

Databehandlertaftale

Databehandleraftale

Version 8, 8.10.2026 13:03

FDE A/S ("Organisationen")

Lyren 1, Bovmark

6330 Padborg

DK

CVR: 15452986

Indholdsfortegnelse

1. Parterne
2. Præambel
3. Den Dataansvarliges rettigheder og forpligtelser
4. Databehandleren handler efter instruks
5. Fortrolighed
6. Behandlingssikkerhed
7. Anvendelse af underdatabehandlere
8. Overførsel til tredjelande eller internationale organisationer
9. Bistand til den Dataansvarlige
10. Underretning om brud på persondatasikkerheden
11. Sletning og returnering af oplysninger
12. Revision, herunder inspektion
13. Parternes aftale om andre forhold
14. Ikrafttræden og ophør
15. Kontaktpersoner hos den Dataansvarlige og Databehandleren
16. Bilag A - Oplysninger om behandlingen
17. Bilag B - Underdatabehandlere
18. Bilag C - Instruks vedrørende behandling af personoplysninger
19. Bilag D - Parternes regulering af andre forhold
20. Bilag E - Standard Contractual Clauses for the transfer of personal data to third countries

1. Parterne

Databehandlersaftale udarbejdet efter Datatilsynets standardkontraktbestemmelser accepteret af Det Europæiske Databeskyttelsesråd i henhold til artikel 28, stk. 3, i forordning 2016/679 (GDPR) med henblik på databehandlerens behandling af personoplysninger

mellem

kunden, herefter den "Dataansvarlige"

og

FDE A/S
Lyren 1, Bovmark
6330 Padborg
DK
CVR: 15452986

herefter "Databehandleren"

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

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

2. Præambel

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

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").

I forbindelse med leveringen af Databehandlersaftale for de enhver tid værende kunder behandler Databehandleren personoplysninger på vegne af den Dataansvarlige i overensstemmelse med disse Bestemmelser.

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

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

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.

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

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.

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

Hvis standardkontraktbestemmelser som omhandlet i GDPR, artikel 46, stk. 1, litra c og d, udgør grundlag for overførsel af personoplysninger mellem den Dataansvarlige og Databehandleren til tredjelande som omhandlet i GDPR, kapitel V, er disse vedlagt i engelsk version som Bilag E og E1.

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

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

3. Den Dataansvarliges rettigheder og forpligtelser

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.

3.1 Den Dataansvarliges beslutningskompetence

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

3.2 Behandlingsgrundlag for personoplysninger

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

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.

4.1 Underretning om ulovlige instrukser

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 Adgang til personoplysninger og fortrolighed

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 Dokumentation for tavshedspligt

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 Tekniske og organisatoriske sikkerhedsforanstaltninger

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:

1. Pseudonymisering og kryptering af personoplysninger
2. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
3. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
4. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

6.2 Databehandlerens risikovurdering

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 Bistand til overholdelse af behandlingssikkerhed

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

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).

7.1 Generel skriftlig godkendelse

Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den Dataansvarlige.

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

7.2 Forpligtelser for underdatabehandlere

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.

7.3 Dokumentation for underdatabehandleraftaler

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.

7.4 Den dataansvarlige som begunstiget tredjemand

Databehandleren skal i sin aftale med underdatabehandleren indføre den Dataansvarlige som begunstiget tredjemand, således at den Dataansvarlige i tilfælde af at Databehandleren faktisk eller retligt set er ophørt med at eksistere eller i tilfælde af Databehandlerens konkurs, har ret til at opsig underdatabehandleraftalen og instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

7.5 Ansvar for underdatabehandlere

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 Instruks ved overførsel til tredjelande

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.

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

1. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
2. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
3. behandle personoplysningerne i et tredjeland

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.

Disse Bestemmelser skal ikke forveksles med standardkontraktbestemmelser 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.

8.2 Underretning ved retligt krav om overførsel

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.

9. Bistand til den Dataansvarlige

9.1 Bistand ved registreredes rettigheder

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:

1. oplysningspligten ved indsamling af personoplysninger hos den registrerede
2. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
3. indsigtsretten
4. retten til berigtigelse
5. retten til sletning ("retten til at blive glemt")
6. retten til begrænsning af behandling
7. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
8. retten til dataportabilitet
9. retten til indsigelse
10. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

9.2 Bistand ved sikkerhedsbrud og konsekvensanalyser

I tillæg til Databehandlerens forpligtelse til at bistå den Dataansvarlige i henhold til Bestemmelse 6.3, bistår Databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for Databehandleren, den Dataansvarlige med:

1. den Dataansvarliges forpligtelse til uden unødigt forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder
2. den Dataansvarliges forpligtelse til uden unødigt forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder
3. den Dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)
4. den Dataansvarliges forpligtelse til at høre Datatilsynet, 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 Fastlæggelse af bistand i bilag C

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

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

10.1 Frist for underretning om brud

Databehandlerens underretning til den Dataansvarlige skal om muligt ske traks og senest 24 timer efter det tidspunkt, hvor databehandleren 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.

