

Changelog

VERSION	ÆNDRINGER
1.1	Ændringer i Bestemmelserne 7.7., 9.2., 10.4. og Bilag C.8. (<i>Tastefejl og opdaterede krydshenvisninger</i>).
1.2.	Syddjurs Kommune har tilføjet og nummeret underafsnit i Bilag C.2. og C.3.
1.3.	Registreret på forsiden, at aftalens bestemmelser har forrang før alle øvrige bestemmelser i aftaler, der er indgået eller bliver indgået med leverandøren
1.4.	Præudfyldt behandlingsinstruks i Bilag C.1.
1.5.	Prædefinering af registrerede tilføjet i tabel i bilag A.3. og A.4.
1.6.	Præcisering i punkt A.5.

Denne aftales bestemmelser har forrang i forhold til alle øvrige bestemmelser i aftaler, som er eller bliver indgået med databehandleren

AFTALE

Standardkontraktbestemmelser

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

mellem

NAVN
CVR
ADRESSE
POSTNR OG BY
LAND

herefter "den dataansvarlige"

og

NAVN
CVR
ADRESSE
POSTNR OG BY
LAND[NAVN]
[CVR-NR][ADRESSE]
[POSTNUMMER OG BY]
[LAND]

herefter "databehandleren"

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

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

1. Indhold

1. Indhold.....	3
2. Præambel	4
3. Den dataansvarliges rettigheder og forpligtelser	4
4. Databehandleren handler efter instruks	5
5. Fortrolighed	5
6. Behandlingssikkerhed	5
7. Anvendelse af underdatabehandlere.....	6
8. Overførsel til tredjelande eller internationale organisationer	7
9. Bistand til den dataansvarlige.....	8
10. Underretning om brud på persondatasikkerheden	9
11. Sletning og returnering af oplysninger	10
12. Revision, herunder inspektion	10
13. Parternes aftale om andre forhold	10
14. Ikrafttræden og ophør.....	11
15. Kontaktpersoner hos den dataansvarlige og databehandleren	12
Bilag A Oplysninger om behandlingen	13
Bilag B Underdatabehandlere	15
Bilag C Instruks vedrørende behandling af personoplysninger.....	16
Bilag D Parternes regulering af andre forhold.....	25

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 [TJENESTE] 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 er 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 medlemsstaternes¹ 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.

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.

Konsekvensen af en potentiel ulovlig instruks fremgår af punkt D.2.

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

¹ Henvvisninger til "medlemsstat" i disse bestemmelser skal forstås som en henvisning til "EØS medlemsstater".

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 **specifik skriftlig godkendelse** fra den dataansvarlige.

3. Databehandleren må kun gøre brug af underdatabehandlere med den dataansvarliges forudgående specifikke skriftlige godkendelse. Databehandleren skal indgive anmodningen om en specifik godkendelse mindst **120 dage** inden anvendelsen af den pågældende underdatabehandler. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.
4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.
6. Databehandleren skal i sin aftale med underdatabehandleren indføre 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.5.
5. Disse Bestemmelser skal ikke forveksles med standardkontraktbestemmelser 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. indsigtretten
- 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:
 1. den dataansvarliges forpligtelse til uden unødigt 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
 2. den dataansvarliges forpligtelse til uden unødigt forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder
 3. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)
 4. 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 unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.
2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest **24 timer** efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.
3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:
 - a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger

- b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
 - c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.
4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at **tilbagelevere alle personoplysningerne og slette eksisterende kopier**, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.
2. Følgende regler i EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne efter ophør af tjenesterne vedrørende behandling af personoplysninger:

-

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. Procedurene for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.6. og C.7.
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

[BEMÆRK: I TILFÆLDE AF FLERE BEHANDLINGSAKTIVITETER, SKAL DISSE OPLYSNINGER FREMGÅ FOR HVER ENKELT BEHANDLINGSAKTIVITET]

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

[BESKRIV FORMÅLET MED BEHANDLINGEN]

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

[BESKRIV KARAKTEREN AF BEHANDLINGEN]

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

I tabellen er dels ved beskrivelse dels ved afkrydsning angivet hvilke registrerede, der behandles personoplysninger om samt hvilke typer af personoplysninger, der behandles om de respektive typer af registrerede. Se Databeskyttelsesforordningens art. 6, 9 og 10 samt Databeskyttelsesloven § 11 f.s.v.a. typer af personoplysninger og nedenstående pkt. A.4. f.s.v.a. typen af registrerede.

