dataansvarlige anmoder om at få oplysningerne tilbageleveret og/eller slettet.

Ved udfasning/kassation af udstyr skal databehandleren sikre at oplysninger er slettet med et anerkendt sletteværktøj.

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:

Der henvises til bilag B.1.2.

I de tilfælde, hvor personoplysninger efter aftale med den dataansvarlige, jf. bilag C.6., behandles i ikke-sikre tredjelande, skal disse lokaliteter særligt fremhæves. Ligeledes skal databehandlere, der er koncernforbundne med moderselskaber i ikke sikre tredjelande særligt fremhæves, og det pågældende lands nationale hjemmel til mulige udleveringskrav angives.

Databehandler skal løbende vedligeholde overblikket og udtrykkeligt meddele den dataansvarlige, hvis der sker ændringer dels i lokaliteten for behandlingen dels i databehandlerens koncernkonstruktioner.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande
Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsel af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler. Instruksen omfatter også forbud mod at anvende underdatabehandlere i EU, EØS eller tredjelande, der opfylder EU-kommissionens tilstrækkelighedsvurdering, når disse er koncernforbundne med moderselskaber i ikke-sikre tredjelande.

Såfremt databehandler, på baggrund af en konkret, forudgående udtrykkelig og skriftlig aftale med den dataansvarlige, overfører personoplysninger til et tredjeland, må disse oplysninger alene:

Enten overføres til lande, der efter EU-Kommissionens tilstrækkelighedsvurdering, jf. art. 45, er erklærede sikre. Se EU-Kommissionens liste over de til enhver tid værende sikre tredjelande: Adequacy decisions | Europa-Kommissionen. Databehandleren er ansvarlig for løbende af følge op på landets status og straks orientere den dataansvarlige, hvis tilstrækkelighedsvurderingen ikke kan fastholdes samt træffe foranstaltninger til at sikre persondata overført til behandling i EU, EØS eller andet sikkert tredje land.

Eller have et til enhver tid værende gyldigt overførselsgrundlag som dokumenteres i tabellen under bilag C.5. Databehandleren skal overfor den dataansvarlige dokumentere beslutningsgrundlag, overvejelser og konklusioner samt foranstaltninger i overensstemmelse med EDPB's "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Versions 2.0. Adopted on 18.06.2021" punkt 43 samt 43.1-43.3

Databehandleren og dennes underdatabehandlere skal anfægte enhver anmodning om videregivelse af data fra et hvilket som helst lands myndigheder og er hver især selvstændig ansvarlige for straks at underrette den dataansvarlige om anmodningen. Begge skal endvidere informere om hvorvidt de, trods anfægtelsen, har imødekommet anmodningen. Såfremt databehandleren eller underdatabehandlere er bundet af det pågældende lands lovgivning om tavshedspligt, skal de pågældende i stedet straks oplyse den dataansvarlige om, at de misligholder nærværende aftale. En sådan misligholdelse er at betragte som væsentlig. Misligholdelsesbeføjelser er reguleret i Hovedaftalen.

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

Den dataansvarlige har anvendt Datatilsynets 'Vejledning om tilsyn med databehandlere - Pointskala og seks tilsynskoncepter' fra oktober 2021, ved afgørelse om, hvilken tilsynsform der skal anvendes ved tilsyn med databehandleren.

Ved vurdering af hvilken tilsynsform der skal anvendes, har den dataansvarlige vurderet fire aspekter ved den databehandling der overlades til databehandleren, se side 6-11 i Datatilsynets 'Vejledning om tilsyn med databehandlere - Pointskala og seks tilsynskoncepter' fra oktober 2021.

Den dataansvarlige har valgt:

Tilsynskoncept 5

En uafhængig tredjepart fører et dokumenteret tilsyn med databehandleren, som dækker over databehandleraftalens behandlingsaktiviteter. Det dokumenterede tilsyn udarbejdes som en revisionserklæring fx ISAE 3000 type II.

Databehandleren indhenter for egen regning revisionserklæringen

Databehandleren fremsender årligt al relevant tilsynsmateriale til Det fælleskommunale Databehandlersekretariat, e-mail: dbsinfo@kommunedbs.dk med kopi til den dataansvarlige via kontaktpersonen, angivet i pkt. 14. Såfremt Det fælleskommunale Databehandlersekretariat (DBS) giver

besked til databehandleren om, at DBS ikke fører tilsyn med systemet, skal tilsynsmateriale fremsendes til den dataansvarlige via kontaktpersonen, angivet i pkt. 14.