10.2 Bistand ved anmeldelse af brud

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:

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
2. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
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.

Parterne skal i [Bilag D](#) 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 Sletning af personoplysninger ved ophør

Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er Databehandleren forpligtet til at slette alle personoplysninger, 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 Opbevaring i henhold til lovgivning

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

1. Sletning følger reglerne i bogføringsloven, medmindre andet er angivet i kontrakten med kunden.

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 Bistand til revision og inspektion

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 Procedurer for revision og inspektion

Procedurerne for den Dataansvarliges revisioner, herunder inspektioner, med Databehandleren og underdatabehandlere er nærmere angivet i Bilag [C.7](#).

12.3 Adgang for tilsynsmyndigheder

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

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 Ikrafttræden

Bestemmelserne er bindende mellem Parterne.

14.2 Genforhandling

Begge Parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller u hensigtsmæssigheder i Bestemmelserne giver anledning hertil.

14.3 Varighed

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 Opsigelse

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 Bindende virkning

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

Parterne kan kontakte hinanden via nedenstående kontaktpersoner. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

Kontaktoplysninger for den Dataansvarlige:

Kontaktoplysninger for den Dataansvarlige følger af Hovedaftalen.

Kontaktoplysninger for Databehandleren:

Kontaktoplysninger for Databehandleren følger af Hovedaftalen.

16. Bilag A - Oplysninger om behandlingen

16.1 Formålet med Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige

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

Behandlingen af personoplysninger foretages herudover med henblik på opfyldelsen af følgende formål:

De omfattede Personoplysninger behandles med det formål at opfylde de i Hovedaftalen nævnte kommercielle ydelser

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

De omfattede Personoplysninger behandles med det formål at opfylde de i Hovedaftalen nævnte kommercielle ydelser

16.3 Typer af personoplysninger

Behandlingen omfatter følgende typer af personoplysninger om de registrerede:

- Adgangskode til et eller flere systemer
- Adresse
- Bankoplysninger (kortoplysninger eller kontooplysninger)
- Brugernavn til et eller flere systemer
- CPR-nummer
- E-mail
- Fakturerings- og bogføringsbilag
- Fødselsdato
- Navn
- Oplysninger om brugeres anvendte device
- Telefonnummer
- Varierende personoplysninger, som kunden eller kundens kunder afgiver eller registrerer uden organisationens aktive behandling og identificering heraf

16.4 Kategorier af registrerede

Behandlingen omfatter følgende kategorier af registrerede:

- Kunder (hvor kunderne er forbrugere eller enkeltmandsorganisationer)
- Kunders ansatte (hvor kunderne er organisationer)
- Kunders kunder og deres ansatte (eksempelvis til CRM-leverandører)
- Leverandører (hvor leverandørerne er personer eller enkeltmandsorganisationer)
- Nuværende ansatte
- Samarbejdspartnere (hvor samarbejdspartnerne er personer eller enkeltmandsorganisationer)
- Samarbejdspartneres ansatte (hvor samarbejdspartnerne er organisationer)

16.5 Varighed

Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden.

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.

17. Bilag B - Underdatabehandlere

17.1 Godkendte underdatabehandlere

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

ITD Holding A/S, Lyren 1, 6330 Padborg. ITD Holding varetager driften af Databehandlerens IT og hosting. Lokale agenter og VAT handlers. Disse tredjeparter er udspecificeret og accepteret af hver kunde i forbindelse med hver enkelt kundes accept og underskrift af fuldmagt til den lokale agent eller VAT handler. De Dataansvarlige anerkender - uanset eventuelle andre bestemmelser i denne Databehandleraftale med andet indhold - at der ved accept og underskrift af fuldmagt også gives tilladelse til brug af samme tredjepart som underdatabehandler.