Typer af personoplysninger	Registrerede		
	Borgere	Umyndige borgere	Ansatte af kommunen
	[BESKRIV TYPEN AF ALMINDELIGE PERSONOPLYSNINGER DER BEHANDLES, F.EKS. NAVN, TELEFONNUMMER, E-MAIL, ADRESSE ETC]	[BESKRIV TYPEN AF ALMINDELIGE PERSONOPLYSNINGER DER BEHANDLES, F.EKS. NAVN, TELEFONNUMMER, E-MAIL, ADRESSE ETC]	[BESKRIV TYPEN AF ALMINDELIGE PERSONOPLYSNINGER DER BEHANDLES, F.EKS. NAVN, TELEFONNUMMER, E-MAIL, ADRESSE ETC]
Almindelige og fortrolige oplysninger			
CPR nr.			
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 ori- entering			
Straffedomme			
Lovovertrædelse			

A.4. Behandlingen omfatter følgende kategorier af registrerede

Syddjurs Kommune sonderer mellem 3 kategorier af registrerede:

1. Myndige borgere
2. Umyndige borgere, herunder børn under 18 år og umyndiggjorte
3. Kommunens ansatte, herunder fastansatte, tidsbegrænsede ansatte, vikarer og konsulenter, der varetager opgaver for kommunen uden at være underlagt kommunens ansættelsesretlige instruksbeføjelser.

De registrerede og de oplysninger, der behandles om disse i nærværende aftale, fremgår af skemaet under punkt A.3.

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

Behandlingen er tidsbegrænset og varer indtil Hovedaftalen ophører, hvorefter databehandleren sletter personoplysningerne i overensstemmelse med vilkårene i hoveddokumentets punkt 11, medmindre den dataansvarlige forinden har instrueret databehandleren i at forlænge behandlingsperioden.

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 indgive anmodningen om en specifik godkendelse mindst 120 dage inden anvendelsen af den pågældende underdatabehandler. jf. aftalens punkt. 7.3.

Den dataansvarliges afvisning af brug af underdatabehandlere i ikke sikre tredjelande, er ikke opsigelsesgrund for databehandleren.

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:

- | | |
|---|--|
| <input type="checkbox"/> Indsamling | <input type="checkbox"/> Brug |
| <input type="checkbox"/> Opbevaring | <input type="checkbox"/> Sletning |
| <input type="checkbox"/> Søgning | <input type="checkbox"/> Profilering |
| <input type="checkbox"/> Videregivelse | <input type="checkbox"/> Systematisering |
| <input type="checkbox"/> Sammenstilling eller samkøring | |
| <input type="checkbox"/> Driftsovervågning | |
| <input type="checkbox"/> Registrering | |
| <input type="checkbox"/> Arkivering | |
| <input type="checkbox"/> Andre – Angiv: _____ | |

Databehandleren forpligter sig til alene at behandle personoplysninger på baggrund af dokumenterede instrukser fra den dataansvarlige og i overensstemmelse med den til enhver tid gældende databeskyttelseslovgivning.

Overlader databehandleren behandling af kommunens oplysninger til underdatabehandlere, er databehandleren ansvarlig for at indgå skriftlige (under)databehandleraftaler med disse, jf. Aftalens pkt. 7.4 og 8. Databehandleren er ansvarlig for, at kommunens instruks fremsendes til og accepteres af eventuelle underdatabehandlere.

