RISMA Systems – Databehandleraftale

Bilag 2 til Partneraftale

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

mellem	**IT RELATION A/S** CVR-nr. DK 27 00 10 92 Dalgas Plads 7B, 1. sal 2 7400 Herning Danmark herefter "partneren"	og	**RISMA Systems A/S** CVR-nr. 32 76 97 13 Ejby Industrivej 34-38 2600 Glostrup Danmark herefter "databehandleren"

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

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

INDHOLD

1. PRÆAMBEL

1.1. Parterne har indgået en partneraftale, der regulerer parternes rettigheder og forpligtelser, i forbindelse med partnerens anvendelse af samt køb og salg af licenser til databehandlerens compliance-platform ("Partneraftalen").

1.2. Disse Bestemmelser finder både anvendelse, når partneren er dataansvarlig (i hvilket tilfælde RISMA Systems A/S er databehandler), samt hvor partneren selv er databehandler for en anden dataansvarlig (i hvilket tilfælde RISMA Systems A/S er underdatabehandler).

1.3. I henhold til Partneraftalen vil databehandleren levere og stille visse ydelser og tjenester til rådighed for partneren. Disse Bestemmelser fastsætter herefter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af partneren.

1.4. Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).

1.5. Ved "personoplysning" forstås enhver form for information om en identificeret eller identificerbar, fysisk person, jf. databeskyttelsesforordningens artikel 4. Hvis der som led i opfyldelsen af Bestemmelserne behandles andre fortrolige oplysninger end personoplysninger, f.eks. oplysninger som i medfør af lov om finansiel virksomhed anses for fortrolige, så omfatter enhver henvisning til "personoplysninger" også de øvrige fortrolige oplysninger.

1.6. I forbindelse med hosting af den compliance-platform, som databehandleren stiller til rådighed for partneren, behandler databehandleren personoplysninger på vegne af partneren i overensstemmelse med disse Bestemmelser.

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

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

1.9. 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.

1.10. Bilag B indeholder partnerens betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som partneren har godkendt brugen af.

1.11. Bilag C indeholder partnerens 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.

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

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

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

2. PARTNERENS RETTIGHEDER OG FORPLIGTELSER

2.1. Partneren er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes1 nationale ret og disse Bestemmelser.

2.2. Partneren har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.

2.3. Partneren er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

[1] Henvisninger til "medlemsstat" i disse bestemmelse skal forstås som en henvisning til "EØS medlemsstater".

3. DATABEHANDLEREN HANDLER EFTER INSTRUKS

3.1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra partneren, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt.

3.2. Denne instruks skal være specificeret i Bilag A og C. Efterfølgende instruks kan også gives af partneren, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.

3.3. Databehandleren underretter omgående partneren, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

4. FORTROLIGHED

4.1. Databehandleren skal holde personoplysningerne fortrolige.

4.2. Databehandleren må kun give adgang til personoplysninger, som behandles på partnerens vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.

4.3. Databehandleren skal efter anmodning fra partneren kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

5. BEHANDLINGSSIKKERHED

5.1. Databeskyttelsesforordningens artikel 32 fastslår, at partneren 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.

Partneren skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

a) Pseudonymisering og kryptering af personoplysninger

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

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

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

5.2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af partneren – også vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder, som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal partneren stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.

5.3. Derudover skal databehandleren bistå partneren med vedkommendes overholdelse af partnerens forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for partneren vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for partnerens overholdelse af sin forpligtelse efter forordningens artikel 32.

Hvis imødegåelse af de identificerede risici – efter partnerens vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal partneren angive de yderligere foranstaltninger, der skal gennemføres, i Bilag C.

6. ANVENDELSE AF UNDERDATABEHANDLERE

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

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

6.3. Databehandleren har partnerens generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette partneren om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 dages varsel og derved give partneren 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 partneren allerede har godkendt, fremgår af bilag B.

6.4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af partneren, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

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

6.6. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter partnerens anmodning herom – i kopi til partneren, 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 partneren.

6.7. Databehandleren skal i sin aftale med underdatabehandleren indføje partneren som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at partneren kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør partneren i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

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

7. OVERFØRSEL TIL TREDJELANDE ELLER INTERNATIONALE ORGANISATIONER

7.1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra partneren og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.

7.2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af partneren, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette partneren om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

7.3. Uden dokumenteret instruks fra partneren kan databehandleren således ikke inden for rammerne af disse Bestemmelser:

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

b) overlade behandling af personoplysninger til en underdatabehandler i et tredjeland

c) behandle personoplysningerne i et tredjeland

7.4. Partnerens 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.

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

8. BISTAND TIL PARTNEREN

8.1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt partneren ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af partnerens forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III.