Dækker revisionserklæringen ikke alle krav, der er beskrevet i databehandleraftalen, kan den dataansvarlige eller en repræsentant for den dataansvarlige foretage skriftlig inspektion, eksempelvis i form af spørgeskema, af databehandlerens behandling af personoplysninger, med henblik på at fastslå databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og denne aftale.

Den dataansvarliges eventuelle udgifter i forbindelse hermed er reguleret i Hovedaftalen.

Den dataansvarlige forbeholder sig retten til at eskalere sit tilsyn med databehandleren i overensstemmelse med tilsynskoncept 6, såfremt den dataansvarlige via informationer i pressen, tilsynsrapporter eller egne erfaringer med sikkerhedsbrud, evt. får indtryk af problemer hos databehandleren.

Hvis den dataansvarlige vælger at eskalere sin tilsynsform med databehandleren til et andet tilsynskoncept, efter tilsynskoncept 6, skal rammerne for tilsynet udarbejdes som et tillæg til den eksisterende databehandleraftale.

C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere
Databehandleren eller en repræsentant for databehandleren foretager tilsyn med underdatabehandlere. Databehandleren baserer sit valg af tilsynsform og hyppighed af tilsyn på en risikovurdering.

Tilsyn kan f.eks. ske ved skriftlig informationsindsamling eller i form af en fysisk inspektion af lokaliteterne, hvorfra underdatabehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen, med henblik på at fastslå underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse bestemmelser.

Ud over det planlagte tilsyn, skal databehandleren gennemføre en inspektion, fx i form af skriftlig informationsindsamling eller fysisk besøg, med underdatabehandleren, når databehandleren eller den dataansvarlige finder det nødvendigt.

Såfremt underdatabehandleren får udarbejdet en årlig revisionserklæring fra en uafhængig tredjepart angående underdatabehandlerens overholdelse af denne databehandleraftale og de heri aftalte tekniske og organisatoriske sikkerhedsforanstaltninger, skal databehandleren modtage kopi heraf. Databehandleren gennemgår revisionserklæringen og følger op på eventuelle forhold, der giver anledning til yderligere undersøgelser.

Databehandleren dokumenterer afholdte tilsyn. Dokumentation for afholdte tilsyn skal fremlægges i en tilsynsrapport indeholdende beskrivelse af scope, væsentlige findings og plan for eventuelle mitigerende foranstaltninger. Den dataansvarliges adgang hertil er reguleret i kontrakten.

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

Den dataansvarlige kan – hvis det findes nødvendigt – vælge at initiere og deltage på en fysisk inspektion hos underdatabehandleren. Dette kan blive aktuelt, hvis den dataansvarlige vurderer, at databehandlerens inspektion hos underdatabehandleren ikke har givet den dataansvarlige tilstrækkelig sikkerhed for, at behandlingen hos underdatabehandleren sker i overensstemmelse med databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse bestemmelser. Sådan inspektion gennemføres for den dataansvarliges egen regning, efter forudgående aftale med databehandleren/underdatabehandleren og normalt med et skriftligt varsel på mindst 10 arbejdsdage til databehandleren/underdatabehandleren.

Besigtigelse af underdatabehandlerens lokationer sker under overholdelse af underdatabehandlerens krav til sikkerhed og fortrolighed, uanset om besigtigelse foretages af den dataansvarlige selv eller tredjepart. Underdatabehandleren må alene nægte godkendelse af brug af tredjepart af saglige årsager, herunder men ikke begrænset til, at tredjeparten er en konkurrent. Databehandleren skal oplyse den dataansvarlige, om eventuel godtgørelse til underdatabehandleren for tidsforbrug på tilsynet.

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

I tilfælde af at tilsynsmyndigheder, såsom Datatilsynet, ønsker at foretage inspektion hos underdatabehandleren med henblik på at undersøge underdatabehandlerens forhold, afholder databehandler eller underdatabehandleren egen tid og egne omkostninger forbundet hermed. I tilfælde af at tilsynsmyndigheder, såsom Datatilsynet, ønsker at foretage inspektion hos underdatabehandleren i forbindelse med tilsyn med en dataansvarlig, godtgør den dataansvarlige underdatabehandlerens tid og rimelige omkostninger forbundet med tilsynet, medmindre tilsynet hovedsageligt er foranlediget af underdatabehandlerens manglende efterlevelse af sine forpligtelser som underdatabehandler i henhold til databeskyttelsesforordningen.