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. Derfor er nedenstående elementer afgørende for sikkerhedsniveauet:

Behandlingen omfatter [en mindre/ større / stor] mængde personoplysninger omfattet af databeskyttelsesforordningens artikel [6 om lovlig behandling/ 9 om særlige kategorier af personoplysninger/ 10 om personoplysninger vedrørende straffedomme og lovovertrædelser] hvorfor der skal etableres et [tilstrækkeligt/ middel/ højt] sikkerhedsniveau.

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

Databehandleren skal ved tilrettelæggelsen af disse sikkerhedsforanstaltninger sikre et sikkerhedsniveau, der passer til de aftalte behandlinger, jf. bilag A. Foranstaltningerne fastlægges, så de opfylder Databeskyttelsesforordningens artikel 32 om behandlingssikkerhed ud fra overvejelser om:

- Hvad der kan lade sig gøre rent teknisk
- Implementeringsomkostningerne
- Den pågældende behandlings karakter, omfang, sammenhæng og formål, jf. bilag A
- Konsekvenserne for borgerne ved et sikkerhedsbrud
- Den risiko der er forbundet med behandlingerne, herunder risikoen for:
 - Tilintetgørelse af oplysninger
 - Tab af oplysninger
 - Ændring af oplysningerne
 - Uautoriseret videregivelse af oplysningerne
 - Uautoriseret adgang til oplysningerne

Databehandleren skal derudover tage stilling til behovet for at implementere foranstaltninger på følgende områder jf. informationssikkerhedsstandard ISO 27001 (Anneks A), herunder:

- Informationssikkerhedspolitikker
- Organisering af informationssikkerhed
- Medarbejdersikkerhed
- Styring af informationsaktiver
- Logisk adgangsstyring
- Anvendelse af kryptografi
- Fysisk sikkerhed
- Sikkerhed i driften
- Netværksikkerhed
- Sikkerhed i anskaffelse, udvikling og vedligeholdelse af systemer
- Sikkerhed i leverandørforhold
- Styring af sikkerhedsbrud
- Beredskabs- og reetableringsstyring
- Efterlevelse af lov- og kontraktmæssige krav

C.2.1. Krav vedrørende fysisk udstyr (hardware)

1. Der anvendes antivirus og antimalware på alle maskiner således, at det forhindres, at malware og virus spredes fra de enkelte laptops gennem jumpservere til miljøerne.
2. Der anvendes både enterprise-firewalls til netværkssegmentering og lokale firewalls på alle servere i alle miljøer.
3. Alle niveauer af løsningen patches løbende i henhold til den aftalte patch management-politik.

C.2.2. Lagring og kopiering af data, herunder personoplysninger

1. Data fra den dataansvarliges miljøer må aldrig lagres lokalt på databehandlerens it-udstyr.
2. Data må aldrig behandles lokalt på databehandlerens it-udstyr eller på anden måde behandles uden for de miljøer, der indeholder den Dataansvarliges data.

3. Databehandleren må aldrig foretage kopier af data fra den dataansvarliges miljøer, medmindre dette er særskilt aftalt med den dataansvarlige. Når der foretages sådanne kopier, skal databehandleren bistå den dataansvarlige med at sikre tilstrækkelig sikkerhed af kopierne samt bistå med at opsætte frister for sletning af kopierne.

C.2.3. Krav vedrørende cybersikkerhed

1. Der anvendes sikkerhedsforanstaltninger mod cyberangreb svarende til det til enhver tid værende trusselsbillede. Herunder, men ikke begrænset til, at software og operativsystemer til enhver tid er supporteret og opgraderet til seneste version.
2. Der er løbende kontrol af softwareløsning og systemer i forhold til OWASP top 10 sårbarheder, herunder brug af "ethical hacker".
3. Der patches løbende med formål at forbedre funktionaliteten, anvendeligheden, ydeevnen eller rette fejl i forhold til funktionalitet eller sikkerhedssårbarheder.

C.2.4. Vedrørende eksterne kommunikationsforbindelser

1. Der må kun etableres eksterne it-kommunikationsforbindelser med tilladelse fra den dataansvarlige og der træffes foranstaltninger til at sikre, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.