Dette indebærer, at databehandleren så vidt muligt skal bistå partneren i forbindelse med, at partneren skal sikre overholdelsen af:

a) oplysningspligten ved indsamling af personoplysninger hos den registrerede

b) oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede

c) indsigtsretten

d) retten til berigtigelse

e) retten til sletning ("retten til at blive glemt")

f) retten til begrænsning af behandling

g) underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling

h) retten til dataportabilitet

i) retten til indsigelse

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

8.2. I tillæg til databehandlerens forpligtelse til at bistå partneren i henhold til Bestemmelse 5.3, bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, partneren med:

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

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

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

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

8.3. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå partneren samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 8.1 og 8.2.

9. UNDERRETNING OM BRUD PÅ PERSONDATASIKKERHEDEN

9.1. Databehandleren underretter uden unødig forsinkelse partneren efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

9.2. Databehandlerens underretning til partneren skal om muligt ske senest 48 timer efter, at denne er blevet

bekendt med bruddet, sådan at partneren kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.

9.3. I overensstemmelse med Bestemmelse 8.2.a skal databehandleren bistå partneren 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 partnerens anmeldelse af bruddet til den kompetente tilsynsmyndighed:

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

b) de sandsynlige konsekvenser af bruddet på persondatasikkerheden

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

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

10. SLETNING OG RETURNERING AF OPLYSNINGER

10.1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at tilbagelevere alle personoplysningerne og slette eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

11. REVISION, HERUNDER INSPEKTION

11.1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for partneren og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af partneren eller en anden revisor, som er bemyndiget af partneren.

11.2. Procedurerne for partnerens revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmeret angivet i Bilag C.7. og C.8.

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

12. PARTERNES AFTALE OM ANDRE FORHOLD

12.1. Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

13. IKRAFTTRÆDEN OG OPHØR

13.1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.

13.2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.

13.3. 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.

13.4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til partneren i overensstemmelse med Bestemmelse 10.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.

13.5. Underskrift

På vegne af partneren		*På vegne af databehandleren*	
NAVN	Anders Kaag	NAVN	Steen Rath
STILLING	CTO, Group Procurement	STILLING	Salgsdirketør
TLF. NUMMER	+45 61 62 68 62	TLF. NUMMER	+45 41 37 22 28
E-MAIL	ak@itm8.com	E-MAIL	sra@rismasystems.com

UNDERSKRIFT

UNDERSKRIFT

14. KONTAKTPERSONER HOS PARTNEREN OG DATABEHANDLEREN

14.1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

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

Partneren		*Databehandleren*	
NAVN	[NAVN]	NAVN	Nicolai Ascanius
STILLING	[STILLING]	STILLING	CIO
TLF. NUMMER	[TELEFONNUMMER]	TLF. NUMMER	+45 70 25 47 00
E-MAIL	[E-MAIL]	E-MAIL	nas@rismasystems.com

BILAG A – OPLYSNINGER OM BEHANDLINGEN

A.1. Formålet med databehandlerens behandling af personoplysninger på vegne af partneren

Som det fremgår af Bestemmelse 1.1, har parterne indgået en Partneraftale, der regulerer parternes rettigheder og forpligtelser, i forbindelse med at databehandleren stiller en compliance-platform til rådighed for partneren. Som led i dette samarbejde, skal databehandleren hoste partnerens compliance-platform på vegne af partneren.

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

Se beskrivelsen under Bilag A.1. ovenfor.

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

Følgende personoplysninger vil blive behandlet (opdelt på kategorier af registrerede, jf. Bilag A.4. nedenfor):

a) Generelle kontaktoplysninger, såsom navn, emailadresse og telefonnummer

b) Afhænger af partnerens brug af compliance-platformen, men vil typisk alene inkludere generelle kontaktoplysninger, såsom navn og emailadresse

A.4. Behandlingen omfatter følgende kategorier af registrerede

Der vil blive behandlet personoplysninger om følgende kategorier af registrerede:

a) Partnerens medarbejdere

b) Oplysninger om øvrige personer, som partneren vælger at indtaste oplysninger om

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

Databehandleraftalen gælder frem til Partneraftalens ophør, og i øvrigt så længe databehandleren behandler personoplysninger på vegne af partneren.

