**Databehandleraftale vedrørende [SYSTEMNAVN]:**

skabelon for et orange system

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

mellem

Aabenraa Kommune

CVR 28189854

Skelbækvej 2

6200 Aabenraa

herefter ”den dataansvarlige”

og

[NAVN PÅ SYSTEM/PRODUKT/AKTIVITET]

[NAVN PÅ LEVERANDØR]

CVR

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

[2. Præambel 3](#_Toc58338061)

[3. Den dataansvarliges rettigheder og forpligtelser 3](#_Toc58338062)

[4. Databehandleren handler efter instruks 4](#_Toc58338063)

[5. Fortrolighed 4](#_Toc58338064)

[6. Behandlingssikkerhed 4](#_Toc58338065)

[7. Anvendelse af underdatabehandlere 5](#_Toc58338066)

[8. Overførsel til tredjelande eller internationale organisationer 6](#_Toc58338067)

[9. Bistand til den dataansvarlige 7](#_Toc58338068)

[10. Underretning om brud på persondatasikkerheden 8](#_Toc58338069)

[11. Sletning og returnering af oplysninger 8](#_Toc58338070)

[12. Revision, herunder inspektion 9](#_Toc58338071)

[13. Parternes aftale om andre forhold 9](#_Toc58338072)

[14. Ikrafttræden og ophør 9](#_Toc58338073)

[15. Kontaktpersoner hos den dataansvarlige og databehandleren 10](#_Toc58338074)

[Bilag A Oplysninger om behandlingen 11](#_Toc58338075)

[Bilag B Underdatabehandlere 13](#_Toc58338076)

[Bilag C Instruks vedrørende behandling af personoplysninger 14](#_Toc58338077)

[Bilag D Parternes regulering af andre forhold 22](#_Toc58338078)

# 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 [xx-system/xx-aktivitet] 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.

# 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]](#footnote-2) nationale ret og disse Bestemmelser.
2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.
3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

# Databehandleren handler efter instruks

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

# Fortrolighed

1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.
2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

# Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

* 1. Pseudonymisering og kryptering af personoplysninger
	2. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
	3. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
	4. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.
1. 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.
2. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

# Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).
2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående 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.

1. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.
2. Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.
3. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

# Overførsel til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.
2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.
3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:
	1. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
	2. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
	3. 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.

# Bistand til den dataansvarlige

1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III.

Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

* 1. oplysningspligten ved indsamling af personoplysninger hos den registrerede
	2. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
	3. indsigtsretten
	4. retten til berigtigelse
	5. retten til sletning (”retten til at blive glemt”)
	6. retten til begrænsning af behandling
	7. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
	8. retten til dataportabilitet
	9. retten til indsigelse
	10. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering
1. 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:
2. 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
3. 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
4. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)
5. 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.
6. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

# Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.
2. Databehandlerens underretning til den dataansvarlige skal om muligt ske uden unødigt ophold og senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.
3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:
	1. 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
	2. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
	3. 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.

# Sletning og returnering af oplysninger

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

# Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.
2. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmeret angivet i Bilag C.7. og C.8.
3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

# Parternes aftale om andre forhold

1. Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

# Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.
2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.
3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.
4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.
5. Underskrift

På vegne af den dataansvarlige

Navn

Stilling

Telefonnummer

E-mail

Underskrift

På vegne af databehandleren

Navn

Stilling

Telefonnummer

E-mail

Underskrift

# Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.
2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

**Dataansvarlige – skal udfyldes af Aabenraa Kommune**

Navn

Stilling

Telefonnummer

E-mail

**Databehandler/leverandør – skal udfyldes af leverandør**

Navn

Stilling

Telefonnummer

E-mail

# Bilag A Oplysninger om behandlingen

[BEMÆRK: I TILFÆLDE AF FLERE BEHANDLINGSAKTIVITETER, SKAL DISSE OPLYSNINGER FREMGÅ FOR HVER ENKELT BEHANDLINGSAKTIVITET. Hvis I er i tvivl om, hvorvidt der er flere, kan I eventuelt tilgå jeres fortegnelser, eller spørge databehandler. Hvis der ikke e r flere behandlingsaktiviteter, skal dette afsnit slettes.]

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

[BESKRIV FORMÅLET MED BEHANDLINGEN]

Eksempelvis:

”er, at den dataansvarlige kan anvende systemet X, som ejes og administreres af databehandleren, til at indsamle og behandle oplysninger om den dataansvarliges medlemmer”.

