Databehandleraftale gældende for IntraManager A/S' kunder og øvrige samarbejdspartnere, hvor IntraManager A/S kan betragtes som Databehandler

Virksomheder som har en:

Samarbejdsaftale/kundekontrakt

(Herefter den "Dataansvarlige")

og

IntraManager A/S

CVR 33966458

Helgavej 26

5230 Odense M

Danmark

(Herefter den "Databehandleren")

1 Indhold

2 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 parternes "hovedaftale".

4. Databehandleraftalen og "hovedaftalen" er indbyrdes afhængige, og kan ikke opsiges særskilt. Databehandleraftalen kan dog – uden at opsige "hovedaftalen" – erstattes af en anden gyldig databehandleraftale.

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

6. Til denne aftale hører tre 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. Databehandleraftalen med tilhørende bilag opbevares skriftligt, herunder elektronisk af begge parter.

11. Denne databehandleraftale frigør ikke databehandleren for forpligtelser, som efter databeskyttelsesforordningen eller enhver anden lovgivning direkte er pålagt databehandleren.

3 Den dataansvarliges forpligtelser og rettigheder

1. Den dataansvarlige har overfor omverdenen (herunder den registrerede) som udgangspunkt ansvaret for, at behandlingen af personoplysninger sker indenfor rammerne af databeskyttelsesforordningen 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 hjemmel til den behandling, 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; 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 underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5 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 det er nødvendigt 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.

6 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 foranstaltninger for at imødegå identificerede risici. Der kan herunder bl.a., alt efter hvad der er relevant, være tale om følgende foranstaltninger:

    a. 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".

7 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. De nærmere betingelser for databehandlerens brug af eventuelle underdatabehandlere fremgår af denne aftales Bilag B.

3. Når databehandleren har orienteret den dataansvarlige til at gøre brug af en underdatabehandler og opdateret Bilag B, har databehandleren sørget 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.

4. Underdatabehandleraftalen og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom - i kopi eller som link 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.

5. 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.

6. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser.

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 denne aftale:

a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
c. behandle personoplysningerne i et tredjeland

4. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i Bilag C.6.

5. Denne databehandleraftale skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og denne aftale 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. 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 hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, jf. art 28, stk. 3, litra f.

Dette indebærer, at databehandleren under hensyntagen 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. Parterne skal i Bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

10 Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en eventuel underdatabehandler.

   Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 48 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 9.2., litra b, skal databehandleren - under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for denne – 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

11 Sletning og tilbagelevering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling 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.

12 Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen 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. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.

3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13 Parternes aftaler om andre forhold

1. En eventuel (særlig) regulering af konsekvenserne af parternes misligholdelse af databehandleraftalen vil fremgå af parternes "hovedaftale".
2. En eventuel regulering af andre forhold mellem parterne vil fremgå af parternes "hovedaftale".

14 Ikrafttræden og ophør

1. Denne aftale træder i kraft ved begge parters underskrift af hovedaftalen og hvor der ikke er truffet anden databehandleraftale.

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".

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 "hovedaftalens" og/eller databehandleraftalens opsigelse, vil databehandleraftalen forblive i kraft frem til behandlingens ophør og oplysningernes sletning hos databehandleren og eventuelle underdatabehandlere.

15 Kontaktpersoner/kontaktpunkter hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner/kontaktpunkter, som nævnt i "hovedaftalen" mellem parterne.

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

16 Underskrift

På vegne af databehandleren:

Dato	10. juni 2022
Navn	Lars Klausen
Stilling	*Direktør*
Telefonnummer	+45 33 60 66 09
E-mail	LK@intramanager.com

Underskrift _____

Bilag A Oplysninger om behandlingen

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er:

At den dataansvarlige kan anvende systemerne ”IntraManager Work” og ”IntraManager Board”, som ejes og administreres af databehandleren til, at indsamle og behandle oplysninger om den dataansvarliges kunder og/eller medarbejdere.

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

At databehandleren stiller systemerne ”IntraManager Work” og ”IntraManager Board” til rådighed for den dataansvarlige og herigennem opbevarer personoplysninger om den dataansvarliges kunder og/eller medarbejdere på virksomhedens servere.

Behandlingen omfatter følgende typer af personoplysninger om de registrerede:

Navn, e-mailadresse, telefonnummer, adresse, køn, cpr-nummer, bankoplysninger, skattekort, pårørendes kontaktoplysninger, medarbejdernummer, lønnummer.