C.2.5. Krav vedrørende evnen til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og tjenester

1. Databehandleren foretager løbende mitigerende foranstaltninger af teknisk og organisatorisk karakter, når dette viser sig påkrævet. F.eks. efter et brud på persondatasikkerheden, vejledning fra it-revisionen og i forbindelse med revisionserklærings udvisende.
2. Databehandleren udbedrer uden ugrundet ophold udeståender, konstateret i forbindelse med udfærdigelse af revisionserklæringer
3. Databehandleren sikrer endvidere, at:
 - Organisatoriske sikkerhedsforanstaltninger implementeres således, at kun autoriserede personer kan tilgå miljøer, der indeholder den dataansvarliges data, og at autoriserede personer altid efterlever den adgangsprocedure, som den dataansvarlige har opsat, eksempelvis brugen af multifaktor autentifikation.
 - Autoriserede personer skal kunne fremvise billed-ID ved on-site databehandling hos den dataansvarlige.
 - Ansatte og eventuelle samarbejdspartnere skal til stadighed være bekendt med og have tilstrækkelig uddannelse og instruktion om databehandlingens formål, politikker, arbejdsgange og om deres tavshedspligt.

C.2.6. Krav vedrørende procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden

Databehandleren har til enhver tid tidssvarende procedurer for gennemførelse af:

1. Regelmæssig kontrol, vurdering, tilpasning og forbedring af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren er underlagt efter den til enhver tid gældende lovgivning, retspraksis, Datatilsynets afgørelser, anbefalinger og retningslinjer samt vilkårene i nærværende databehandleraftale.
2. Kontrol med at det fysiske sikkerhedsniveau er afstemt med det til enhver tid værende trusselsbillede.

C.2.7. Krav vedrørende fysisk sikring af lokaliteter, hvor der behandles oplysninger

Databehandleren sikrer, at:

1. Der er passende sikkerhedsforanstaltninger mod enhver uautoriseret adgang til lokationer, hvor den dataansvarliges data behandles. Databehandleren skal desuden, hvor det er nødvendigt, evaluere og forbedre effektiviteten af sådanne forhåndsregler.
2. Niveaulet for den fysiske sikkerhed til enhver tid er afstemt med det aktuelle trusselsbillede samt den følsomhed og mængde af persondata som databehandleren behandler for den dataansvarlige.

C.2.8. Krav vedrørende anvendelse af hjemme-/fjernarbejdspladser

Databehandleren sikrer, at:

1. Der anvendes kryptering af kommunikationsforbindelser.
2. Databehandlerens fjernadgang til den dataansvarliges netværk og systemer altid sker via den dataansvarliges krypterede VPN-forbindelse, Citrix eller anden lige så sikker fjernskrivebordsteknologi, som den dataansvarlige stiller til rådighed for databehandleren.
3. Databehandlerens ansattes udstyr er udleveret og administreret af databehandleren.
4. Databehandleren og dennes ansatte ikke tilgår den dataansvarliges miljøer ved brug af privat it-udstyr.
5. Applikationer og operativsystemer på udstyret er supporteret og opdateret.

6. Der er klare retningslinjer for ansattes adfærd ved anvendelse af fjern- og hjemmearbejdspladser. Retningslinjerne følger som minimum altid Center for Cybersikkerheds seneste vejledninger for hjemmearbejde.
7. Der er procedurer for løbende orientering og vejledning omkring sikkerhedsforanstaltninger i forhold til brug af hjemme-/fjernarbejdspladser.
8. De tekniske foranstaltninger bakkes op af velinformerede medarbejdere, som er bekendt med de angrebsmetoder, der også benyttes parallelt med tekniske angreb.
9. Uvedkommende ikke kan se og høre, hvad databehandleren beskæftiger sig med i den dataansvarliges miljøer. Databehandleren skal i den forbindelse undlade, at:
 - Tale i mobiltelefon om den dataansvarlige og dens fortrolige eller forretningskritiske aktiviteter, når der er uvedkommende inden for hørevidde.
 - Tilgå den dataansvarliges miljøer, når der er uvedkommende inden for synsvidde.
 - Lade mobile enheder ude af syne, så uvedkommende kan tilegne sig uberettiget adgang til den dataansvarliges miljøer og for at undgå tyveri af databehandlerens mobile enheder.