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

[BESKRIV KARAKTEREN AF BEHANDLINGEN]

Eksempelvis:

”at databehandleren stiller systemet X til rådighed for den dataansvarlige og herigennem opbevarer personoplysninger om den dataansvarliges medlemmer på virksomhedens servere.”

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

[BESKRIV TYPEN AF PERSONOPLYSNINGER DER BEHANDLES]

[EKSEMPELVIS]

”Navn, e-mailadresse, telefonnummer, adresse, personnummer, betalingskortoplysninger, væsentlige sociale forhold, CPR.nr., uddannelse, fotos m.m.”

[BEMÆRK: BESKRIVELSEN BØR VÆRE SÅ SPECIFIK SOM MULIGT, OG UNDER ALLE OMSTÆNDIGHEDER, SKAL TYPEN AF PERSONOPLYSNINGER PRÆCISERES YDERLIGERE END BLOT ”PERSONOPLYSNINGER”.]

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

[BESKRIV KATEGORIERNE AF REGISTREREDE. I KAN TILGÅ JERES FORTEGNELSER OG SE; HVILKE KATEGORIER AF REGISTREREDE, I ARBEJDER MED]

Eksempelvis:

* + - Frivillige
		- Pårørende
		- Afdøde
		- Børn og unge under 18
		- Frivillige
		- Leverandører
		- M.m.

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

[BESKRIV VARIGHEDEN AF BEHANDLINGEN]

Eksempelvis:

”Behandlingen er ikke tidsbegrænset og varer indtil aftalen opsiges eller ophæves af en af parterne”.

# Bilag B Underdatabehandlere

**B.1. Godkendte underdatabehandlere**

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere.

| 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**

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).

Underretningen sendes til databehandlerens kontaktperson hos den dataansvarlige og til kommunens DPO.

# 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:

[BESKRIV BEHANDLINGEN, SOM DATABEHANDLEREN INSTRUERES I AT FORETAGE. SOM OFTEST KAN INSPIRATION FINDES I HOVEDAFTALEN]

**C.2. Behandlingssikkerhed**

Sikkerhedsniveauet skal afspejle følgende risikovurdering:



 = Børn, unge og sårbare personer nyder en særlig beskyttelse inden for databeskyttelsesretten, da de oftest er mindre bevidste om de risici og konsekvenser, som kan være forbundet med en behandling af deres personoplysninger.

Risikoen for behandling af personoplysninger om børn, unge og sårbare personer vurderes derfor som højere (gul farve).

Grøn = Lavrisikosystem

Gul = Middelrisikosystem

Orange = middelhøjrisikosystem

Rød = Højrisikosystem

[HER SKAL VURDERINGEN AF SYSTEMET SKRIVES IND – BESKRIV HVOR I FIGUREN SYSTEMET HØRER TIL VED EKSEMPELVIS AT BESKRIVE ANTAL PERSONER; SOM BEHANDLES OG DE PERSONOPLYSNINGER SOM BEHANDLES.

DETTE ER EKSEMPELVIS NØDVENDIGT AT AFKLARE, FØR DET KAN BESLUTTES HVILKE SIKKERHEDSFORANSTALTNINGER, DER SKAL IVÆRKSÆTTES, ELLER HVORDAN TILSYN SKAL FØRES.]

[EKSEMPELVIS]

”BEHANDLINGEN OMFATTER EN STØRRE MÆNGDE ALMINDELIGE PERSONOPLYSNINGER, OG SYSTEMET ARBEJDER MED 750 REGISTREREDE.

DERFOR VURDERES SYSTEMET TIL AT VÆRE ET LAVRISIKOSYSTEM. HVORFOR DER ETABLERES ET ”LAVT” SIKKERHEDSNIVEAU.

NÆSTE AFSNIT REDEGØRER FOR DE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER, DATABEHANDLER SOM MINIMUN SKAL GENNEMFØRE.]