BILAG B – UNDERDATABEHANDLERE

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har partneren godkendt brugen af følgende underdatabehandlere

Navn	CVR	Adresse	Beskrivelse af behandling	Lokalitet(er) for behandling
Hetzner Online GmbH	Registration Court Ansbach, HRB 6089 VAT ID No. DE 812871812	Industriestraße 25 91710 Gunzenhausen Tyskland	Hetzner Online GmbH hoster den compliance-platform, som databehandleren stiller til rådighed for partneren.	Se adresse
Hetzner Online GmbH (datacenter Nürnberg)	Se ovenfor.	Sigmundstraße 135 90431 Nürnberg Tyskland	Se ovenfor.	Se adresse
Hetzner Finland Oy (datacenter Helsinki)	Business ID: 2720758-9	Huurrekuja 10, 04360 Tuusula, Finland	Hetzner Finland Oy hoster en krypteret back-up af den compliance-platform, som databehandleren stiller til rådighed for partneren.	Se adresse

Ved Bestemmelsernes ikrafttræden har partneren godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden iagttagelse af Bestemmelse 6 – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

B.2. Varsel for godkendelse af underdatabehandlere

Dette er reguleret under Bestemmelse 6.3.

BILAG C – INSTRUKS VEDRØRENDE BEHANDLING AF PERSONOPLYSNINGER

C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af partneren sker ved, at databehandleren udfører følgende:

Se beskrivelsen under Bilag A.1. ovenfor.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle, at behandlingen omfatter en begrænset mængde personoplysninger, som generelt alene omfatter generelle kontaktoplysninger, såsom navne, emailadresser og telefonnumre.

Databehandleren er på denne baggrund berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etablere et passende sikkerhedsniveau under hensyntagen til det enhver tid værende trusselsbillede.

I denne forbindelse skal databehandleren i nødvendigt omfang implementere sikkerhedsforanstaltninger indenfor følgende områder, jf. informationssikkerhedsstandarden ISO:27001:2013 (Annex A):

- Informationssikkerhedspolitikker
- Organisering af informationssikkerhed
- Personalesikkerhed
- Styring af informationsaktiver
- Adgangsstyring
- Kryptografi
- Fysisk sikring og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Anskaffelse, udvikling og vedligeholdelse af systemer
- Leverandørforhold
- Styring af informationssikkerhedsbrud
- Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
- Overholdelse af retlige og kontraktuelle forpligtelser

Databehandleren skal dog uanset hvad - efter aftale med partneren - implementere følgende sikkerhedsforanstaltninger:

a) Baseret på de identificerede risici for fysiske personers rettigheder eller frihedsrettigheder efter databeskyttelsesforordningens artikel 32 og Bestemmelse 6.2, skal databehandleren definere informationssikkerhedspolitikker, som skal godkendes på ledelsesniveau hos databehandleren, samt gøres tilgængeligt og kommunikeres ud til databehandlerens medarbejdere, evt. underdatabehandlere samt partneren;

b) Databehandleren skal kræve, at alle medarbejdere hos databehandleren samt øvrige leverandører overholder de gældende informationssikkerhedspolitikker- og procedurer;

c) Databehandleren skal tilsikre, at alle medarbejdere hos databehandlere, og hvor relevant øvrige leverandører, modtager passende træning i gældende informationssikkerhedspolitikker og -procedurer, som det findes passende for den pågældende jobfunktion;

d) Databehandleren skal implementere tekniske og organisatoriske foranstaltninger for at tilsikre, at medarbejdere hos databehandlere samt evt. underdatabehandlere og øvrige tredjeparter, kun gives adgang til personoplysninger i nødvendigt omfang (need-to-know basis), som det findes passende for den pågældende jobfunktion. Sådanne foranstaltninger skal inkludere identifikation og autorisation af personer, som gives adgang, ligesom der skal foretages regelmæssige auditeringer af sådanne tildelte adgange;

e) Databehandleren skal logge al adgang til personoplysninger. Disse logdata og logningsfaciliteter skal regelmæssigt auditeres og beskyttes mod uautoriseret adgang;

f) Adgang til systemer og applikationer af relevans for behandling af personoplysninger skal ske på baggrund af en sikker log-in løsning, og databehandleren skal vedtage en politik for sikker brug af passwords;

g) Databehandleren skal implementere tekniske foranstaltninger og vedtage en politik for brugen af mobile enheder og fjernarbejde;

h) Databehandleren skal udforme og anvende fysiske sikkerhedsforanstaltninger for fysiske lokaliteter, hvor der behandles personoplysninger for at beskytte mod uautoriseret adgang til eller manipulation af personoplysninger;

