Capptain ApS
Uldjydevej 2, Birk
7400 Herning
info@capptain.dk
www.capptain.dk

Version 1.1., senest revideret 17. marts 2025

Databehandleraftale

Mellem

Den dataansvarlige:

Brugere af Capptain

og

Databehandleren:

Capptain ApS

CVR 45287203

Uldjydevej 2

7400 Herning

Danmark

Capptain ApS
Uldjydevej 2, Birk
7400 Herning
info@capptain.dk
www.capptain.dk

Indhold

Capptain ApS
Uldjydevej 2, Birk
7400 Herning
info@capptain.dk
www.capptain.dk

1. Baggrund for databehandleraftalen

1. Denne aftale fastsætter de rettigheder og forpligtelser, som finder anvendelse, når Databehandleren foretager behandling af personoplysninger på vegne af den Dataansvarlige.

2. Aftalen 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), som stiller specifikke krav til indholdet af en databehandleraftale.

3. Databehandlerens behandling af personoplysninger sker med henblik på opfyldelse af den mellem parterne indgåede aftale om licens til SaaS-platformen Capptain.

4. Databehandleraftalen og Hovedaftalen om levering af Capptain (herefter benævnt som hovedaftalen) er indbyrdes afhængige, og kan ikke opsiges særskilt. Databehandleraftalen kan dog – uden at opsige hovedaftalen – erstattes af en anden gyldig databehandleraftale, såfremt dette måtte blive nødvendigt.

5. Denne databehandleraftale har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne, herunder i hovedaftalen.

6. Til denne aftale hører fire bilag. Bilagene fungerer som en integreret del af databehandleraftalen.

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

8. Databehandleraftalens Bilag B indeholder den Dataansvarliges betingelser for, at Databehandleren kan gøre brug af eventuelle underdatabehandlere, samt en liste over de eventuelle underdatabehandlere, som den Dataansvarlige har godkendt.

9. Databehandleraftalens Bilag C indeholder en nærmere instruks om, hvilken behandling Databehandleren skal foretage på vegne af den Dataansvarlige (behandlingens genstand), hvilke sikkerhedsforanstaltninger, der som minimum skal iagttages, samt hvordan der føres tilsyn med Databehandleren og eventuelle underdatabehandlere.

10. Databehandleraftalens Bilag D indeholder parternes eventuelle regulering af forhold, som ikke ellers fremgår af databehandleraftalen eller parternes hovedaftale.

11. Databehandleraftalen med tilhørende bilag opbevares skriftligt, herunder elektronisk af begge parter.

12. Denne databehandleraftale frigør ikke Databehandleren for forpligtelser, som efter persondataforordningen eller enhver anden lovgivning direkte eller indirekte er eller bliver pålagt Databehandleren.

2. Den dataansvarliges forpligtelser og rettigheder

1. Den Dataansvarlige er overfor omverdenen (herunder den registrerede) ansvarlig for, at behandlingen af personoplysninger sker indenfor rammerne af Databeskyttelses-forordningen og databeskyttelsesloven.

2. Den Dataansvarlige har derfor både rettighederne og forpligtelserne til at træffe beslutninger om, til hvilke formål og med hvilke hjælpemidler der må foretages behandling.

3. Den Dataansvarlige er blandt andet ansvarlig for, at der foreligger fornødent hjemmelsgrundlag til den behandling, 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. I så fald underretter Databehandleren den Dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. art 28, stk. 3, litra a.

2. Databehandleren forpligtes til straks at underrette den Dataansvarlige, hvis en instruks efter Databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret. En sådan underretning skal være skriftlig.

4. Fortrolighed

1. Databehandleren sikrer, at kun de personer, der aktuelt er autoriseret hertil, har adgang til de personoplysninger, der behandles på vegne af den Dataansvarlige. Adgangen til oplysningerne skal derfor straks lukkes ned, hvis autorisationen fratages eller udløber.

2. Der må alene autoriseres personer, for hvem der foreligger en saglig nødvendighed til at have adgang til personoplysningerne for at kunne opfylde Databehandlerens forpligtelser overfor den Dataansvarlige.

