Databehandleraftale udarbejdet efter Datatilsynets standardkontraktbestemmelser accepteret af Det Europæiske Databeskyttelsesråd

Standardkontraktsbestemmelser

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

mellem

De til enhver tid værende kunder
-
- -

CVR-nr.: -
herefter den "Dataansvarlige"

og

Dstny A/S
Skodsborgvej 305 D
2850 Nærum
DK
CVR-nr.: 28313160
herefter "Databehandleren"

der hver især er en "Part" og sammen udgør "Parterne"

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

Dette er version 22, sidst opdateret den 28.06.2022 14:12.

1. **Indholdsfortegnelse**

2. Præambel ..... (link)

3. Den dataansvarliges rettigheder og forpligtelser ..... (link)

4. Databehandleren handler efter instruks ..... (link)

5. Fortrolighed ..... (link)

6. Behandlingssikkerhed ..... (link)

7. Anvendelse af underdatabehandlere ..... (link)

8. Overførsel til tredjelande eller internationale organisationer ..... (link)

9. Bistand til den Dataansvarlige ..... (link)

10. Underretning om brud på persondatasikkerheden ..... (link)

11. Sletning og returnering af oplysninger ..... (link)

12. Revision, herunder inspektion ..... (link)

13. Parternes aftale om andre forhold ..... (link)

14. Ikrafttræden og ophør..... (link)

15. Kontaktpersoner hos den Dataansvarlige og Databehandleren ..... (link)

Bilag A Oplysninger om behandlingen ..... (link)

Bilag B Underdatabehandlere ..... (link)

Bilag C Instruks vedrørende behandling af personoplysninger ..... (link)

Bilag D Parternes regulering af andre forhold ..... (link)

Bilag E Standardkontraktbestemmelser ..... (link)

2. **Præambel**

2.1 Disse Bestemmelser fastsætter Databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysningerne på vegne af den Dataansvarlige.

2.2 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 ("GDPR").

2.3 I forbindelse med leveringen af mobiltelefoni, ip telefoni, PBX services, netværksinfrastruktur og relaterede services behandler Databehandleren personoplysninger på vegne af den Dataansvarlige i overensstemmelse med disse Bestemmelser.

2.4 Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem Parterne.

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

2.6 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.

2.7 Bilag B indeholder den Dataansvarliges betingelser for Databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den Datansvarlige har godkendt brugen af.

2.8 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.

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

2.10 Hvis standardkontraktbestemmelser som omhandlet i GDPR, artikel 46, stk. 2, litra c og d, udgør grundlag for overførsel af personoplysninger mellem den Dataansvarlige og Databehandleren som omhandlet i GDPR, kapitel V, er disse vedlagt i engelsk version som Bilag E og E1.

2.11 Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge Parter.

2.12 Disse Bestemmelser frigør ikke Databehandleren fra forpligtelser, som Databehandleren er pålagt efter GDPR eller enhver anden lovgivning.

2.13 For så vidt den Dataansvarlige reelt behandler de omhandlede personoplysninger på vegne af en anden ultimativt dataansvarlig, fungerer disse Bestemmelser som

underdatabehandleraftale, under hvilken den Dataansvarlige og Databehandleren skal referere til henholdvist databehandleren og under-databehandleren.

3. Den Dataansvarliges rettigheder og forpligtelser

3.1 Den Dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med GDPR (se GDPR, artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller EU/EØS-medlemsstaternes nationale ret og disse Bestemmelser.

3.2 Den Datansvarlige har ret og pligt til at træffe beslutning om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.

3.3 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

4.1 Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den Dataansvarlige, medmindre det kræves i henhold til EU-ret eller EU-/EØS-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.

4.2 Databehandleren underretter omgående den Dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med GDPR eller databeskyttelsesbestemmelser i anden EU-ret eller EU-/EØS-medlemsstaternes nationale ret.

5. Fortrolighed

5.1 Databehandleren må kun give adgang til personoplysninger, som behandles på den Dataansvarliges vegne, til personer, som er underlagt Databehandlerens instruktionsbeføjelser, og 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.

5.2 Databehandleren skal efter anmodning fra den Dataansvarlige kunne påvise, at de pågældende personer, som er underlagt Databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. Behandlingssikkerhed

6.1 GDPR, 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:

6.1.1 Pseudonymisering og kryptering af personoplysninger

6.1.2 evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

6.1.3 evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse

6.1.4 en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

6.2 Efter GDPR, 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.

6.3 Derudover skal Databehandleren bistå den Dataansvarlige med vedkommendes overholdelse af den Dataansvarliges forpligtelse efter GDPR, 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 GDPR, artikel 32, og al anden information, der er nødvendig for den Dataansvarliges overholdelse af sin forpligtelse efter GDPR, 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

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

7.2 Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af

disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den Dataansvarlige.