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:

C.3.1. Bistand til overholdelse af de registreredes rettigheder

Databehandleren skal indrette løsningerne således, at de understøtter den dataansvarliges pligt til at overholde reglerne om registreredes rettigheder.

Databehandleren har derfor implementeret en proces, hvor hver enkelt rettighed i forhold til de ”registreredes rettigheder”, jf. Punkt 9.1. litra a – j, gennemgås for at fastslå, om løsningen har funktionalitet, der understøtter den pågældende rettighed. Databehandleren dokumenterer denne vurdering.

Hvis ikke løsningen har funktionalitet, der understøtter den pågældende rettighed, vurderer databehandleren mindst en gang årligt efter aftalens indgåelse muligheden for videreudvikling af løsningen med henblik på at understøtte den dataansvarliges håndtering af registreredes rettigheder.

Databehandleren er ansvarlig for – inden hovedaftalens indgåelse - at underrette den dataansvarlige om, hvordan den konkrete løsning understøtter håndtering af registreredes rettigheder.

der, samt hvilke dele den dataansvarlige selv er ansvarlig for at løfte samt hvilke planer databehandleren har for videreudvikling af løsningens funktioner med henblik på at understøtte den dataansvarliges forpligtelser.

Den dataansvarlige kan instruere databehandleren i at iværksætte specifikke tiltag for, at den dataansvarlige kan imødekomme anmodninger fra registrerede.

C.3.2. Underretning af den dataansvarlige

Databehandleren skal have faste procedurer, der sikrer, at den Dataansvarlige uden unødigt forsinkelse skriftligt bliver underrettet om:

1. enhver anmodning rettet til databehandleren eller dennes eventuelle underdatabehandlere fra en registreret om udøvelse af den registreredes rettigheder. Den dataansvarlige besvarer sådanne henvendelser.
2. enhver henvendelse rettet til databehandleren eller dennes eventuelle underdatabehandlere fra Datatilsynet vedrørende behandling af personoplysninger omfattet af databehandleraftalen.
3. enhver henvendelse rettet til databehandleren eller dennes eventuelle underdatabehandlere fra øvrige myndigheder, der vedrører behandling af personoplysninger omfattet af databehandleraftalen.
4. videregivelse af de personoplysninger, som er omfattet af databehandleraftalen, med mindre orienteringen er forbudt i henhold til EU-retten eller lovgivningen i en medlemsstat. Såfremt videregivelsen finder sted som følge af præceptiv lov i et ikke sikkert tredjeland og orienteringen er forbudt i henhold til dette lands lovgivning, skal den pågældende databehandler straks oplyse den dataansvarlige om, at aftalen misligholdes.
5. sikkerhedsbrud i den dataansvarliges it-systemer, som databehandleren på nogen måde er blevet bekendt med eller har mistanke om.

C.3.3. Bistand ved sikkerhedsbrud

Databehandleren bistår den dataansvarlige i tilfælde af sikkerhedsbrud, for så vidt disse brud skyldes eller på anden måde er forbundet med databehandlerens behandling af personoplysninger i medfør af Aftalen. Databehandleren skal indsamle og dokumentere informationer om sikkerhedshændelser hos databehandleren og underdatabehandlere, og underrette den dataansvarlige om sikkerhedsbrud, uden unødigt forsinkelse og senest indenfor det antal timer som fremgår af punkt 10.2. Oplysningerne skal i sidste ende have et omfang og en detaljeringsgrad, som den dataansvarlige i det konkrete tilfælde finder tilstrækkeligt. Databehandleren oplyser så vidt muligt følgende indenfor den angivne tidsramme i punkt 10.2:

Dato og tid	Brud på persondatasikkerheden er konstateret den [DATO] klokken [KLOKKESLÆT]
Karakteren af bruddet	Hændelsen skyldes [BESKRIV ÅRSAGEN/KARAKTEREN AF BRUDET].

