Standardkontraktsbestemmelser

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

mellem

Kunden (som defineret i ”hovedaftalen”)

herefter ”den dataansvarlige”

og

IntraManager A/S
CVR 33966458
Helgavej 26
5230 Odense M
Danmark

herefter ”databehandleren”

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

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

1. Indhold

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 systemerne ”IntraManager Work” og ”IntraManager Board” behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

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

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

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

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

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

9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke af omfattet af Bestemmelserne.

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

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

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 medlemsstaternes[1] nationale ret og disse Bestemmelser.

1 Henvisninger til ”medlemsstat” i disse bestemmelser skal forstås som en henvisning til ”EØS medlemsstater”.

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.

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 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 generel skriftlig godkendelse fra den dataansvarlige.

3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst fjorten (14) dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller

medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

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

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

6. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

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.6.

5. Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

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. indsigtsretten
   d. retten til berigtigelse
   e. retten til sletning (”retten til at blive glemt”)
   f. retten til begrænsning af behandling
   g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
   h. retten til dataportabilitet
   i. retten til indsigelse
   j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:

   a. den dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

   b. den dataansvarliges forpligtelse til uden unødig forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder

   c. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)

d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

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

10. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest otteogfyrre (48) timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.

3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:

    a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger

    b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden

    c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

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.

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. 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 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 af "hovedaftalen".

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.

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via de kontaktpersoner, som fremgår af "hovedaftalen."

2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

Bilag A Oplysninger om behandlingen

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

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.

A.2. 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 hoster, viser, organiserer, modtager, indhenter, videresender, strukturerer, tilpasser, implementerer, søger, behandler, lagrer, gendanner, sletter, begrænser, logger, supporterer og fejlfinder personoplysninger om den dataansvarliges kunder og/eller medarbejdere på virksomhedens servere.

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

1. IntraManager Board:
   Navn, e-mailadresse, kundenummer/-navn

2. IntraManager Work:
   Navn, e-mailadresse, kundenummer/-navn, telefonnummer, adresse, CPR-nummer, medarbejdernummer, og bankoplysninger.

A.4. Behandlingen omfatter følgende kategorier af registrerede

- Den dataansvarliges kunder
- Den dataansvarliges medarbejdere

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

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

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Amazon Web Services EMEA SARL (AWS Europe)	B 186284	38 Avenue John F. Kennedy L-1855 Luxembourg Luxembourg (Datalokation: Greenhills Road, Tymon North, Dublin, Ireland)	AWS anvendes til hosting af løsningen, herunder lagring og behandling af data, og dermed behandles alle data i platformen, inklusive den dataansvarliges 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. Databehandleren benytter ikke supportaftale hos AWS, da denne ikke har samme beskyttelse.
Elastic AS	NO 994 812 564	Postboka 539 1373 Asker Norge	Elastic Cloud benyttes til serverhåndtering hos AWS. Elastic Cloud overholder bestemmelserne for SOC 2 & 3. Elastic er certificeret med bl.a. ISO 27001, 27017, 27018, ISAE 3000, mv. (https://www.elastic.co/trust/security-and-compliance)
inMobile ApS	31426472	Axel Kiers Vej 18 L 8270 Højbjerg Danmark	SMS Gateway (**NB**: Denne underdatabehandler benyttes udelukkende, hvis den dataansvarlige tilvælger databehandlerens service til system SMS)
Criipto ApS	35142207	Dronninggårds Alle 136 2840 Holte Danmark	MitID broker (**NB**: Denne underdatabehandler benyttes udelukkende, hvis den dataansvarlige tilvælger databehandlerens service til digital signering med MitID)

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

Den dataansvarliges skal senest fjorten (14) dage efter modtagelse af en anmodning fra databehandleren om tilføjelse eller erstatning af en underdatabehandler fremsende indsigelse mod valg og brug af den pågældende underdatabehandler til databehandleren. Ellers anses den valgte underdatabehandler som godkendt af den dataansvarlige.

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:

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, behandling, lagring, gendannelse, sletning, begrænsning, 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

Sikkerhedsniveauet skal afspejle:

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 registrerede.

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

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

<u>Informationssikkerhed</u>
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.

<u>Instruks</u>
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.

<u>Fysisk sikkerhed</u>
Databehandlerenen skal opretholde fysiske sikringsforanstaltninger til sikring af lokaliteter, som anvendes til behandling af personoplysninger, herunder opbevaring af personoplysninger omfattet af disse Bestemmelser mod uvedkommendes adgang og manipulation.

Databehandlerenen skal have passende fysiske 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 er afstemt med det aktuelle trusselbillede samt den følsomhed og mængde af persondata, som disse Bestemmelser 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 transmissionen 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. Databehandleren er forpligtet til at kryptere persondata, der behandles på vegne af den dataansvarlige i databehandlerens applikation inden der sker overførsel af personoplysninger til underdatabehandlere angivet i punkt B.1.

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 software-løsningen. 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 disse Bestemmelser 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 lever generelt 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 awarenesstræning 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 awarenesstræning.

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 i databeskyttelsesforordningen.

Idet databehandleren i udgangspunktet alene behandler almindelige personoplysninger om den dataansvarliges brugere af software-løsningen, 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. bestemmelse 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 indhentes
- 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. Den dataansvarliges personoplysninger slettes dog automatisk og senest tredive (30) dage efter ophør af Bestemmelserne.

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret den dataansvarlige oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

C.5 Lokalitet for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end 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 disse Bestemmelser eller efterfølgende giver dokumenteret instruks vedrørende overførsel af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler.

Databehandleren må ikke overføre personoplysninger til eller tilgå personoplysninger fra lande uden for EU/EØS eller internationale organisationer.

Såfremt databehandleren efterfølgende har modtaget dokumenteret skriftlig instruks fra den dataansvarlige, er databehandleren forpligtet til at sikre sig, at (i) en sådan overførsel er lovlig, herunder at der er et tilstrækkeligt beskyttelsesniveau for overførslen af personoplysninger, ved indgåelse af EU Kommissionens standardkontraktbestemmelser herom eller andet lovligt grundlag for overførslen skal iværksættes, (ii) alle nødvendige godkendelser er indhentet,

samt (iii) alle nødvendige meddelelser vedrørende den pågældende overførsel er blevet givet til den relevante tilsynsmyndighed. Databehandleren er forpligtet til at opdatere skemaet i bilag B.1 samt angive grundlaget for overførslen, jf. databeskyttelsesforordningens kapitel V.

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

Databehandleren stiller mindst en (1) gang årligt en egenkontrol 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 disse Bestemmelser.

Den dataansvarlige kan 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.

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 disse Bestemmelser.

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.

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

Databehandlerens tilsyn med underdatabehandlere skal 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 disse Bestemmelser.

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.

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 disse Bestemmelser.

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 disse Bestemmelser.

Bilag D Parternes regulering af andre forhold

D.1 Vederlag for etablering af yderligere sikkerhedsforanstaltninger

Parternes eventuelle regulering/aftale om vederlæggelse eller lignende i forbindelse med den dataansvarliges efterfølgende krav om etablering af yderligere sikkerhedsforanstaltninger end dem, som navnlig fremgår pkt. 6, C.2 og C.7 vil fremgå af parternes ”hovedaftale”.