7.3 Databehandleren har den Dataansvarliges generelle godkendelse til brug af underdatabehandlre. Databehandleren skal skriftligt underrette den Dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 kalenderdages 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.

7.4 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 EU-/EØS-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 GDPR.

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

7.5 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.

7.6 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 GDPR, herunder særligt GDPR, artikel 79 og 82, over for den Dataansvarlige og Databehandleren, herunder underdatabehandleren.

8. Overførsel til tredjelande eller internationale organisationer

8.1 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 GDPR, kapitel V.

8.2 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 EU-/EØS-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.

8.3 Uden dokumenteret instruks fra den Dataansvarlige kan Databehandleren således ikke inden for rammerne af disse Bestemmelser:

8.3.1 overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation

8.3.2 overlade behandling af personoplysninger til en underdatabehandler i et tredjeland

8.3.3 behandle personoplysningerne i et tredjeland

8.4 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.

8.5 Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i GDPR, artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i GDPR, kapitel V, medmindre sådanne standardkontraktbestemmelser er vedhæftet i Bilag E.

9. Bistand til den Dataansvarlige

9.1 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 GDPR, kapitel III.

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

9.1.1 oplysningspligten ved indsamling af personoplysninger hos den registrerede

9.1.2 oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede

9.1.3 indsigtsretten

9.1.4 retten til berigtigelse

9.1.5 retten til sletning (”retten til at blive glemt”)

9.1.6 retten til begrænsning af behandling

9.1.7 underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling

9.1.8 retten til dataportabilitet

9.1.9 retten til indsigelse

9.1.10 retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

9.2 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:

9.2.1 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 Datatilsynet eller en anden kompetent tilsynsmyndighed, som måtte have kompetence, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

9.2.2 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

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

9.2.4 den Dataansvarliges forpligtelse til at høre Datatilsynet eller en anden kompetent tilsynsmyndighed, som måtte have kompetence 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.

9.3 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

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

10.2 Databehandlerens underretning til den Dataansvarlige skal om muligt ske straks og senest 24 timer efter det tidspunkt, hvor Databehandleren er blevet bekendt med bruddet på persondatasikkerheden, 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. GDPR, artikel 33.

10.3 I overensstemmelse med Bestemmelse 9.2.1 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:

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

10.3.2 de sandsynlige konsekvenser af bruddet på persondatasikkerheden

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

10.4 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

11.1 Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er Databehandleren forpligtet til at slette alle personoplysinger, der er blevet behandlet på vegne af den Dataansvarlige og bekræfte over for den Dataansvarlige, at oplysningerne er slettet, medmindre EU-retten eller EU-/EØS-medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

11.2 Følgende regler i EU-retten eller EU-/EØS-medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne efter ophør af tjenesterne vedrørende behandling af personoplysninger:

11.2.1 vi er påkrævet fortsat at opbevare oplysninger jf. logningsbekendtgørelsen og bogføringsloven efter Databehandler aftalens ophør.

Databehandleren forpligter sig til alene at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som disse regler foreskriver.

12. Revision, herunder inspektion

12.1 Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af GDPR, 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.

12.2 Procedurerne for den Dataansvarliges revisioner, herunder inspektioner, med

Databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7 .

12.3 Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivning 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

13.1 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 GDPR.

14. Ikrafttræden og ophør

14.1 Bestemmelserne er gældende mellem Parterne.

14.2 Begge Parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.

14.3 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.

14.4 Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den Dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge Parter.

14.5 Databehandleren er bundet af Bestemmelserne uden Parternes underskrift. Bestemmelserne indgås således uden fysiske/digitale underskrifter, idet Bestemmelserne er bindende i overensstemmelse med kravet i GDPR, artikel 28, stk. 3, 1. pkt.

15. Kontaktpersoner hos den Dataansvarlige og Databehandleren

15.1 Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

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

Kontaktoplysninger for den Dataansvarlige:
De til enhver gældende kontaktinformationer, som er modtaget ved indgåelsen af kontrakten og gennem det løbende samarbejde.

Kontaktoplysninger for Databehandleren:
Carsten Thomsen
dpo@dstny.dk

Bilag A Oplysninger om behandlingen

1. Formålet med Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige

1.1 Følgende formål ligger til grund for Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige:

a) Databehandleren leverer cloudstorage, -hosting, storage og backup til den Dataansvarlige.

Levering af en eller flere af følgende tjenester
- Mobiltelefoni
- IP telefoni
- Internet adgang
- MPLS
- PBX funktionalitet
- Integration mellem interne systemer og Telefoni
- Firewall og Sikkerhed
- Call center løsninger
- Voice recording
- Mødefunktionalitet online / telefonisk
- Relaterede services til ovenstående områder

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

2.1 Databehandleren bruger data fra den dataansvarlige for at kunne levere de ønskede services. Eksempelvis for at gøre det muligt at søge kollegaer frem i telefoni systemet (PBX) for at kunne se om kollegaen er ledig, eller for at muliggøre en ønsket integration.