3. Databehandleren sikrer, at de personer, der er autoriseret til at behandle personoplysninger på vegne af den Dataansvarlige, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

4. Databehandleren skal efter anmodning fra den Dataansvarlige kunne påvise, at de relevante medarbejdere er underlagt ovennævnte tavshedspligt.

Capptain ApS
Uldjydevej 2, Birk
7400 Herning
info@capptain.dk
www.capptain.dk

5. Behandlingssikkerhed

1. Databehandleren iværksætter alle foranstaltninger, som kræves i henhold til databeskyttelsesforordningens artikel 32, hvoraf det bl.a. fremgår, at der under hensyntagen til det aktuelle niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.

2. Ovenstående forpligtelse indebærer, at Databehandleren skal foretage en risikovurdering, og herefter gennemføre nødvendige foranstaltninger for at imødegå eventuelt identificerede risici. Der kan herunder bl.a., alt efter hvad der er relevant, være tale om følgende foranstaltninger:

    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

3. Databehandleren skal i forbindelse med ovenstående – i alle tilfælde – som minimum iværksætte det sikkerhedsniveau og de foranstaltninger, som er specificeret nærmere i denne aftales Bilag C.

4. Parternes eventuelle regulering/aftale om vederlæggelse eller lign. i forbindelse med den Dataansvarliges eller Databehandlerens efterfølgende krav om etablering af yderligere sikkerhedsforanstaltninger vil fremgå af parternes hovedaftale eller af denne aftales bilag D.

6. Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2 og 4, for at gøre brug af en anden databehandler (underdatabehandler).

2. Databehandleren må således ikke gøre brug af en anden databehandler (underdatabehandler) til opfyldelse af databehandleraftalen uden forudgående specifik eller generel skriftlig godkendelse fra den Dataansvarlige.

3. I tilfælde af generel skriftlig godkendelse skal Databehandleren underrette den Dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre databehandlere og derved give den Dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer.

4. Den Dataansvarliges nærmere betingelser for Databehandlerens brug af eventuelle underdatabehandlere fremgår af denne aftales Bilag B.

5. Den Dataansvarliges eventuelle godkendelse af specifikke underdatabehandlere er anført i denne aftales Bilag B.

6. Når Databehandleren har den Dataansvarliges godkendelse til at gøre brug af en underdatabehandler, sørger Databehandleren for at pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er fastsat i denne databehandleraftale, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen. Databehandleren er således ansvarlig for – igennem indgåelsen af en underdatabehandleraftale – at pålægge en eventuel underdatabehandler mindst de forpligtelser, som Databehandleren selv er underlagt

efter databeskyttelsesreglerne og denne databehandleraftale med tilhørende bilag.

7. Underdatabehandleraftalen 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 der er indgået en gyldig aftale mellem Databehandleren og underdatabehandleren. Eventuelle kommercielle vilkår, eksempelvis priser, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den Dataansvarlige.

8. 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 underdatabehandleren, f.eks. så den Dataansvarlige kan instruere underdatabehandleren om at foretage sletning eller tilbagelevering af oplysninger.

9. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver Databehandleren fuldt ansvarlig over for den Dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser.

7. Overførsel af oplysninger til tredjelande eller internationale organisationer

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den Dataansvarlige, herunder for så vidt angår overførsel (overladelse, videregivelse samt intern anvendelse) af personoplysninger til tredjelande eller internationale organisationer, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Databehandleren er underlagt; i så fald underretter Databehandleren den Dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige

interesser, jf. art 28, stk. 3, litra a.

2. Uden den Dataansvarliges instruks eller godkendelse kan Databehandleren – indenfor rammerne af databehandleraftalen – derfor bl.a. ikke;

    a. overføre personoplysningerne til en dataansvarlig eller databehandler i et tredjeland eller en international organisation,
    b. overlade behandlingen af personoplysninger til en underdatabehandler i et tredjeland,
    c. lade oplysningerne behandle i en anden af databehandlerens afdelinger, som er placeret i et tredjeland.

3. Den Dataansvarliges eventuelle instruks eller godkendelse af, at der foretages overførsel af personoplysninger til et tredjeland, vil fremgå af denne aftales Bilag C.

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 3.