**Krav til sikkerhedsforanstaltninger**

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:

1. **Risikostyring**
	1. Databehandleren skal tage de nødvendige skridt til at identificere, vurdere og begrænse enhver, med rimelighed forudsigelig, intern og ekstern risiko for tilgængeligheden, fortroligheden, og/eller integriteten af alle personoplysninger omfattet af Databehandleraftalen.
	2. Databehandleren skal have passende tekniske foranstaltninger til at begrænse risikoen for enhver uautoriseret adgang. Databehandleren skal evaluere og forbedre effektiviteten af sådanne forholdsregler, når det er nødvendigt.
	3. Databehandleren skal dokumentere de identificerede risici og hvordan risikoen er nedbragt til et acceptabelt niveau. Ovenstående forpligtelse indebærer, at databehandleren skal foretage en risikovurdering, og herefter gennemføre foranstaltninger for at imødegå identificerede risici. Der kan herunder bl.a., alt efter hvad der er relevant, være tale om følgende foranstaltninger:
	4. Pseudonymisering og kryptering af personoplysninger
	5. Evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og – tjenester
	6. Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
	7. En procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed
	8. Databehandleren skal have formelle procedurer for håndtering af sikkerhedshændelser.
2. **Autorisation og adgangskontrol**
	1. Autorisationer skal angive, i hvilket omfang brugeren må forespørge, inddatere eller slette personoplysninger.
	2. Kun de personer som autoriseres dertil, må have adgang til de personoplysninger, der behandles i henhold til Databehandleraftalen. Kun de personer, der har et arbejdsbetinget behov for at behandle personoplysningerne, må autoriseres.
	3. Der må desuden autoriseres personer, for hvem adgang til personoplysningerne er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.
	4. Databehandleren skal kunne dokumentere hvilke medarbejdere der har autorisation til at tilgå personoplysninger, der behandles i henhold til Databehandleraftalen.
	5. Den autoriserede bruger udstyres med en personlig brugeridentifikation og et personligt password, der skal anvendes hver gang, brugerne får adgang til databehandlingen. Passwords skal som minimum skiftes hvert halve år. Passwords skal have en tilstrækkelig længde og kompleksitet.
	6. Databehandleren skal træffe foranstaltninger til at sikre, at kun autoriserede brugere kan få adgang til de personoplysninger, som den pågældende er autoriseret til.
	7. Databehandleren skal have rimelige restriktioner for fysisk adgang. Områder hvor der sker behandling af personoplysninger i henhold til Hovedaftalen, skal være effektivt adskilt fra områder, hvortil der er generel adgang.
	8. Databehandleren skal have formelle procedurer for håndtering af nulstilling af adgangskoder og for andre situationer, hvor den normale logiske adgangskontrol sættes ud af kraft.
	9. Der skal løbende og mindst en gang hvert halve år foretages kontrol af, om brugerne er tildelt de adgange og autorisationer, som de bør have. Denne kontrol kan f.eks. indebære, at der i systemerne dannes en statistik over den enkelte brugers anvendelse af systemet, så det kan konstateres, om udstedte adgange og autorisationer fortsat anvendes.
	10. Databehandleren skal uden unødig forsinkelse inddrage autorisationer og adgange for brugere, der efter en konkret vurdering ikke længere bør have disse.
3. **Uddannelse og instruktion**
	1. Databehandleren skal sørge for, at dennes medarbejdere modtager den tilstrækkelige uddannelse og instruktioner for at sikre, at personoplysninger behandles i overensstemmelse med relevant lovgivning samt Databehandlerens og den Dataansvarliges politikker og procedurer herfor.
4. **Kontrol med afviste adgangsforsøg og logning**
	1. Der skal foretages registrering af alle afviste adgangsforsøg. Hvis der inden for en fastsat periode er registreret højst 3 på hinanden følgende afviste adgangsforsøg med samme brugeridentifikation, skal der blokeres for yderligere forsøg fra denne brugeridentifikation. Adgangen åbnes først, når årsagen til afviste adgangsforsøg er klarlagt.
	2. Der skal foretages maskinel registrering (logning) ved al behandling af personhenførbare oplysninger. Loggen skal mindst indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte eller det anvendte søgekriterium. Loggen skal opbevares i seks måneder, hvorefter den skal slettes, medmindre der i overensstemmelse med loggens formål fastsættes en længere opbevaringsperiode, af hensyn til at kunne anvende den som værktøj til brug ved efterforskning.