Databehandleren gemmer de nødvendige oplysninger for at kunne fakturere de ønskede services, fx gemmes en CDR (Call Data Record) for hvert opkald der er foretaget for at sikre at faktureringen sker korrekt.

Herudover gemmes data jf. anden lovgivning, fx. logningsbekendtgørelsen.

2.2 Udvikling af apps og kundeportaler og levering af tjenester i relation hertil:
a) Levering af tjenester i form af it-arkitektur og udviklingskilder

3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

3.1 navn, telefonnummer, e-mail, adresse, IP-adresse, varierende personoplysninger, som kunden eller kundens kunder afgiver eller registrerer uden organisationens aktive behandling og identificering heraf, varierende personoplysninger, som registreres i forbindelse med levering af ydelsen, hvor disse ikke kan defineres præcist, brugernavn til et eller flere systemer, adgangskode til et eller flere systemer, fakturerings- og

bogføringsbilag, oplysninger om brugeres anvendte device, varierende personoplysninger på kunders systemer, som der gives adgang til

Faktureringsformater over opkald, sms og data (CDR filer)

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

4.1 nuværende ansatte, tidligere ansatte, kunders ansatte (hvor kunderne er organisationer)

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

5.1 Personoplysningerne behandles indtil ophør af tjenesterne vedrørende behandling af personoplysninger, hvorefter personoplysningerne slettes eller returneres i overensstemmelse med afsnit 11. Behandlingen foretages således så længe den eller de bagvedliggende kommercielle aftaler består.

Bilag B Underdatabehandlere

1. Godkendte underdatabehandlere

1.1 Ved Bestemmelsernes ikrafttræden har den Dataansvarlige godkendt brugen af følgende underdatabehandlere:

Generelle underdatabehandlere:

SuperOffice Danmark A/S (CVR-nr.:20020695)
Delta Park 46, st.
2665 Vallensbæk Strand
Danmark
Databehandling: Super Office behandler data for Dstny ved anvendelse af deres Customer Relationship Management løsning

Penneo (CVR-nr: 35633766)
Gyngemose Parkvej 50, 13.
2860 Søborg
Danmark
Databehandling: Penneo behandler data for Dstny ved anvendelse af deres digitale signeringsløsning

Microsoft Corporation (CVR-nr: 13612870)
One Microsoft Way
Redmond, WA 98052-6399
USA
Databehandling: Microsoft behandler data for Dstny ved anvendelse af deres dokumenthåndterings software samt Microsoft Teams

Zendesk's United States Representative:
Zendesk, Inc.
Attn: Hasani Caraway, General Counsel & Chief Privacy Officer
1019 Market Street
San Francisco, CA 94103, United States
Databehandling: Zendesk behandler data for Dstny ved anvendelse af deres ticketsystem til håndtering af kundeservice- og supporthenvendelser

Zendesk's European Representative:
Zendesk International Ltd
Attn: Rachel Tobin, AGC, EMEA & Global Privacy Counsel
55 Charlemont Place, Saint Kevin's, Dublin, D02 F985 Ireland
Databehandling: Zendesk behandler data for Dstny ved anvendelse af deres ticketsystem til håndtering af kundeservice- og supporthenvendelser

Produktspecifikke underdatabehandlere:

Telenor A/S (CVR-nr.:19433692)
Frederikskaj 8
2450 København SV

Danmark
Databehandling: Telenor behandler data for Dstny ved anvendelse Telenor mobiltelefoni

Mitel Networks, OCH A/S (CVRnr.:18936909)
Holmbladsgade 139
2300 København S
Danmark
Databehandling: Mitel behandler data for Dstny ved anvendelse af deres kommunikationsplatform Connect 3.0

MeetingZone AB
Södra Förstadsgatan 40A
21143
Malmø
Sverige
Databehandling: MeetingZone behandler data for Dstny ved anvendelse af produktet telefonmøder

OCH A/S c/o Telia Company Danmark A/S (CVRnr.: 18936909)
Holmbladsgade 139
2300
København S
Danmark
Databehandling: OCH A/S driver den fælles nummer database i Danmark, og er det fælles referencepunkt for udveksling af oplysninger om porterede telefonnumre i Danmark. Dstny anvender OCH i forbindelse med import og export af telefonnumre i Danmark

Dateltek ApS (CVRnr.: 31060559)
Birkevej 4
4640
Faxe
Danmark
Databehandling: Dateltek behandler data for Dstny ved anvendelse af deres ICH-system til håndtering af nummerporteringsprocesser. ICH-systemet anvendes kun ved numre der skal på Telenors netværk

NPS.TODAY ApS (CVRnr.: 36464917)
Bredgade 41, 2. tv.
1260 København K
Danmark
Databehandling: NPS.TODAY behandler data for Dstny ved anvendelse af produktet Net Promoter Score - SMS Survey

Revolvo ApS (CVRnr.: 35250379)
Herredsvejen 2
3400 Hillerød
Danmark
Databehandling: Revolvo ApS behandler data for Dstny ved anvendelse af produktet

Connect Pop-up (integrationsservice) og Integration Middleware Services.