i) Databehandleren skal tilsikre, at transmission af personoplysninger via eksterne kommunikationskanaler sker i krypteret form ved brug af stærk kryptering baseret på anerkendte algoritmer;

j) Databehandleren skal fastlægge ledelsesmæssige ansvarsområder og procedurer for at tilsikre hurtig, effektiv og korrekt håndtering af brud på persondatasikkerheden. Sådanne procedurer skal indeholde en forpligtelse til at reagere på brud på persondatasikkerheden via passende kommunikationskanaler så hurtigt som muligt. Viden opnået i forbindelse med håndteringen af brud på persondatasikkerheden skal anvendes for i størst muligt omfang at reducere sandsynligheden for og virkningen af fremtidige hændelser;

k) Databehandleren skal implementere foranstaltninger og udforme politikker for at tilsikre, at personoplysninger slettes ved udgangen af de af partneren fastsatte opbevaringsperioder;

l) Databehandleren skal implementere procedurer for styring af bærbare medier baseret på typen af personoplysninger tilknyttet det enkelte medie og bortskaffe sådanne medier sikkert, når mediet ikke længere er nødvendigt;

m) Databehandleren skal implementere tekniske og organisatoriske foranstaltninger for at tilsikre korrekt og sikker drift af faciliteter og systemer forbundet med behandling af personoplysninger. Sådanne foranstaltninger skal omfatte beskyttelse af systemer, der anvendes til behandling af personoplysninger, mod virus, malware og lignende, ligesom der skal ske regelmæssig sikkerhedskopiering (back-up) af sådanne systemer;

n) Databehandleren skal udforme beredskabsplaner og procedurer for at tilsikre, at tilgængeligheden af og adgangen til persondata kan genoprettes rettidigt i tilfælde af en hændelse; og

o) Databehandleren skal udforme en politik for regelmæssig testning, vurdering og evaluering af effektiviteten af implementerede tekniske og organisatoriske foranstaltninger.

C.3 Bistand til partneren

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

Databehandleren skal stille alle relevante personoplysninger til rådighed og skal om nødvendigt hjælpe partneren med at identificere relevante personoplysninger. Herudover skal databehandlerens bistand primært bestå i at sikre et tilstrækkeligt sikkerhedsniveau i overensstemmelse med Bilag C.2.

C.4 Opbevaringsperiode/sletterutine

Personoplysninger opbevares indtil aftalens ophør, eller indtil partneren selv sletter personoplysninger.

Ved ophør af aftalen, skal databehandleren tilbagelevere personoplysningerne og slette eksisterende kopier i overensstemmelse med Bestemmelse 10.1, medmindre partneren – efter underskriften af disse bestemmelser – har ændret partneren oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

C.5 Lokalitet for behandling

Se oplistningen under Bilag B.1.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Hvis partneren 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.

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

Databehandleren skal hvert år for egen regning indhente en revisionserklæring fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende typer af revisionserklæringer kan anvendes i overensstemmelse med disse Bestemmelser:

- ISAE 3402-erklæring, type 2

Revisionserklæringen gøres tilgængelig på databehandleren hjemmeside, og fremsendes uden unødig forsinkelse til partneren, når partneren anmoder om det.

Baseret på resultaterne af erklæringen, er partneren berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Sådanne yderligere foranstaltninger planlægges i samarbejde med databehandleren, og partnerens eventuelle udgifter i forbindelse med sådanne yderligere foranstaltninger afholdes af partneren selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at bistå partneren.

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

Databehandleren skal hvert tredje år for underdatabehandlerens regning indhente en revisionserklæring fra en uafhængig tredjepart vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende typer af revisionserklæringer kan anvendes i overensstemmelse med disse bestemmelser:

- ISO/IEC 27001:2013

Revisionserklæringer fremsendes uden unødig forsinkelse til partneren, når partneren anmoder om det.

BILAG D – PARTERNES REGULERING AF ANDRE FORHOLD

Udfyldes, hvis nogle – ellers udgår bilag D.

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registereret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Kasper Holton Hülsen
Chief Market Dev. Officer
Serienummer: PID:9208-2002-2-282004995990
IP: 31.3.xxx.xxx
2022-03-28 06:53:37 UTC
NEM ID

Jan Axel Jansson
CCO
Serienummer: PID:9208-2002-2-501681799774
IP: 31.3.xxx.xxx
2022-03-28 06:58:58 UTC
NEM ID

Anders Kaag
CTO, Group Procurement
Serienummer: PID:9208-2002-2-374838695553
IP: 91.142.xxx.xxx
2022-03-28 07:07:38 UTC
NEM ID