18. Bilag C - Instruks vedrørende behandling af personoplysninger

18.1 Behandlingens genstand/instruks

De omfattede Personoplysninger behandles med det formål at opfylde de i Hovedaftalen nævnte kommercielle ydelser

18.2 Behandlingssikkerhed

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:

Fysisk sikkerhed

Databehandleren gennemfører følgende fysiske sikkerhedsforanstaltninger:

- Databehandleren anvender nøglestyring, dvs. udlevere nøgler til de relevante og nødvendige medarbejdere mv.
- Databehandleren har alarmsystem til at opdage og forhindre indbrud.
- Databehandleren har brandalarm og røgdetektorer.
- Databehandleren har testet beredskabs- og evakueringsplan til nødsituationer.
- Databehandleren og besøgende m.fl. identificeres ved brug af identifikationskort.
- Databehandlerens bygning(er) er opdelt i adgangszoner, hvorefter adgangskort er påkrævet for adgang til zonerne.
- Databehandlerens kontorlokaler kan aflåses.
- Databehandlerens medarbejdere har pligt til at bære identitetskort.
- Databehandlerens udstyr (herunder PC'er, eventuelle servere mv.) er sikret bag låste døre.
- Der anvendes kontrolproces eller -system til kontrol med besøgendes identitet.
- Der føres protokol over Databehandlerens besøgende.
- Reception bemandes 24/7 eller der er vagtselskab udenfor kontortid.

Organisatorisk sikkerhed

Databehandleren gennemfører følgende organisatoriske sikkerhedsforanstaltninger:

- Alle medarbejdere er underlagt fortrolighedsforpligtelse, der gælder for alle behandlede personoplysninger.
- Databehandleren har en dokumenteret procesbeskrivelse for brud på persondatasikkerheden, der minimum tages op til revidering årligt.
- Databehandleren har en fast proces, der sikrer, at der ved reparation, service og kassation af hardware sørges for sletning eller fortsat fortrolighed vedrørende personoplysninger på det berørte hardware.
- Databehandleren har en it-sikkerhedspolitik.
- Databehandleren har mulighed for at reagere ansættelsesretligt på medarbejderes brud på databehandlerens datasikkerhed eller brud på instruks om behandling af personoplysninger.
- Databehandlerens medarbejdere dokumenterer og rapporterer regelmæssigt brud på persondatasikkerheden eller risici herfor.
- Medarbejderes behandling af personoplysninger logges helt eller delvis og kan kontrolleres efter behov.
- Medarbejdernes adgang til personoplysninger i systemer og på eventuelle fysiske medier eller faciliteter er begrænset, sådan at det kun er de relevante medarbejdere, der har adgang til de relevante personoplysninger.

Teknisk sikkerhed: Adgang til og beskyttelse af systemer

Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende adgang til og beskyttelse af systemer:

- Databehandleren benytter antivirus-programmer, som opdateres jævnligt.
- Databehandleren kræver, at medarbejdere anvender individuelle adgangskoder (passwords).
- Databehandlerens PC'er har automatisk adgangsbeskyttelse ved inaktivitet, dvs. låst pauseskærm.
- Databehandlerens systemer har logisk adgangskontrol ved brugernavn og adgangskode eller anden autorisation.
- Der anvendes politik for sammensætningen af adgangskoder, herunder minimumskrav.
- Der er procedure(r) for tilbagekaldelse af tilladelser, når en medarbejder stopper hos databehandleren eller skifter afdeling.
- Der er procedure(r) for tildeling af autorisationer til it-systemer ved en medarbejders ansættelse.
- Der foretages logning og kontrol af uautoriserede eller gentagne mislykkede forsøg på log-in på databehandlerens systemer.

Teknisk sikkerhed: Adgang til personoplysninger (data)

Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende adgang til personoplysninger:

- Databehandleren foretager regelmæssig gennemgang og kontrol af brugerautorisationer til specifikke systemer.
- Databehandleren foretager regelmæssigt gennemgang af systemkontrol.
- Databehandleren har procedure(r) for at genskabe/reetablere data fra backup.
- Databehandleren har sporbarhed af adgang til, ændring af og sletning af data foretaget af individuelle brugere.
- Databehandleren tildeler enkelte eller grupper af brugere autorisationer til at tilgå, ændre og slette behandlede personoplysninger.

Teknisk sikkerhed: Kryptering

Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende kryptering:

- Databehandlerens hjemmesider anvender HTTPS (Hyper Text Transfer Protocol Secure).
- Der anvendes kryptering af netværk.

Teknisk sikkerhed: Kontrol af transmission

Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende kontrol af transmission:

- Databehandleren anvender og har retningslinjer for sikker e-mail.
- Retningslinjer for brug af arbejdsmail, herunder brug til privat brug, passende brug, kryptering, sikker brug mv.
- Udgående e-mails med følsomme personoplysninger eller oplysninger om rent private forhold krypteres.