Behandlingen omfatter følgende kategorier af registrerede:

Personer, som har eller har haft et ansættelses- og/eller et kundeforhold 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 Underdatabehandlere

B.1 Godkendte underdatabehandlere

Den dataansvarlige har ved databehandleraftalens ikrafttræden godkendt anvendelsen af følgende underdatabehandlere:

Virksomhed	Amazon Web Services EMEA SARL (AWS Europe)
Registreringsnr.	B 186284
Adresse	38 Avenue John F. Kennedy L-1855 Luxembourg Luxembourg
Behandling	Datacenter hosting af servere
Særligt	AWS anvendes til hosting af løsningen, herunder lagring og processering af data, og dermed behandles alle data i platformen, inklusive kundernes persondata. Data opbevares krypteret. Denne behandling af data er AWS kontraktuelt forpligtet til at foretage inden for dataregion EU-WEST (Irland), og dermed indenfor EU/EØS, i henhold til og med de undtagelser, der fremgår af deres standard underdatabehandleraftale, i hvilket overførsel sker i henhold til SCC bestemmelser (som den dataansvarlige ved denne aftale giver fuldmagt til databehandleren til at indgå, herunder indgåelse af nye baseret på ændret SCC standarder), og med passende supplerende sikkerhedsforanstaltninger.

Virksomhed	inMobile ApS
Registreringsnr.	DK31426472
Adresse	Axel Kiers Vej 18 L 8270 Højbjerg Danmark
Behandling	SMS Gateway

Virksomhed	CPR-Administrationen
Registreringsnr.	DK29136815
Adresse	Holmens Kanal 22 1060 København K
Behandling	CPR-opslag

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.

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: generel drift, herunder hosting, visning, organisering, modtagelse, indhentelse, videresendelse, strukturering, tilpasning, implementering, søgning, processering, lagring, gendannelse, sletning, begrænsning, vedligeholdelse, udvikling, modeltræning, logning, support, fejlfinding og andre it-ydelser forbundet med databehandlerens levering af Software platformen til den dataansvarlige i henhold til den mellem parterne indgåede abonnementsaftale til databehandlerens Software løsninger.

C.2 Behandlingssikkerhed

Eftersom databehandlerens software muliggør, at den dataansvarlige kan uploade og på anden vis tilføje platformen data, vil databehandleren potentielt behandle en ukendt mængde af personoplysninger og ukendte kategorier af personoplysninger og datasubjekter. Derfor har databehandleren valgt at implementere et generelt sikkerhedsniveau afspejlende, at der kan ske behandling af en større mængde personoplysninger og af alle former for kategorier af personoplysninger og datasubjekter.

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

Informationssikkerhed

Databehandleren har implementeret politikker, kontroller og processer, som dækker de nedenfor beskrevne informationssikkerhedsområder:

Fortrolighed: Sikre at uautoriserede personer ikke kan få adgang til data, som kan misbruges til skade for databehandlerens kunder, forretningsforbindelser og ansatte.

Integritet: Sikre at systemer indeholder akkurat og komplet information.

Tilgængelighed: Sikre at relevant information og relevante systemer er tilgængelige og stabile.

Instruks

Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres. Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.

Fysisk sikkerhed

Databehandlerenen skal opretholde fysiske sikringsforanstaltninger til sikring af lokaliteter, som anvendes til behandling af personoplysninger, herunder opbevaring af personoplysninger omfattet af databehandleraftalen mod uvedkommendes adgang og manipulation.

Databehandlerenen skal have passende tekniske foranstaltninger til at begrænse risikoen for enhver uautoriseret adgang til lokaler, hvor der behandles persondata. Databehandleren skal desuden, hvor det er nødvendigt, evaluere og forbedre effektiviteten af sådanne forholdsregler. Sikrer at niveauet for den fysiske sikkerhed til enhver tid være er afstemt med det aktuelle trusselbillede samt den følsomhed og mængde af persondata som databehandleraftalen omfatter.

Kommunikationsforbindelser og kryptering

Databehandleren har passende tekniske foranstaltninger til at beskytte systemer og netværk, herunder beskyttelse af data under transmission og adgang via internettet, samt til at begrænse risikoen for uautoriseret adgang og/eller installering af skadelig kode.

Databehandleren anvender passende krypteringsteknologier og andre tilsvarende foranstaltninger i overensstemmelse med kravene i lovgivningen, godkendte standarder for kryptering af klassificeret information samt god databehandlingsskik.

I det omfang det er et krav i medfør af gældende national og international lovgivning, standarder vedrørende kryptering af klassificeret information eller god databehandlingsskik anvender databehandler krypteringsteknologier og andre tilsvarende foranstaltninger.

Transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af kryptering. Teknologiske løsninger til kryptering er tilgængelige og aktiveret. Firewall tillader kun krypteret datatrafik. Der foreligger formaliserede procedurer, der sikrer, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering baseret på en anerkendt algoritme.

Krypteringsnøgler administreres på vegne af den dataansvarlige og under kontrol af databehandleren, således at underdatabehandlere eller andre ikke har adgang til kundens data i klar tekst.