Scantalk ApS (CVRnr.: 26717078)
Farum Gydevej 65, 1
3520 Farum
Danmark
Databehandling: Scantalk Aps behandler data for Dstny ved anvendelse af produktet Ekstern mobilstatus og Connect 3.0 - Ekstern mobilbruger licens.

1.2 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

1. Behandlingens genstand/instruks

1.1 Leverer Telefoni, netværk og PBX funktionalitet til den Data ansvarlige.

2. Behandlingssikkerhed

2.1 Sikkerhedsniveauet skal afspejle:

Databehandleren skal etablere et passende sikkerhedsniveau under hensyntagen til behandlingens karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

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:

Teknisk sikkerhed: Tilgængelighed og robusthed
Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende tilgængelighed og robusthed:

a) Kun autoriserede medarbejdere har adgang til Databehandlerens eventuelle egne servere.
b) Serverrum har røgalarm og brandslukkere.
c) Serverrum har airconditionssystem.
d) Der er regler og retningslinjer for backup af data.
e) Der er regler og retningslinjer for genskabelse af data fra backup.
f) Der foretages regelmæssig backup (enten egen eller hos leverandør).
g) Der anvendes uafbrudt strømforsyning (UPS).
h) Temperatur og luftfugtighed overvåges i serverrum.
i) Databehandlerens har procedurebeskrivelse(r) for brud på persondatasikkerheden, der minimum tages op til revidering årligt.
j) Aktiv alarmering ved forsøg på uautoriseret adgang til serverrum og/eller behandlingssystemer og data.

3. Bistand til den dataansvarlige

3.1 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:

3.1.1 Hvis den Dataansvarlige modtager en anmodning om udøvelsen af personers rettigheder efter gældende databeskyttelseslovgivning, og korrekt besvarelse af

anmodningen kræver bistand fra Databehandleren, skal Databehandleren bistå den Dataansvarlige med nødvendige og relevante oplysninger og dokumentation samt passende tekniske og organisatoriske sikkerhedsforanstaltninger.

3.1.2 Hvis den Dataansvarlige vil have hjælp til at besvare en anmodning fra en registreret person, skal den Dataansvarlige sende skriftlig anmodning herom til Databehandleren, og Databehandleren skal som svar herpå levere den nødvendige hjælp eller dokumentation hurtigst muligt og senest 7 kalenderdage efter modtagelse af anmodning herom.

3.1.3 Hvis Databehandleren modtager en anmodning om udøvelsen af personers rettigheder efter gældende databeskyttelseslovgivning fra andre end den Dataansvarlige, og anmodningen vedrører personoplysninger behandlet på vegne af den Dataansvarlige, skal Databehandleren uden unødvendig forsinkelse videresende anmodningen til den Dataansvarlige.

4. Opbevaringsperiode/sletterutine

4.1 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 sit oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til Bestemmelserne.

5. Lokalitet for behandling

5.1 Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den Dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

Hos Databehandleren egne hovedkontorer og på hovedkontorerne for godkendte underdatabehandlere, som angivet i bilag B.

6. Instruks vedrørende overførsel af personoplysninger til tredjelande

6.1 Personoplysningerne behandles kun af Databehandleren på de lokationer, som er beskrevet i Bestemmelse C.5.
Databehandleren overfører som led i opfyldelse af Hovedaftalen Personoplysningerne til følgende lande: USA.

6.2 Når Personoplysninger i forbindelse med disse Bestemmelser, og den underliggende aftale, overføres til tredjelande som ikke har været genstand for en afgørelse om

tilstrækkelig sikkerhed efter Artikel 45 i GDPR, skal det lovlige overførselsgrundlang være standardkontraktsbestemmelser efter Artikel 46(1) og 46(2)(c) i GDPR.

6.3 I det omfang personoplysninger overføres til tredjelande, som ikke har været genstand for en afgørelse om tilstrækkelig sikkerhed efter Artikel 45 i GDPR, hvor begge parter er dataansvarlige, og denne overførsel ikke er omfattet af en eller flere af undtagelsesreglerne i artikel 49, skal retsgrundlaget ligeledes være standardkontraktbestemmelser som indeholdt i bilag E.

6.4 Hvis den Dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsel af personoplysninger til et tredjeland, er Databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler.