    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. den registreredes indsigtsret
    d. retten til berigtigelse
    e. retten til sletning (»retten til at blive glemt«)

f. retten til begrænsning af behandling
g. underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
h. retten til dataportabilitet
i. retten til indsigelse
j. retten til at gøre indsigelse mod resultatet af automatiske individuelle afgørelser, herunder profilering

2. Databehandleren bistår den dataansvarlige med at sikre overholdelse af den Dataansvarliges forpligtelser i medfør af databeskyttelsesforordningens artikel 32-36 under hensynstagen til behandlingens karakter og de oplysninger, der er tilgængelige for Databehandleren, jf. art 28, stk. 3, litra f.

   Dette indebærer, at Databehandleren under hensynstagen til behandlingens karakter skal bistå den Dataansvarlige i forbindelse med, at den Dataansvarlige skal sikre overholdelsen af:

   a. forpligtelsen til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med behandlingen
   b. forpligtelsen til at anmelde brud på persondatasikkerheden til tilsynsmyndigheden (Datatilsynet) uden unødig forsinkelse og om muligt senest 72 timer, efter at den Dataansvarlige er blevet bekendt med bruddet. Medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.
   c. forpligtelsen til – uden unødig forsinkelse – at underrette den/de registrerede om brud på persondatasikkerheden, når et sådant brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
   d. forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder

e. forpligtelsen til at høre tilsynsmyndigheden (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. Parternes eventuelle regulering/aftale om vederlæggelse eller lignende i forbindelse med Databehandlerens bistand til den Dataansvarlige vil fremgå af parternes hovedaftale eller af denne aftales bilag D.

9. Underretning om brud på persondatasikkerheden

1. Databehandleren er forpligtet til – uden unødig forsinkelse at underrette den Dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos Databehandleren eller en eventuel underdatabehandler.

   Databehandlerens underretning til den Dataansvarlige skal om muligt ske senest 24 timer efter at denne er blevet bekendt med bruddet, sådan at den Dataansvarlige har mulighed for at efterleve sin eventuelle forpligtelse til at anmelde bruddet til tilsynsmyndigheden indenfor 72 timer.

2. I overensstemmelse med denne aftales afsnit 10.2., litra b, skal Databehandleren til – under hensynstagen til behandlingens karakter og de oplysninger, der er tilgængelige for denne – at bistå den Dataansvarlige med at foretage anmeldelse af bruddet til tilsynsmyndigheden.

   Det kan betyde, at Databehandleren bl.a. skal hjælpe med at tilvejebringe nedenstående oplysninger, som efter databeskyttelsesforordningens artikel 33, stk. 3, skal fremgå af den Dataansvarliges anmeldelse til tilsynsmyndigheden:

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. Sandsynlige konsekvenser af bruddet på persondatasikkerheden
c. Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden, herunder hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger

10. Sletning og tilbagelevering af oplysninger

1. Ved opsigelse af den mellem parterne indgåede hovedaftale og nærværende databehandleraftale forpligtes Databehandleren til, efter den Dataansvarliges valg, at slette eller tilbagelevere alle personoplysninger til den Dataansvarlige, samt at slette eksisterende kopier, medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne.

11. Tilsyn og revision

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise Databehandlerens overholdelse af databeskyttelsesforordningens artikel 28 og denne aftale, 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. Den nærmere procedure for den Dataansvarliges tilsyn med Databehandleren fremgår af denne aftales Bilag C.

3. Den Dataansvarliges tilsyn med eventuelle underdatabehandlere sker som udgangspunkt gennem Databehandleren. Den nærmere procedure herfor fremgår af denne aftales Bilag C.

4. Databehandleren er forpligtet til at give myndigheder, der efter den til enhver tid gældende lovgivning har adgang til den Dataansvarliges og Databehandlerens

faciliteter, eller repræsentanter, der optræder på myndighedens vegne, adgang til Databehandlerens fysiske faciliteter mod behørig legitimation.

12. Parternes aftaler om andre forhold

1. En eventuel (særlig) regulering af konsekvenserne af parternes misligholdelse af Databehandleraftalen vil fremgå af parternes hovedaftale eller af denne aftales Bilag D.

2. En eventuel regulering af andre forhold mellem parterne vil fremgå af parternes hovedaftale eller af denne aftales Bilag D.