5. **Inddata- og uddatamateriale**
	1. Inddatamateriale og uddatamateriale skal opbevares på en sådan måde, at uvedkommende ikke kan gøre sig bekendt med de personoplysninger, der er indeholdt heri.
	2. Inddatamateriale og uddatamateriale må kun anvendes af personer, som er beskæftiget med inddateringen og behandling af data, samt i forbindelse med revision, teknisk vedligeholdelse, driftsovervågning og fejlretning mv.
6. **Mobile lagringsenheder**
	1. Mobile lagringsmedier med personoplysninger skal være mærket, og skal opbevares med en tilstrækkelig stærk kryptering og under opsyn eller under lås, når de ikke benyttes.
	2. Mobile lagringsmedier med personoplysninger må kun udleveres til autoriserede personer med henblik på revision eller drifts- og systemtekniske opgaver.
	3. Der skal føres en fortegnelse over hvilke mobile lagringsmedier, der benyttes i forbindelse med databehandlingen.
	4. Der skal udarbejdes skriftlige instrukser for anvendelse og opbevaring af mobile lagringsmedier.
	5. I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, samt ved salg og kassation af anvendte datamedier skal der træffes fornødne foranstaltninger for at sikre, at personoplysningerne ikke hændeligt eller bevidst tilintetgøres, fortabes eller forringes eller, at personoplysningerne kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med gældende lov. Dette skal ske efter best practice.
7. **Sikkerhedskopier**
	1. Der gælder de samme retningslinjer for sikkerhedskopier som for al anden behandling af personoplysninger i medfør af denne aftale.
	2. Databehandleren skal sikre, at systemer og personoplysninger sikkerhedskopieres regelmæssigt.
	3. Sikkerhedskopier skal opbevares adskilt fra serveren i et ikke tilstødende rum for at sikre, at disse ikke går tabt f.eks. som følge af brand eller oversvømmelse. Opbevaring af sikkerhedskopier skal altid ske på betryggende vis så de ikke fortabes.
	4. Databehandleren skal regelmæssigt kontrollere, at sikkerhedskopier er læsbare. Dette skal blandt andet gøres ud fra et beredskabssynspunkt, f.eks. ved større ændringer af et systems tekniske setup.
8. **Opdatering og ændringer**
	1. Databehandleren skal have formelle procedurer til sikring af, at opdateringer til operativsystemer, databaser, applikationer og anden software bliver vurderet og implementeret inden for rimelig tid.
	2. Databehandleren skal have formelle procedurer for ændringshåndtering med henblik på at sikre, at enhver ændring er behørigt autoriseret, testet og godkendt inden implementering. Proceduren skal understøttes af en effektiv funktionsadskillelse eller ledelsesopfølgning med henblik på at sikre, at ingen enkeltpersoner kan implementere en ændring alene.
9. **Driftsafbrydelser**
	1. Databehandleren skal have dokumenterede beredskabsprocedurer, der sikrer genetablering af services inden for rimelig tid i tilfælde af driftsafbrydelser.
10. **Bortskaffelse af udstyr**
	1. Databehandleren skal have formelle processer i overensstemmelse med best practice og den Dataansvarliges krav med henblik på at sikre, at der sker effektiv sletning af personoplysninger inden bortskaffelse af elektronisk udstyr.
	2. Ved bortskaffelse af udstyr skal Databehandleren dokumentere fremgangsmåden herfor, og kunne forevise denne dokumentation efter anmodning herom.
11. **Tilsyn**
	1. Databehandleren skal føre og dokumentere et tilsyn med Databehandlerens organisations overholdelse af lovkrav, politikker, procedurer og denne Databehandleraftale med bilag.
12. **Fjernadgang**
	1. Der må kun etableres eksterne IT-kommunikationsforbindelser, hvis dataforbindelsen er krypteret.
	2. Der skal anvendes 2-faktor-autentifikation. Autentifikationsmetoden kan f.eks. være MitID, medarbejdersignatur, SMS-token, Rfid eller lignende.
	3. Arbejdsstationen, som anvendes til fjernadgang, skal være opdateret med nyeste patch og være beskyttet af en opdateret EndPointProtection applikation.
13. **Underretning og assistance**
	1. Ved brud på persondatasikkerheden skal den Dataansvarlige uden unødig forsinkelse og skriftligt orienteres på nedenstående adresse, således at den Dataansvarlige kan indberette bruddet til Datatilsynet og om nødvendigt underrette de registrerede. Underretningen skal ske til Aabenraa Kommunes DPO.