Firewall eller lignende tekniske foranstaltninger

Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem en VPN. Der skal foreligge administrativ adgang til at vedligeholde firewall-konfiguration og -regelsæt.

Antivirus

Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.

Sikkerhedskopiering

Databehandler skal have interne beredskabsprocedurer, der sikrer genetablering af services uden ugrundet ophold i tilfælde af driftsafbrydelser i henhold til hovedaftalen. Databehandleren sikrer backup.

Sikkerhedskopiering af konfigurationsfiler og data skal finde sted i et ubrudt forløb, således relevant data kan reetableres. Sikkerhedskopierne opbevares således, at de ikke hændeligt eller ulovligt (eks. ved brand, oversvømmelse, uheld, tyveri eller lignende) tilintetgøres, fortabes, forringes, kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.

Sikkerhedskopierne skal opbevares fysisk adskilt fra primære data og i et sikkerhedsgodkendt datacenter.

Databehandleren anvender redundant-miljø til sikring af adgang og kontinuerlig drift af softwareløsningen. Databehandleren sikrer at backup gemmes i sin fulde længde.

Anvendelse af hjemme/fjernarbejdspladser

Såfremt der foretages databehandling fra ad hoc og/eller hjemmearbejdspladser, sikre databehandleren at disse lever op til de sikkerhedsmæssige krav i denne Databehandleraftale med bilag og lovgivning i øvrigt.

Databehandler skal blandt andet opfylde følgende:

- At der anvendes krypteret forbindelse mellem ad hoc arbejdspladsen og Databehandlerens/Dataansvarliges netværk.
- Databehandleren har en intern instruks til egne medarbejdere vedrørende ad hoc og hjemmearbejdspladser.

Derudover skal databehandleren, hvis det er teknisk muligt anvende 2-faktor-autentifikation.

Logning

1. Der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger.
2. Databehandler sikrer, at sikkerhedsloggens omfang er defineret ud fra en af databehandleren udført risikovurdering.
3. Databehandler sikrer, at der er plads nok til at sikkerhedsloggene kan gemmes for perioden.
4. Databehandler sikrer, at der gennemføres løbende stikprøvekontroller af, at sikkerhedsloggene indeholder det forventede.
5. Databehandler afvejer sikkerhedsloggens slettefrister imellem muligheden for at analysere cyberangreb, understøtte efterforskning og hensynet til beskyttelses af fysiske personers rettigheder og frihedsrettigheder.

6. Databehandler sikrer, at opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod sletning og manipulation.
7. Databehandler sikrer at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret.
8. Databehandler sikrer logning i alle miljøer, hvor personoplysninger behandles.
9. Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder.
10. Ændringer i logopsætninger, herunder deaktivering af logning.
11. Ændringer i systemrettigheder til brugere.
12. Fejlede forsøg på log-on til systemer, databaser og netværk.

Brugeradministration

Databehandleren sikrer at løsningen understøtter hensigtsmæssig brugeradministration. Den dataansvarlige sikres mulighed for anvendelse af automatisk eller manuel brugeradministration.

Løsningen understøtter oprettelse, periodisk gennemgang og nedlæggelse af brugere. Den dataansvarlige kan alene varetage disse funktioner, men databehandleren kan bistå hermed såfremt det findes nødvendigt og indenfor et rimeligt omfang.

Instruktion af medarbejdere

Databehandleren sikrer at ansatte til stadighed er bekendt med og har tilstrækkelig uddannelse og instruktion om databehandlingens formål, politikker, arbejdsgange og om deres tavshedspligt.

Der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.

Informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler.

Der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.

Medarbejdere har underskrevet en fortrolighedsaftale i forbindelse med ansættelsen. Medarbejdere er blevet introduceret til:

- Informationssikkerhedspolitikken.
- Procedurer vedrørende databehandling, samt anden relevant information.

Der foreligger procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon osv. inddrages.

Der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt. Ansættelseskontrakten indeholder retningslinjer for, at medarbejdere er underlagt tavshedspligt efter ophørt samarbejde.

Databehandleren udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger.

Der foreligger dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning.

Medarbejderne hos databehandleren er forpligtet til at følge intern procedure om brug af support hos anvendte underdatabehandlere. Formålet med proceduren er at sikre korrekt brug af support og at forhindre anvendelsen af "follow the sun" support og dermed eliminere risikoen for tilgang af personoplysninger fra usikre tredjelande.

Underretning ved myndighedsudøvelse

Der er udarbejdet procedure for notifikation af den dataansvarlige ved eventuel direkte eller indirekte henvendelse fra myndigheder om udlevering af eller adgang til data.

Bortskaffelse af udstyr

Databehandleren skal have formelle processer med henblik på at sikre, at der sker en effektiv sletning af personoplysninger inden bortskaffelse af elektronisk udstyr.