6.5 Overførsel af personoplysninger må i alle tilfælde kun ske som foreskrevet i Bestemmelserne, på den Dataansvarliges instruks, og i det omfang det er tilladt i medfør af databeskyttelseslovgivningen.

6.6 Når Databehandleren, i overensstemmelse med disse bestemmelser, overfører personoplysninger omfattet af aftalen videre til underdatabehandlere eller selvstændigt dataansvarlige i tredjelande, skal Databehandleren selv sørge for at sikre, at overførslen overholder kapitel 5 i Forordning 2016/679.

7. Procedurer for den Dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til Databehandleren

7.1 Databehandleren skal på skriftlig anmodning dokumentere overfor den Dataansvarlige, at Databehandleren

7.1.1 overholder sine forpligtelser efter denne Databehandleraftale og Instruksen, og

7.1.2 overholder bestemmelserne i GDPR, for så vidt angår personoplysningerne, som behandles på den Dataansvarliges vegne.

7.2 Databehandlerens dokumentation i henhold til afsnit C.7.1 skal sendes til den Dataansvarlige inden for rimelig tid efter modtagelsen af anmodningen herom.

7.3 Databehandleren skal som dokumentation for løbende overholdelse af Bestemmelserne stille egenkontrolrapporter til rådighed for den Dataansvarlige. Disse egenkontrolrapporter skal som minimum udarbejdes én gang årligt og skal følge principperne og kontrolmålene i revisionsstandarden ISAE 3000 som udarbejdet af FSR-danske revisorer og Datatilsynet (og/eller alternativt andre internationalt anerkendte standarder såsom ISO/IEC 27701:2019). Egenkontrolrapporterne kan efter den Dataansvarliges valg ske ved den Dataansvarliges informationsindsamling og skal underskrives af Databehandlerens ledelse. For at dække den Dataansvarliges behov for indsigt og sikring af Databehandlerens betryggende behandling af Personoplysningerne, skal Databehandleren hver 18. måned foretage revision (audit) af Databehandlerens overholdelse af Databehandleraftalen, herunder de angivne

implementerede sikkerhedsforanstaltninger, ved ekstern(e) uafhængig(e) tredjepart(er) og fremsende fuldstændig protokollat herfor til den Dataansvarlige.

7.4 Uanset afsnit C.7.3 skal Databehandleren derudover give mulighed for og bidrage til revisioner og inspektioner hver 12. måned, der foretages af revisorer udpeget af den Dataansvarlige, de offentlige myndigheder i Danmark eller af anden kompetent jurisdiktion, i det omfang det er nødvendigt for at kontrollere, at Databehandleren overholder Bestemmelserne og gældende databeskyttelseslovgivning. Den pågældende revisor skal være underlagt fortrolighed i henhold til lov eller aftale. Den Dataansvarlige skal skriftligt varsle revisioner som beskrevet med 30 kalenderdage.

Bilag D Parternes regulering af andre forhold

1. Bemærkning til proceduren for den Dataansvarliges revisioner i bilag C punkt 7

1.1 I henhold til vores dokumentation for overholdelse af Databehandler aftalen henviser til proceduren i bilag C punkt 7.3, da det i praksis ikke vil være muligt at komme på et fysisk tilsyn af vores datacentre.

2. Opdatering af Databehandleraftalen

2.1 Det er altid den nyeste version af databehandleraftalen, der er gældende imellem parterne, se https://ipvision.dk/databehandleraftale.

Databehandleren forbeholder sig retten til løbende at foretage ændringer i, herunder præciseringer af, aftalen. Disse ændringer vil typisk være et resultat af nye anbefalinger fra f.eks. Datatilsynet eller EU-Kommissionen samt ændringer i praksis og lovgivning på området.

Den Dataansvarlige opfordres derfor til at skrive sig op til at modtage notifikationer, når der sker ændringer i aftalen:
https://ipvision.dk/databehandleraftale

Den Dataansvarlige har efter modtagelse af en notifikation om en ændring, 14 hverdage til at gøre indsigelse, hvis ændringen med rimelighed ikke kan accepteres.

Nærværende bestemmelse gælder ikke for så vidt angår ændringer i brugen af underdatabehandlere, som er reguleret i aftalens afsnit 7.

Bilag E Standard Contractual Clauses for the transfer of personal data to third countries

Note: *These Standard Contractual Clauses figure in English within the context of a Data Processing Agreement in Danish. Where reference is made to the Data Processing Agreement, and its Appendices, the standard translation of terms shall apply; Appendix to mean "Bilag", Data Processing Agreement to mean Databehandleraftale, and so forth.*

Regarding transfer of personal data to the Data Processor in a third country that does not ensure adequate level of data protection, and according to article 46 in the General Personal Data Regulation, the Parties have agreed to the following Standard Contract Clauses in order to provide appropriate safeguards regarding the protection of privacy and the fundamental rights and freedoms of natural persons in relation to the disclosure of personal data by the data exporter in this Agreement, including Appendix A, B, C and D.