3. Den Dataansvarlige har selv adgang til dokumenter og personoplysninger, som uploades eller håndteres via platformen, og skal således selv sikre at kun betroede medarbejdere har adgang til disse oplysninger, samt at adgangskoder har en tilfredsstillende sikkerhed, og opbevares forsvarligt.

13. Ikrafttræden og ophør

1. Denne aftale træder i kraft ved kontraktindgåelse med Capptain. Den erstatter enhver tidligere indgået databehandleraftale indgået mellem parterne.

2. Aftalen kan af begge parter kræves genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i aftalen giver anledning hertil.

3. Parternes eventuelle regulering/aftale om vederlæggelse, betingelser eller lignende i forbindelse med ændringer af denne aftale vil fremgå af parternes hovedaftale eller af denne aftales bilag D.

4. Opsigelse af databehandleraftalen kan ske i henhold til de opsigelsesvilkår, inkl. opsigelsesvarsel, som fremgår af hovedaftalen.

5. Aftalen er gældende, så længe behandlingen består. Uanset eventuel opsigelse af hovedaftalen og/eller nærværende databehandleraftale, vil databehandleraftalen

forblive i kraft frem til behandlingens ophør og oplysningernes sletning hos Databehandleren og eventuelle underdatabehandlere.

6. Godkendelsen i Capptain-platformen af ejer eller systemadministrator er at sidestille med underskrift på nærværende aftale.

14. Kontaktpersoner/kontaktpunkter hos den dataansvarlige og databehandleren

1. Dataansvarlige, kan kontakte Capptain, som Databehandleren, via nedenstående kontaktpersoner/kontaktpunkter:

2. Databehandleren kan kontakte den dataansvarlige via kontaktinformationerne skrevet i Capptain-platformen.

3. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersonen/kontaktpunktet.

Navn:	Maria Hindkjær Bonet Clar
Stilling:	Udviklingschef
Tlf.:	+45 81 45 01 02
E-mail:	mc@capptain.dk

Navn:	Torben Olesen
Stilling:	Projektleder & Supporter
Tlf.:	+45 78 70 18 48
E-mail:	to@capptain.dk info@e-miljo.dk

Capptain ApS
Uldjydevej 2, Birk
7400 Herning
info@capptain.dk
www.capptain.dk

15. Bilag

Bilag A: Oplysninger om behandlingen

Formålet med Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige er:

Capptain kunder kan anvende Capptain-platformen, som ejes og administreres af Capptain, til at indsamle og behandle data om den Dataansvarliges afdelinger og ansatte.

Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige drejer sig primært om (karakteren af behandlingen):

Capptain, som Databehandler, stiller systemet Capptain til rådighed for den Dataansvarlige og herigennem opbevarer personoplysninger om den Dataansvarliges medarbejdere på virksomhedens underdatabehandlers servere.

Behandlingen omfatter følgende typer af personoplysninger om de registrerede:

- Navn
- E-mail adresse
- Telefonnummer
- Adresse
- CVR-nummer
- P-nummer
- Billede- og videomateriale
- Registrering af ulykke
- Uddannelses/kursusbeviser
- APV-kommentarer
- Whistleblowerindberetninger
- Andre potentielle personoplysninger, som den Dataansvarlige finder relevant for deres miljø- og arbejdsmiljøstyringsværktøj, Capptain

Behandlingen omfatter følgende kategorier af registrerede:

Personer, som er eller har været ansat hos den Dataansvarlige.

Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige kan påbegyndes efter denne aftales ikrafttræden. Behandlingen har følgende varighed:

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

Bilag B: Betingelser for Databehandlerens brug af underdatabehandlere og liste over godkendte underdatabehandlere

B.1 Betingelser for Databehandlerens brug af eventuelle underdatabehandlere

Databehandleren har den Dataansvarliges generelle godkendelse til at gøre brug af underdatabehandlere. Databehandlerens godkendelse hertil sker ved kontraktindgåelse, da anvendelsen deraf er nødvendig i forhold til udvikling og vedligehold af IT-systemet. Databehandleren skal dog underrette den Dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre Databehandlere og derved give den Dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer. En sådan underretning skal være den Dataansvarlige i hænde minimum to måneder før anvendelsen eller ændringen skal træde i kraft. Såfremt den Dataansvarlige har indsigelser mod ændringerne, skal den Dataansvarlige give meddelelse herom til Databehandleren inden 14 dage efter modtagelsen af underretningen. Den Dataansvarlige kan alene gøre indsigelse, såfremt den Dataansvarlige har rimelige og konkrete årsager hertil.