Kategorierne og det omtrentlige antal berørte registrerede	Typen af berørte registrerede er [ANGIV TYPEN AF BERØRTE REGISTREREDE] og antal berørte er [ANGIV ANTAL BERØRTE FOR HVER TYPE REGISTREREDE. EVT. DET OMTRENTLIGE ANTAL, HVIS EN NÆRMERE SPECIFICERING IKKE ER MULIG]
Typen af personoplysninger	[ANGIV TYPEN AF PERSONOPLYSNINGER]
Varigheden af bruddet	[ANGIV START- OG SLUTTIDSPUNKT]
De sandsynlige konsekvenser af bruddet	[BESKRIV SANDSYNLIGE KONSEKVENSER AF BRUDDET]
Andre oplysninger inkl. umiddelbar persondataretlig vurdering af bruddet	[ANGIV ANDRE OPLYSNINGER OM BRUDDET, DER KAN VÆRE BRUGBARE FOR DEN DATAANSVARLIGES VURDERING AF BRUDDETS INDVIRKNING]
Foranstaltninger truffet	[BESKRIV DE FORANSTALTNINGER, DER ER TRUFFET, ELLER SOM VIL BLIVE TRUFFET SOM LED I HÅNDTERINGEN AF BRUDDET OG DETS MULIGE SKADEVIRKNINGER]
Kontaktoplysninger	[NAVN OG KONTAKTOPLYSNINGER TIL KONTAKTPUNKT, HVOR YDERLIGERE OPLYSNINGER KAN INDHENTES]

Oplysningerne sendes til mailpostkassen: [\[mailadresse\]](#)

C.3.4. Bistand ved gennemførelse af databeskyttelse gennem design og databeskyttelse gennem standardindstillinger

Hvor databehandleren leverer, konfigurerer, opsætter eller udvikler m.m. et System, skal databehandleren bistå den dataansvarlige med at gennemføre passende tekniske og organisatoriske foranstaltninger med henblik på at sikre databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, jf. databeskyttelsesforordningens artikel 25.

C.3.5. Databehandlerens omkostninger ved bistand til den dataansvarlige

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

C.4 Opbevaringsperiode/sletterutine

Databehandleren sikrer, at der sker sletning af personoplysninger i form af evt. midlertidige kopier, jf. afsnit C.2.2, inden for 5 dage fra tidspunktet for foretagelse af kopieringen.

C.5 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.

C.6 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren

Databehandleren skal hvert år for egen regning indhente en **revisionserklæring** fra en uafhængig tredjepart vedrørende databehandlerens 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 **revisionserklæring** kan anvendes i overensstemmelse med disse Bestemmelser:

ISAE 3000 Høj.

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

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

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. **Denne ret er uden beregning for den dataansvarlige.**

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion.

C.7 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere

Databehandleren skal hvert år for egen eller underdatabehandlerens regning indhente en **revisionserklæring** fra en uafhængig tredjepart 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 revisionserklæring kan anvendes i overensstemmelse med disse bestemmelser:

ISAE 3000 Høj.

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

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

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

Dokumentation for sådanne inspektioner fremsendes uden unødigt forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden af inspektionen og kan i sådanne tilfælde anmode om gennemførelsen af en ny inspektion under andre rammer og/eller under anvendelse af anden metode.

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.

Den dataansvarliges eventuelle deltagelse i en inspektion 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.

Databehandlerens og underdatabehandlerens eventuelle udgifter i forbindelse med en fysisk inspektion af underdatabehandlerens lokaliteter er den dataansvarlige uvedkommende – uanset om den dataansvarlige har initieret og deltaget i en sådan inspektion.