Unless otherwise provided in this Appendix E, words and phrases with a capital letter have the same meaning as set out in the Agreement, including Appendix A, Appendix B, Appendix C and Appendix D.

The Standard Contractual Clauses regulate all transfers between the Parties, conducted in fulfillment of the services specified in Clause 2.3 of the Data Processing Agreement, to third countries outside the EU/EEA, not subject to an adaquacy decison on the basis of Article 45 of Regulation (EU) 2016/679, insofar as none of the derogations for a specific situation referred to in Article 49 of Regulation (EU) 2016/679 apply.

The appropriate modules take effect accordingly:

Module One applies to transfers of personal data between the Parties for which both Parties are controllers, whether jointly or independently.
Module Two applies to transfers of personal data from the Data Controller to the Data Processor, where the Data Controller is not acting as a processor for another ultimate data controller.
Module Three applies to transfers of personal data from the Data Controller to the Data Processor, where the Data Controller is acting as a data processor on behalf of another ultimate data controller.
Module Four applies to transfers of personal data from the Data Processor to the Data Controller, where the Data Controller is based in a third country outside the EU / EEA, not subject to an adaquacy decison on the basis of article 45 of Regulation (EU) 2016/679.

SECTION I

1. Purpose and scope

1.1 The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

1.2 The Parties:

1.2.1 the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

1.2.2 the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

1.3 These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

1.4 The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

2. Effect and invariability of the Clauses

2.1 These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

2.2 These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

3. Third-party beneficiaries

3.1 Data subjects may invoke and enforce these Clauses, as third-party beneficiaries,

against the data exporter and/or data importer, with the following exceptions:

3.1.1 Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

3.1.2 Clause 8 – Module One: Clause 8.5.5 and Clause 8.9.2; Module Two: Clause 8.1.2, 8.9.1, 8.9.3, 8.9.4 and 8.9.5; Module Three: Clause 8.1.1, 8.1.3 and 8.1.4 and Clause 8.9.1, 8.9.3, 8.9.4, 8.9.5, 8.9.6 and 8.9.7; Module Four: Clause 8.1.2 and Clause 8.3.2;

3.1.3 Clause 9 – Module Two: Clause 9.1, 9.3, 9.4 and 9.5; Module Three: Clause 9.1, 9.3, 9.4 and 9.5;

3.1.4 Clause 12 – Module One: Clause 12.1 and 12.4; Modules Two and Three: Clause 12.1, 12.4 and 12.6;

3.1.5 Clause 13;

3.1.6 Clause 15.1.3, 15.1.4 and 15.1.5;

3.1.7 Clause 16.5;

3.1.8 Clause 18 – Modules One, Two and Three: Clause 18.1 and 18.2; Module Four: Clause 18.

3.2 Paragraph 3.1 is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

4. Interpretation

4.1 Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

4.2 These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

4.3 These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

5. Hierarchy

5.1 In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

5.2 Paragraf 5.1 not withstanding, insofar as the contradiction with a later agreement between the parties strictly concerns the optional content of paragraf 9.1, and/or the Appendix, the later agreement shall prevail, provided this does not interfere with the function of the Clauses as sufficient safeguards pursuant to Article 46(1) and Article

46(2)(c) of Regulation (EU) 2016/679.

6. Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

7. Docking Clause (NOT IN EFFECT)

7.1 ~~An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.~~

7.2 ~~Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.~~

7.3 ~~The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.~~

SECTION II – OBLIGATIONS OF THE PARTIES

8. Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE ONE: Transfer controller to controller

8.1 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

8.1.1 where it has obtained the data subject's prior consent;

8.1.2 where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

8.1.3 where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 **Transparency**

8.2.1 In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;
(ii) of the categories of personal data processed;
(iii) of the right to obtain a copy of these Clauses;
(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

8.2.2 Paragraph 8.2.1 shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

8.2.3 On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.2.4 Paragraphs 8.2.1 to 8.2.3 are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.2.5 Insofar as the content matter of these Clauses and the Appendix is determined by reference to other agreements betweeen the parties, the relevant parts of such other agreements are likewise subject to the provisions of transparency, contained in paragraphs 8.2.1 to 8.2.4.

8.3 **Accuracy and data minimisation**

8.3.1 Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

8.3.2 If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

8.3.3 The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 **Storage limitation**

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation[2] of the data and all back-ups at the end of the retention period.

8.5 **Security of processing**

8.5.1 The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

8.5.2 The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

8.5.3 The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.5.4 In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

8.5.5 In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain

(i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned);
(ii) its likely consequences;
(iii) the measures taken or proposed to address the breach;
(iv) the details of a contact point from whom more information can be obtained.