Teknisk sikkerhed: Tilgængelighed og robusthed

Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende tilgængelighed og robusthed:

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

18.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den Dataansvarlige i overensstemmelse med Bestemmelse 8.1 og 8.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

- 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.

- 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.
- 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.

18.4 Opbevaringsperiode/sletterutine

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal Databehandleren slette 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.

18.5 Lokalitet for behandling

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.

18.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Personoplysningerne behandles kun af Databehandleren på de lokationer, som er beskrevet i dette bilag.

Overførsler til USA sker på grundlag af dataimportørens certifikation under EU-U.S. Data Privacy Framework (se certificerede organisationer [her](#).)

Sikre tredjelande

Databehandleren overfører som led i opfyldelse af Bestemmelserne personoplysningerne til følgende lande:

- Færøerne
- Schweiz
- Storbritannien

Sådanne overførsler sker på baggrund af beslutninger fra EU-Kommissionen, hvorefter der generelt enten via lovgivning eller via andre foranstaltninger er sikret et tilstrækkeligt beskyttelsesniveau.

Usikre tredjelande

Databehandleren overfører som led i opfyldelse af Hovedaftalen Personoplysningerne til følgende lande: USA

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 GDPR, artikel 45, skal det lovlige overførselsgrundlag være standardkontraktbestemmelser efter GDPR, artikel 46(1) og 46(2)(c).

I det omfang personoplysninger overføres til tredjelande, som ikke har været genstand for en afgørelse om tilstrækkelig

sikkerhed efter GDPR, artikel 45, 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.

Generelt

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.

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.

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.

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

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

- overholder sine forpligtelser efter denne Databehandleraftale og Instruksen, og
- overholder bestemmelserne i GDPR, for så vidt angår personoplysningerne, som behandles på den Dataansvarliges vegne.

Databehandlerens dokumentation skal sendes til den Dataansvarlige inden for rimelig tid efter modtagelsen af anmodningen herom.

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.

Uanset forudgående 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 7 kalenderdage.

19. Bilag D - Parternes regulering af andre forhold

19.1 Øvrige forhold

Databehandleraftalen regulerer ikke øvrige forhold.

20. 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 Databehandlersaftale, 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 GDPR, article 46, 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 connection with the services governed by the Data Processing Agreement, to third countries outside the EU/EEA, not subject to an adequacy decision on the basis of GDPR, article 45, insofar as none of the derogations for a specific situation referred to in GDPR, article 49 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 adequacy decision on the basis of GDPR, article 45.

21. Section I

• 21.1 Purpose and scope

- a. 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.
- b. The Parties:

- i. 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
 - ii. 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').
- c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

• 21.2 Effect and invariability of the Clauses

- a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to GDPR, article 46(1) and 46(2)(c), with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to GDPR, article 28(7), 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.
- b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of GDPR.

• 21.3 Third-party beneficiaries

- a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
 - i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
 - ii. 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;
 - iii. 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;
 - iv. Clause 12 – Module One: Clause 12.1 and 12.4; Modules Two and Three: Clause 12.1, 12.4 and 12.6;
 - v. Clause 13;
 - vi. Clause 15.1.3, 15.1.4 and 15.1.5;
 - vii. Clause 16.5;
 - viii. Clause 18 – Modules One, Two and Three: Clause 18.1 and 18.2; Module Four: Clause 18.
- b. Paragraph 3.1 is without prejudice to rights of data subjects under GDPR.

• 21.4 Interpretation

- a. Where these Clauses use terms that are defined in GDPR, those terms shall have the same meaning as in that Regulation.
- b. These Clauses shall be read and interpreted in the light of the provisions of GDPR.
- c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in GDPR.

• 21.5 Hierarchy

- a. 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.
- b. Paragraph 5.1 notwithstanding, insofar as the contradiction with a later agreement between the parties strictly concerns the optional content of paragraph 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 GDPR, article 46(1) and article 46(2)(c).

• 21.6 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.

• 21.7 Docking Clause (NOT IN EFFECT)

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

22. Section II - OBLIGATIONS OF THE PARTIES

• 22.1 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 THREE: Transfer processor to processor (IN EFFECT)

1. Instructions

- a. 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.
- b. 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.
- c. 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.
- d. 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].

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.

3. Transparency

- a. 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.
- b. Insofar as the content matter of these Clauses and the Appendix is determined by reference to other agreements between the parties, the relevant parts of such other agreements are likewise subject to the provisions of transparency contained in paragraph 8.3.1.