Bilag D Parternes regulering af andre forhold

D.1. Misligholdelse og erstatning

1. Den dataansvarlige, databehandleren og eventuelle underdatabehandlere er erstatningsansvarlige i overensstemmelse med dansk rets almindelige regler i tilfælde af misligholdelse af databehandleraftalen eller overtrædelse af den til enhver tid gældende databeskyttelseslovgivning.
2. Ved databehandlerens misligholdelse af databehandleraftalen har den dataansvarlige de misligholdelsesbeføjelser, der følger af dansk rets almindelige regler.
3. Databehandleraftalen er en del af hovedaftalen, hvorved en misligholdelse af databehandleraftalen også er en misligholdelse af hovedaftalen. Ved væsentlig misligholdelse af databehandleraftalen er den dataansvarlige berettiget til at ophæve databehandleraftalen og hovedaftalen.
4. Den dataansvarliges ophævelse af hovedaftalen og databehandleraftalen indebærer ikke, at den dataansvarlige giver afkald på sin ret til at kræve erstatning, hvis betingelserne herfor er opfyldt.
5. Såfremt den dataansvarlige vælger ikke at ophæve hovedaftalen og databehandleraftalen i ét eller flere tilfælde af databehandlerens væsentlige misligholdelse, medfører det ikke, at den dataansvarlige mister retten til at ophæve hovedaftalen og databehandleraftalen i andre tilfælde.
6. Såfremt den dataansvarlige af tredjemand gøres tort- og/eller erstatningsansvarlig – herunder i form af evt. kompensationskrav fra den/de registrerede – som følge af databehandlerens eller eventuelle underdatabehandleres misligholdelse af databehandleraftalen eller overtrædelse af den til enhver tid gældende databeskyttelseslovgivning, skal databehandleren holde den dataansvarlige skadesløs for alle omkostninger og tab.
7. Enhver ansvarsbegrænsning eller erstatningsmaksimering, der er fastlagt i hovedaftalen eller andet sted, er ikke gældende i tilfælde af databehandlerens misligholdelse af databehandleraftalen eller den til enhver tid gældende databeskyttelseslovgivning.
8. Databehandleren skal bistå med at forsvare den dataansvarliges interesser i en eventuel rets- eller voldgiftssag, uagtet databehandlerens eventuelle indsigelser i forhold til den påberåbte misligholdelse, såfremt databehandlerens bistand er af betydning for varetagelsen af den dataansvarliges interesser, og at dette ikke samtidig skader databehandlerens stilling.

D.2. Konsekvenser ved eventuel ulovlig instruks

Såfremt databehandleren vurderer, at en instruks er ulovlig, skal databehandleren straks oplyse om og dokumentere dette overfor den dataansvarlige. Den dataansvarlige er herefter pligtig til at genoverveje lovligheden af instruksen. Begge parter indgår loyalt og konstruktivt i samarbejdet om at tilrette instruksen, så den utvivlsomt bliver lovlig.

D.3. Overdragelse

Databehandleren må ikke overdrage sine rettigheder og forpligtelser i henhold til denne databehandleraftale uden den dataansvarliges forudgående samtykke.

D.4. Tavshedspligt

Følgende supplerer punkt 5 i hoveddokumentet:

1. Databehandleren er - under og efter denne og hovedaftalens ophør - pålagt tavshedspligt om alle oplysninger, denne bliver bekendt med gennem samarbejdet. Aftalen indebærer, at bestemmelserne i straffelovens §§ 152-152f, jf. straffelovens § 152a, om tavshedspligt finder anvendelse.
2. Databehandleren sikrer, at alle, der behandler oplysninger omfattet af denne aftale, herunder ansatte, tredjeparter (f.eks. en reparatør) og underdatabehandlere, forpligter sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.
3. Databehandleren må ikke hverken offentligt eller til tredjeparter kommunikere om brud på persondatasikkerheden, uden forudgående skriftlig aftale med dataansvarlige om indholdet af en sådan kommunikation, medmindre databehandleren har en retlig forpligtelse til sådan kommunikation.