B.2 Godkendte underdatabehandlere

Databehandlerens underleverandører er oplistet i den til enhver tid opdaterede liste over underdatabehandlere, som kan ses her: www.capptain.dk/underleverandoerer.

Navn	CVR-nr	Adresse	Beskrivelse af behandling
ABAS Miljøservice	13438692	Uldjydevej 2, 7400 Herning	IT-leverandør
DataSign	26924421	Jernbanegade 54, 1. sal 6000 Kolding	IT-udvikling af E-Miljø.
Concept Data	14918876	Rosenholmvej 13, 7400 Herning	C5 integration til E-Miljø med af-falds- og medlemsdata.
Curanet	29412006	Højvangen 4, 8660 Skanderborg	IT-systemet bliver hostet af Curanet.
Active-Campaign		Chicago, US 1 North Dearborn St 5th Floor Chicago, IL 60602	CRM + E-mail Marketing
Mailchimp		The Rocket Science Group, LLC 675 Ponce de Leon Ave NE Suite 5000 Atlanta, GA 30308 USA	E-mail Marketing

Figur 1: Skal på hjemmesiden (tilføj HubSpot og Azend, slet Active Campaign, Mailchimp og Concept Data)

Den Dataansvarlige har ved databehandleraftalens ikrafttræden specifikt godkendt anvendelsen af de oplistede underdatabehandlere til netop den behandling, som er beskrevet ud for parten. Databehandleren kan ikke – uden den Dataansvarliges specifikke og skriftlige godkendelse – anvende den enkelte underdatabehandler til en "anden" behandling end aftalt eller lade en anden underdatabehandler foretage den beskrevne behandling.

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 opgaver som nærmere beskrevet i den mellem parterne indgåede hovedaftale.

C.2 Behandlingssikkerhed

Til opfyldelse af nærværende databehandleraftale har Databehandleren forpligtet til at iværksætte og implementere nedenstående foranstaltninger for herigennem at kunne leve op til de af den Dataansvarlige udstukne sikkerheds instrukser.

C.2.1. Sikkerhedsforanstaltninger

Databehandleren skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger, mod at de i bilag A anførte personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lov om behandling af personoplysninger. Databehandleren er således blandt andet forpligtet til at:

- sikre at alle medarbejderes telefoner, pc'ere, ipads m.v. er forsynet med forsvarlig adgangskode
- sikre, at alene medarbejdere med arbejdsrelaterede saglige formål har adgang til personoplysningerne
- opbevare datalagermedier på forsvarlig vis, således at disse ikke er tilgængelige for tredjemand
- sikre, at bygninger og systemer, der anvendes i forbindelse med databehandlingen, er sikre
- sikre, at der alene anvendes hardware og software af høj kvalitet
- sikre at anvendt hardware og software opdateres løbende
- sikre at prøver og affaldsmateriale tilintetgøres, i overensstemmelse med kravene til databeskyttelse eller efter nærmere instrukser fra den Dataansvarlige. De makuleres.
- sikre at medarbejdere modtager passende uddannelse, fyldestgørende instruktioner i og retningslinjer for behandlingen af personoplysningerne
- sikre at medarbejdere modtager løbende uddannelse med henblik på til enhver tid at være korrekt instrueret i korrekt og lovlig behandling af personoplysningerne.

Der er tale om behandling af en lille mængde personoplysninger omfattet af databeskyttelsesforordningens artikel 9 om "særlige kategorier af personoplysninger", hvorfor der skal etableres et "højt" sikkerhedsniveau" på denne baggrund.