To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

8.5.6 In case of a personal data breach that is likely to result in a high risk to the rights

and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph 8.5.5, points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

8.5.7 The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 **Onward transfers**

The data importer shall not disclose the personal data to a third party located outside the European Union[3] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 **Processing under the authority of the data importer**

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 **Documentation and compliance**

8.9.1 Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

8.9.2 The data importer shall make such documentation available to the competent supervisory authority on request.

MODULE TWO: Transfer controller to processor

8.1 **Instructions**

8.1.1 The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

8.1.2 The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 **Transparency**

8.3.1 On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data

subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3.2 Insofar as the content matter of these Clauses and the Appendix is determined by reference to other agreements betweeen the parties, the relevant parts of such other agreements are likewise subject to the provisons of transparency contained in paragraph 8.3.1.

8.4 **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14.5 to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14.1.

8.6 **Security of processing**

8.6.1 The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In

complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

8.6.2 The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.6.3 In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

8.6.4 The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[4] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation

8.9 **Documentation and compliance**

8.9.1 The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

8.9.2 The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

8.9.3 The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

8.9.4 The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

8.9.5 The Parties shall make the information referred to in paragraphs 8.9.2 and 8.9.3, including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 **Instructions**

8.1.1 The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

8.1.2 The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

8.1.3 The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

8.1.4 The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter[5].

8.2 **Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 **Transparency**

8.3.1 On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.3.2 Insofar as the content matter of these Clauses and the Appendix is determined by reference to other agreements betweeen the parties, the relevant parts of such other agreements are likewise subject to the provisons of transparency contained in paragraph 8.3.1.

8.4 **Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 **Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14.5 to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14.1.

8.6 **Security of processing**

8.6.1 The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

8.6.2 The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.6.3 In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely

consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

8.6.4 The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[6] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation

8.9 **Documentation and compliance**

8.9.1 The data importer shall promptly and adequately deal with enquiries from the

data exporter or the controller that relate to the processing under these Clauses.

8.9.2 The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

8.9.3 The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

8.9.4 The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

8.9.5 Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

8.9.6 The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

8.9.7 The Parties shall make the information referred to in paragraphs 8.9.2 and 8.9.3, including the results of any audits, available to the competent supervisory authority on request.

MODULE FOUR: Transfer processor to controller

8.1 **Instructions**

8.1.1 The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

8.1.2 The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

8.1.3 The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

8.1.4 After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or

return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 **Security of processing**

8.2.1 The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data[7], the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

8.2.2 The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph 8.3.1. In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

8.2.3 The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 **Documentation and compliance**

8.3.1 The Parties shall be able to demonstrate compliance with these Clauses.

8.3.2 The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

9. Use of sub-processors

MODULE TWO: Transfer controller to processor

9.1 The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

9.2 Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[8] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

9.3 The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

9.4 The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

9.5 The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

9.1 The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

9.2 Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[9] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

9.3 The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

9.4 The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

9.5 The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

10. Data subject rights

MODULE ONE: Transfer controller to controller

10.1 The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.[10] The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

10.2 In particular, upon request by the data subject the data importer shall, free of charge:

10.2.1 provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 11.3.1;

10.2.2 rectify inaccurate or incomplete data concerning the data subject;

10.2.3 erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

10.3 Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

10.4 The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly

affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

10.4.1 inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

10.4.2 implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

10.5 Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

10.6 The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

10.7 If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

MODULE TWO: Transfer controller to processor

10.1 The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

10.2 The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

10.3 In fulfilling its obligations under paragraphs 10.1 and 10.2, the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

10.1 The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

10.2 The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects'

requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

10.3 In fulfilling its obligations under paragraphs 10.1 and 10.2, the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

11. Redress

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

11.1 The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

11.2 In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

11.3 Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

11.3.1 lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

11.3.2 refer the dispute to the competent courts within the meaning of Clause 18.

11.4 The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

11.5 The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

11.6 The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with

applicable laws.

MODULE FOUR: Transfer processor to controller

11.1 The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

12. Liability

MODULE ONE: Transfer controller to controller

MODULE FOUR: Transfer processor to controller

12.1 Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

12.2 Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

12.3 Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

12.4 The Parties agree that if one Party is held liable under paragraph 12.3, it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

12.5 The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

12.1 Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

12.2 The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

12.3 Notwithstanding paragraph 12.2, the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these

Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

12.4 The Parties agree that if the data exporter is held liable under paragraph 12.3 for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

12.5 Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

12.6 The Parties agree that if one Party is held liable under paragraph 12.5, it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

12.7 The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

13. Supervision

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

13.1 [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

13.2 The data importer agrees to submit itself to the jurisdiction of and cooperate with the

competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

14. Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller*(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

14.1 The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

14.2 The Parties declare that in providing the warranty in paragraph 14.1, they have taken due account in particular of the following elements:

14.2.1 the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

14.2.2 the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards [12];

14.2.3 any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the

country of destination.