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.

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.

6. Security of processing

- a. 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.
- b. 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.
- c. 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.

- d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under GDPR, 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.

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. 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 GDPR, article 45, that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to GDPR, articles 46, or 47 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

9. Documentation and compliance

- a. 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.
- b. 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.
- c. 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.
- d. 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.
- e. Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.
- f. 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.

- g. 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.

• 22.2 Data subject rights

MODULE THREE: Transfer processor to processor (IN EFFECT)

- a. 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.
- b. 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 GDPR 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.
- c. 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.

• 22.3 Redress

MODULE THREE: Transfer processor to processor (IN EFFECT)

- 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.
- 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.
- 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:
 - i. 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;
 - ii. refer the dispute to the competent courts within the meaning of Clause 18.
- 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 GDPR, article 80(1).
- 5. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- 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.

• 22.4 Liability

MODULE THREE: Transfer processor to processor (IN EFFECT)

- a. 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.

- b. 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.
- c. 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 GDPR or Regulation (EU) 2018/1725, as applicable.
- d. 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.
- e. 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.
- f. 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.
- g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

• 22.5 Supervision

MODULE THREE: Transfer processor to processor (IN EFFECT)

- b. [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with GDPR 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 GDPR in accordance with its article 3(2) and has appointed a representative pursuant to GDPR, article 27(1):] The supervisory authority of the Member State in which the representative within the meaning of GDPR, article 27(1), 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 GDPR in accordance with its article 3(2) without however having to appoint a representative pursuant to GDPR, article 27(2):] 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.

- c. 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.

23. Section III - LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

• 23.1 Local laws and practices affecting compliance with the Clauses

MODULE THREE: Transfer processor to processor (IN EFFECT)

- a. 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 GDPR, article 23(1), are not in contradiction with these Clauses.
- b. The Parties declare that in providing the warranty in paragraph 14.1, they have taken due account in particular of the following elements:
 - i. 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;
 - ii. 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];
 - iii. 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.
- c. 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.
- d. The Parties agree to document the assessment under paragraph 14.2 and make it available to the competent supervisory authority on request.
- e. 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.]
- f. 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

• 23.2 Obligations of the data importer in case of access by public authorities

MODULE THREE: Transfer processor to processor (IN EFFECT)

1. Notification

- a. 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:
 - i. 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
 - ii. 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.]
- b. 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.
- c. 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.]
- d. 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.
- e. 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.

2. Review of legality and data minimisation

- a. 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.
- b. 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.]
- c. 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.

24. SECTION IV – FINAL PROVISIONS

• 24.1 Non-compliance with the Clauses and termination

- a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- b. 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.
- c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
 - i. 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;
 - ii. the data importer is in substantial or persistent breach of these Clauses; or
 - iii. 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.

- d. [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
- e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to GDPR, article 45(3) that covers the transfer of personal data to which these Clauses apply; or (ii) GDPR 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 GDPR

• 24.2 Governing law

MODULE THREE: Transfer processor to processor (IN EFFECT)

- a. 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.

• 24.3 Choice of forum and jurisdiction

MODULE THREE: Transfer processor to processor (IN EFFECT)

- a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- b. The Parties agree that those shall be the courts of Denmark.
- c. 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.

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

Notes:

[1] Where the data exporter is a processor subject to GDPR acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to GDPR 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 the GDPR, 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 GDPR, 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 GDPR, 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 GDPR, article 28(4) 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 GDPR, 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.

25. 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.

26. ANNEX I

A. LIST OF PARTIES

A.1 Data exporter:

Name:

FDE A/S

Address:

Lyren 1, Bovmark, 6330 Padborg, DK

Contact person's name, position and contact details:

Kontaktoplysninger for Databehandleren følger af Hovedaftalen.

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:

Microsoft

Address:

1 Microsoft Way, Redmond, United States.

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.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:

Reference is made to Appendix A, paragraph 15.4 of the data processing agreement.

Categories of personal data transferred:

Reference is made to Appendix A, paragraph 15.3 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(s) from controller to controller under these clauses will be of a continuous nature.

Nature of the processing:

Reference is made to Appendix A, paragraph 15.2 of the data processing agreement.

Purpose(s) of the data transfer and further processing:

Reference is made to Appendix A, paragraph 15.1 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, paragraph 17.4 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.

27. 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 section 6 of the Data Processing Agreement, sub-processors must supply equivalent technical and organisational protective measures, equivalent to those undertaken by the data processor.