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

Databehandleren skal dog – i alle tilfælde og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den Dataansvarlige (på baggrund af den risikovurdering den Dataansvarlige har foretaget):

Fortrolighed, integritet, tilgængelighed og robusthed er parametre, der dækker over den Dataansvarliges grundlæggende tilgang til datasikkerhed. Der må ikke være uautoriseret adgang til eller anvendelse af personoplysninger eller af det udstyr, der anvendes til behandlingen, og man skal kunne validere om oplysningerne i Capptain er korrekte. Dataansvarlig vil konstant sørge for at Capptain-platformen og dets moduler altid er tilgængelige ved anmodning fra en autoriseret bruger. Skulle der ske brud på dette, såsom en IT-fejl eller nedbrud, så vil der blive handlet på dette prompte, og sørget for at systemet igen er tilgængeligt. Samtidig er alt data i systemet ejet af kunden selv, og systemet er ejet af Capptain. Hvis den eksterne IT-leverandør skulle gå konkurs el.a., så er data forsat altid tilgængeligt.

Dataansvarlig vil sikre, at personoplysninger ikke fortabes, beskadiges eller ændres utilsigtet. Derfor tages der backup af data én gang i døgnet, som opbevares hos underdatabehandler Curanet. Herved vil systemet automatisk synkronisere sikkerhedskopien med de specifikke ændringer. Det betyder, at der til en hver tid kan genskabe Capptain brugeres data. Det eneste krav er, at brugeren skal være forbundet til internettet. Backupoverførslen sikres med en 128-bit SSL kryptering og sendes til deres topsikre datacenter. Det vil sige, at alle Capptain brugere altid kan få fat i deres data, hvis de f.eks. er ude for computernedbrud, hackingangreb, brand, indbrud eller lignende uforudsete hændelser.
Dataansvarlig vil, på bedst mulig vis, sørge for at Capptain er så modstandsdygtigt og stabilt som muligt, ved at sikre systemet imod skadelige hændelser. Dette sikres gennem en lang række faktorer, såsom datacentrets fysiske placering, køling, ventilation, nødgenerator, brandslutningsudstyr, det rigtige hardware, en redundant internetforbindelse og lignende. Underdatabehandleren, Curanet, sikrer en gennemsnitlig oppetid på 99,95%. De ting der

bringer procentsatsen under de hundrede er tvungen nedetid pga. opdateringer m.v., samt mindre driftforstyrrelser, hvilket er umuligt at undgå til fulde.

Datacentrets fysiske placering giver det en række unikke fordele. Det er placeret i et område med sikker afstand til andre bygninger, hævet over såvel vandspejl som jordhøjde og isoleret således at oversvømmelser, røggasser fra brand i nærliggende bygninger eller slukningsvand ikke kan påvirke driften. Datacentret er forbundet med 2 separate strømtilslutninger, hvilket skaber redundans i tilfælde af strømsvigt. En lokal generatorstation leverer strøm i det daglige, mens en 500 kVA dieselgenerator tager over, i tilfælde af at der opleves strømsvigt fra el-nettet. Dieselgeneratoren kan levere minimum 12 timers drift på én tank – hvis nødvendigt vil den løbende blive fyldt op af en tankvogn. Der benyttes redundante køleenheder, således at en vilkårlig komponent kan gå i stykker, uden at det har en væsentlig betydning for temperaturen i driftscentret. Der leveres en nedkølet luft på ca. 23°C med en minimal luftfugtighed. Datacentret bliver beskyttet af et "sniffer" system, der sikrer en hurtig alarmering og aktivering af et inergenanlæg i tilfælde af brand. Det betyder, at ild i en enkel server ikke kan gøre skade på andet udstyr i datacentret. Datacentret ligger 70 meter over havoverfladen – gennemsnittet i området er 60 meter. Det er derved utrolig godt beskyttet mod oversvømmelse og store vandmasser. Indenfor står alle servere på et hævet gulv, 0,5 meter over jordhøjden, hvortil der er tilsluttet flere afløb med højvandslukke. Planlagt systemarbejde vil oftest blive udført om natten, eller når det vurderes at være til mindst mulig ulempe for vores kunder. Systemarbejdet vil alt efter varighed, som minimum blive annonceret, når man logger på Capptain-platformen. I særlige tilfælde, hvor nedetiden overstiger 5 minutter, vil det blive udmeldt mindst to uger før den planlagte nedetid. Alle arbejdsmaskiner og servere er udstyret med firewalls og antivirus software, der har til hensigt at blokere alle former for vira mv. Dertil er der stor fokus på at optimere netværksinfrastrukturen til at kunne modstå alle former for hackerangreb.