14.3 The data importer warrants that, in carrying out the assessment under paragraph 14.2, it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

14.4 The Parties agree to document the assessment under paragraph 14.2 and make it available to the competent supervisory authority on request.

14.5 The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph 14.1, including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph 14.1. [For Module Three: The data exporter shall forward the notification to the controller.]

14.6 Following a notification pursuant to paragraph 14.5, or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16.4 and 16.5 shall apply

15. Obligations of the data importer in case of access by public authorities

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller*(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

15.1 **Notification**

15.1.1 The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

15.1.1.1 receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

15.1.1.2 becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer. [For Module Three: The data exporter shall forward the notification to the controller.]

15.1.2 If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

15.1.3 Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the notification to the controller.]

15.1.4 The data importer agrees to preserve the information pursuant to paragraphs 15.1.1 to 15.1.3 for the duration of the contract and make it available to the competent supervisory authority on request.

15.1.5 Paragraphs 15.1.1 to 15.1.3 are without prejudice to the obligation of the data importer pursuant to Clause 14.5 and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 **Review of legality and data minimisation**

15.2.1 The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data

importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14.5.

15.2.2 The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

15.2.3 The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

16. Non-compliance with the Clauses and termination

16.1 The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

16.2 In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14.6.

16.3 The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

16.3.1 the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph 16.2 and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

16.3.2 the data importer is in substantial or persistent breach of these Clauses; or

16.3.3 the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

16.4 [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph 16.3 shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph 16.3 shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law

16.5 Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679

17. Governing law

17.1 These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Denmark.

18. Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

18.1 Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

18.2 The Parties agree that those shall be the courts of Denmark.

18.3 A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

18.4 The Parties agree to submit themselves to the jurisdiction of such courts.

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts of Denmark.

Notes:

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

[2] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[4] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[5] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

[6] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

[7] This includes whether the transfer and further processing involves personal data

revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

[8] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[9] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[10] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

[12] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Appendix E1 Annexes to Standard Contractual Clauses for the transfer of personal data to third countries

EXPLANATORY NOTE: Where information is available in the data processing agreement and associated appendices, references will be made. Followingly, parts of the dataprocessing agreement and appendices, or summaries thereof, may be required to be disclosed to the data subjects on request, pursuant to the provisoions of transparency contained in these Standard Contractual Clauses.

ANNEX I

A. LIST OF PARTIES

A.1 Data exporter:
Name:
Dstny A/S
Address:
Skodsborgvej 305 D, 2850 Nærum, DK
Contact person's name, position and contact details:
De til enhver gældende kontaktinformationer, som er modtaget ved indgåelsen af kontrakten og gennem det løbende samarbejde.

Role (controller/processor):
Processor

Activities relevant to the data transferred under these Clauses:
Reference is made to the Data Processing Agreement.

Signature and date:
Reference is made to the Data Processing Agreement to which these Clauses form an appendix.

A.2 Data importer:
Name:
De til enhver tid værende kunder
Address:
-, - -,
Contact person's name, position and contact details:
De til enhver gældende kontaktinformationer, som er modtaget ved indgåelsen af kontrakten og gennem det løbende samarbejde.

Role (controller/processor):
Controller

Activities relevant to the data transferred under these Clauses:
Reference is made to the Data Processing Agreement.

Signature and date:
Reference is made to the data processing agreement to which these Clauses form an appendix.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:
Reference is made to Appendix A, paragraf 4 of the data processing agreement.

Categories of personal data transferred:
Reference is made to Appendix A, paragraf 3 of the data processing agreement.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved:
No sensitive data is transferred.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):
The transfer from controller to controller under these clauses will not be continuous, but of a one-off nature.

Nature of the processing:
Reference is made to Appendix A, paragraf 2 of the data processing agreement.

Purpose(s) of the data transfer and further processing:
Reference is made to Appendix A, paragraf 1 of the data processing agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:
Reference is made to Appendix C, paragraf 4 of the data processing agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:
Reference is made to Appendix B of the data processing agreement.

Subject matter
Reference is made to Appendix B of the data processing agreement.

Nature of processing
Reference is made to Appendix B of the data processing agreement.

Duration of processing
Reference is made to the data processing agreement.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13:
Reference is made to the data processing agreement.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Technical and organisational measures taken by the Data Processor:
Reference is made to Appendix C, Clause 2 of the data processing agreement.

Technical and organisational measures taken by sub-processors:
Persuant to Clause 7.4 of the Data Processing Agreement, sub-processors must supply equivalent technical and organisational protective meassures, equivalent to those undertaken by the data processor.