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.

Databehandleren vil, så vidt muligt, og hvis imødekommelse forudsætter databehandlerens bistand, bistå den dataansvarlige med opfyldelsen af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder som fastlagt i kapitel III Europa-Parlamentets og Rådets forordning af 2016-04-27 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

Idet databehandleren i udgangspunktet alene behandler almindelige personoplysninger om den dataansvarliges brugere af softwareløsningen, har databehandleren gennemført sådanne tekniske og organisatoriske foranstaltninger, der tillader umiddelbar eksport af disse brugeres personoplysninger, og vil på den baggrund kunne bistå den dataansvarlige, ligesom den dataansvarlige frit kan råde over de af den dataansvarlige i øvrigt tilførte data.

Ved brud og hændelser, jf. pkt. 9.2 bistår databehandleren med følgende oplysninger:

- Fakta om det konstaterede brud (tid, sted, årsag)
- Hvornår bruddet startede, hvornår det blev opdaget og hvornår bruddet er standset
- Karakteren af bruddet på persondatasikkerheden, herunder om der er sket brud på fortrolighed, integritet og tilgængelighed
- Kategorierne og det omtrentlige antal berørte registrerede, hvis det er muligt
- Kategorierne af personoplysninger, hvis det er muligt
- Navn og kontaktoplysninger til kontaktpunkt, hvor yderligere oplysninger kan indhente

- Beskrivelse af de sandsynlige konsekvenser af bruddet
- Beskrivelse af foranstaltninger der er truffet, eller foreslås truffet som led i håndteringen af bruddet og dets mulige skadevirkninger

C.4 Opbevaringsperiode/sletterutine

Platformen konfigureres til at følge sletterutiner, som fastsættes af den dataansvarlige.

Ved ophør af aftalen skal databehandleren under alle omstændigheder enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af denne aftale – har ændret den dataansvarliges 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 på databehandlerens hjemsted eller de lokationer som anvendes af underdatabehandlerne og som er anført under pkt. B.1.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Hvis den dataansvarlige ikke i denne aftale eller efterfølgende giver dokumenteret instruks vedrørende overførsel af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af denne aftale at foretage sådanne overførsler, medmindre en sådan overførsel sker til en af de autoriseret underdatabehandlere nævnt i Bilag B. Overførselsgrundlag anvendes i henhold til Databeskyttelsesforordningens Kapitel V om overførsler af personoplysninger til tredjelande eller internationale organisationer. De specifikke overførselsgrundlag følger af gældende Bilag B.

C.7 Nærmere procedurer for den dataansvarliges tilsyn med den behandling, som foretages hos databehandleren

Databehandleren stiller sig mindst 1 gang årligt til rådighed for den dataansvarlige med henblik på dennes kontrol af databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og denne aftale.

Den dataansvarlige kan, mod betaling, anfægte rammerne for og/eller metoden i egenkontrollen og kan i sådanne tilfælde anmode om en ny egenkontrol under andre rammer og/eller under anvendelse af anden metode.

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. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendigt, men skal tilrettelægges så de er til mindst mulig gene for databehandleren.

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk og/eller skriftlig inspektion afholdes af den dataansvarlige selv. Databehandleren er forpligtet til at afsætte de ressourcer

(hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion, hvad enten denne er fysisk og/eller skriftlig.

Baseret på resultaterne af den dataansvarliges tilsyn med databehandleren, 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 denne aftale.

C.8 Nærmere procedurer for tilsynet med den behandling, som foretages hos eventuelle underdatabehandlere

Databehandleren skal årligt for egen regning udføre tilsyn med behandling af personoplysninger, som er overladt til underdatabehandlere. Tilsynet skal vedrøre underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og denne aftale.

Databehandlerens tilsyn med underdatabehandlere skal databehandleren tilrettelægges på en måde, så der opnås en tilstrækkelig indsigt i og kontrol af underdatabehandlernes overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og denne aftale.

Tilsynet kan bestå i indhentelse af en revisionserklæring eller inspektionsrapport fra en uafhængig tredjepart, inspektioner, og/eller skriftlige spørgsmål. Databehandleren har som udgangspunkt valgfrihed i forhold til metoden, hvormed der føres tilsyn med underdatabehandlere. Den dataansvarlige kan dog, såfremt der er rimeligt belæg herfor, anfægte rammerne for og/eller metoden af tilsynet og kan i sådanne tilfælde anmode om gennemførelsen af et nyt tilsyn under andre rammer og/eller under anvendelse af anden metode.

Den dataansvarlige kan – hvis det findes nødvendigt – vælge at bistå med kontrollen af underdatabehandleren. Dette kan blive aktuelt, hvis den dataansvarlige vurderer, at databehandlerens kontrol af 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 denne aftale.

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