C.2.2. Afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed

For at træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger for at beskytte personoplysningerne i Capptain vil sikkerheden løbende blive vurderet, grundet den konstante teknologiske udvikling. Der vil ske en afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af

behandlingssikkerhed mindst én gang årligt via en egenkontrol.

C.2.3. Krav vedrørende adgang til data

Data i Capptain bør nødvendigvis ikke være tilgængeligt for alle i virksomheden. I opsætnings-modulet er det muligt at definere præcis hvilke brugerrettigheder de specifikke brugere har. Det er vigtigt at få koblet de rigtige personer til i forhold til adgangen til personfølsom data. Capptain har foreslået nogle generelle brugerrettigheder i forbindelse med hvert brugerniveau. Disse kan dog ændres, så det passer den individuelle virksomhed.

Derudover, yder Capptain også en support-funktion. Hvis en bruger har brug for hjælp, og henvender sig derom. I den forbindelse vil vores Capptain supporter og IT-projektleder håndtere data – både almindeligt data, persondata og personfølsom data. Hvis den skriftlige kommunikation mellem kunden og Capptain på nogen måde indeholder personfølsom data, så vil disse blive slettet eller makuleret med det samme efter ydet hjælp.

C.2.4. Krav vedrørende beskyttelse af data, hvor de transmitteres og opbevares

Capptain (samt underdatabehandlere) hverken anvender, systematiserer eller læser personoplysningerne lagret i IT-systemet. Disse oplysninger er dog af primær karakter for at IT-systemet kan få den funktion, som hjælpeværktøj til virksomheders arbejde med miljø, arbejdsmiljø og compliance.

Personoplysninger vil altid blive behandlet i overensstemmelse med god databehandlingsskik. Dette betyder, at personoplysningerne behandles i overensstemmelse med:

- tydeligt angivne formål (eksempelvis oprettelse af en brugerprofil), og at senere behandling af oplysningerne ikke er uforenligt med det oplyste formål.
- At der ikke må indsamles flere oplysninger end hvad der er nødvendigt og relevant.
- At behandlingen af oplysningerne tilrettelægges så oplysningerne kan ajourføres, berigtiges og slettes når behandlingen af oplysningerne ikke længere er nødvendigt.

Vi indsamler ikke flere personoplysninger end nødvendigt, og vi opbevarer ikke oplysningerne længere end nødvendigt, og vi anvender ikke oplysningerne til andre formål, end de formål, som oplysningerne oprindeligt blev indsamlet til.

C.2.5. Sikring af behandlede personoplysninger

Capptain er på bedste vis sikret mod ulovlig indtrængen eller misbrug af personoplysninger. Dette bliver gjort både via kryptering af specifikt følsomt data, samt password til IT-systemet. Brugere har mulighed for at aktivere to-faktor-autentificering for at øge sikkerheden i systemet. Derudover, anbefaler vi en sikring af netværket, som bliver brugt til at køre Capptain (eksempelvis password til wifi, firewall, instrusion detection m.v.), samt privat login til enheden, som bliver brugt.

Systemet kører med internetstandarden HTTPS (Hypertext Transfer Protocol Secure). Det vil sige, at siden er mere sikker, og beskytter brugerens persondata. Denne standard understøtter en sikker kommunikation mellem browseren og webserverne. Dette bliver gjort i gennem et SSL-certifikat (Secure Socket Layer), som beskytter de data brugerne indtaster på sitet, og gør systemet sikkert for besøgende.

C.3 Opbevaringsperiode/sletterutine

Personoplysningerne opbevares hos databehandleren, indtil den dataansvarlige anmoder om at få oplysningerne slettet eller tilbageleveret.

Ved opsigelse af Capptain-abonnement vil de tilknyttede brugere og data automatisk blive slettet. Derudover kan en bruger til en hver tid kræve, at vi fjerner, retter eller blokerer personoplysninger vedrørende en specifik bruger i IT-systemet, som denne ikke længere ønsker offentliggjort, opbevaret eller behandlet.