**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:

Leverandøren skal på opfordring fra Kommunen hjælpe med at opfylde Kommunens forpligtelser i forhold til den registreredes rettigheder, herunder besvarelse af anmodninger fra borgere om indsigt i egne oplysninger, udlevering af borgerens oplysninger, rettelse og sletning af oplysninger, begrænsning af behandling af borgerens oplysninger, samt Kommunens forpligtelser i forhold til underretning af den registrerede ved brud på persondatasikkerheden, i medfør af databeskyttelsesforordningens kap. III samt artikel 34.

Leverandøren skal således være i stand til at udtrække, ændre og slette personoplysninger efter anmodning fra Kommunen med henblik på opfyldelse af Aabenraa Kommunens forpligtelser i forhold til den registreredes rettigheder, jf. databeskyttelsesforordningens kap. III. Leverandøren skal desuden på anmodning fra Kommunen ændre en evt. formulering til opfyldelse af Kommunens oplysningspligt overfor den registrerede, jf. artikel 13 og 14.

Hvis der sker brud på persondatasikkerheden, skal leverandøren være i stand til at udlevere oplysninger om de berørte registrerede, der gør det muligt for Aabenraa Kommune at underrette disse i overensstemmelse med artikel 34.

**C.4 Opbevaringsperiode/sletterutine**

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 følgende:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Virksomhedens navn og adresse** | **CVR** | **Lokalitet for behandling** | **Type oplysninger** | **Overførselsgrundlag** |
|  |  |  |  |  |
|  |  |  |  |  |

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

Hvis leverandøren overfører til tredjelande, skal Leverandøren enten overføre til sikre tredjelande, jf. Datatilsynets opdaterede liste over sikre tredjelande på deres hjemmeside.

* eller have et gyldigt overførselsgrundlag som dokumenteres i tabellen under C.5

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**

Databehandleren skal én gang årligt vederlagsfrit til Aabenraa Kommune fremsende en erklæring om overholdelse af denne Aftale. Erklæringen skal udarbejdes af en uvildig tredjepart og være af typen ***ISAE 3000***, eller tilsvarende, og skal omfatte både Leverandørens og eventuelle underdatabehandleres databehandling. Den første erklæring skal foreligge 12 måneder efter Hovedaftalens indgåelse.

I tilfælde af, at Kommunen og/eller relevante offentlige myndigheder, særligt Datatilsynet, ønsker at foretage en inspektion af de ovennævnte foranstaltninger i henhold til denne aftale, forpligter databehandleren og databehandlerens underleverandører sig til uden yderligere omkostninger for Aabenraa Kommune at stille tid og ressourcer til rådighed herfor.

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

Databehandleren skal én gang årligt for egen, eller underdatabehandlers regning, indhente en revisionserklæring vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende typer af erklæring, eller tilsvarende, kan anvendes i overensstemmelse med disse bestemmelser:

Ved behandling af personoplysninger, som Aabenraa Kommunes er dataansvarlig for, anvendes følgende erklæring:

* ISAE 3000 eller tilsvarende

Ved hosting eller infrastrukturydelser (gateways mv.) skal nedenstående erklæring anvendes i stedet:

* ISAE 3402 eller tilsvarende

Revisionserklæring jf. pkt. C.7, og C.8, sammen med dokumentation for gennemført tilsyn (gennemgang og vurdering) af revisionserklærings indhold, skal leveres til den dataansvarlige samtidigt, uden unødig forsinkelse inden for 12 måneder af kontraktindgåelsen.

Baseret på resultaterne af revisionserklæringen 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

Parternes erstatningsansvar, der relaterer sig til Bestemmelserne, skal afgøres efter dansk rets almindelige regler. Parternes erstatningsansvar i forhold til de registrerede skal reguleres af databeskyttelsesforordningens artikel 82.

Eventuelle klausuler om ansvarsbegrænsning, erstatning eller skadesløsholdelse, der følger af andre aftaler mellem parterne, herunder hovedaftalen for leveringen af den af disse Bestemmelser omfattede ydelse, finder ikke anvendelse i relation til disse Bestemmelser.

1. Henvisninger til ”medlemsstat” i disse bestemmelse skal forstås som en henvisning til ”EØS medlemsstater”. [↑](#footnote-ref-2)