De personhenførbare data som bedes slettes, vil blive slettet fuldstændigt. Dog kan de omhandlende Capptain-brugere ikke få slettet data, som er vigtigt for systemets opbygning af lovmæssige krav og pligt til opfyldelse deraf, såsom når de har udført et eftersyn af udstyr/værktøj, og derefter beder om at blive slettet. I den forbindelse er det kun brugerens navn, som vil forblive, imens alt andet data vil blive slettet, da virksomheden er bundet af loven til opfyldelse af dette.

Alt slettet data vil efter max 24 timer være ude af systemet. Hvis der bliver brug for at en backup skal ibrugtages inden 24 timer efter en person har gjort brug af "retten til at blive

glemt", så vil Capptain manuelt gå ind og genslette al den data, som er blevet fjernet, siden backuppen blev foretaget.

Derudover, har Capptain-kunder altid ret til at kunne få alt data fra systemet ud i et format, som er brugbart og læseligt.

C.4 Databehandlerens ret til overførsel af personoplysninger

Databehandleren er alene berettiget til at overføre de i Bilag A angivne personoplysninger til andre databehandlere eller underdatabehandlere, såfremt den Dataansvarlige skriftligt har givet instruks og accept herom. Databehandleren er ikke berettiget til at videregive eller overlade personoplysninger til andre databehandlere eller underdatabehandlere uden den Dataansvarliges forudgående skriftlige instruks, med mindre sådan videregivelse eller overladelse sker med direkte hjemmel i den til enhver tid gældende lovgivning.

C.5 Nærmere procedurer for den dataansvarliges tilsyn med den behandling, som foretages hos databehandleren

Databehandleren skal én gang årligt foranledige en egenkontrol af IT-systemets persondatasikkerhed. Derudover, har den Dataansvarlige adgang til at føre tilsyn vedr. databehandleraftalen, herunder fysisk tilsyn, hos databehandleren, når der efter den Dataansvarliges vurdering opstår et behov herfor. I sådan forbindelse skal dataansvarlig give Databehandler et varsel på mindst 30 dage.

Den Dataansvarliges eventuelle udgifter i forbindelse med et fysisk tilsyn afholdes af den Dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsagligt den tid), der er nødvendig for, at den Dataansvarlige kan gennemføre sit tilsyn.

C.6 Nærmere procedurer for tilsynet med den behandling, som foretages hos eventuelle underdatabehandlere

Databehandleren eller en repræsentant for databehandleren har adgang til at føre tilsyn, herunder fysisk tilsyn, hos underdatabehandleren, når der efter databehandlerens (eller den

dataansvarliges) vurdering opstår et behov herfor. Dokumentation for de afholdte tilsyn sendes snarest muligt til orientering hos den dataansvarlige.

Den dataansvarlige kan – hvis det findes nødvendigt – vælge at initiere og deltage på en fysisk inspektion hos underdatabehandleren. Dette kan blive aktuelt, såfremt den dataansvarlige vurderer, at databehandlerens tilsyn med underdatabehandleren ikke har givet den dataansvarlige tilstrækkelig sikkerhed for, at behandlingen hos underdatabehandleren sker i overensstemmelse med denne databehandleraftale.

Den dataansvarliges eventuelle deltagelse i et tilsyn hos underdatabehandleren ændrer ikke ved, at databehandleren også herefter har det fulde ansvar for underdatabehandlerens overholdelse af databeskyttelseslovgivningen og denne databehandleraftale.

Databehandlerens og underdatabehandleres eventuelle udgifter i forbindelse med afholdes af et fysisk tilsyn/en inspektion hos underdatabehandleren er den dataansvarlige uvedkommende – uanset at den dataansvarlige har initieret og eventuelt deltaget på et sådant tilsyn.

Bilag D: Parternes regulering af andre forhold

Hvis Dataansvarlige ønsker yderligere sikkerhedsforanstaltninger, skal denne fremsendes detaljeret beskrivelse til Databehandlerens e-mail info@capptain.dk, jf. pkt. 6 om behandlingssikkerhed. Herefter vil Databehandleren tage stilling til ønskerne, og hvorvidt om de kan imødekommes, samt en prissætning deraf.