

## Tillæg til databehandling

Dette tillæg til databehandling ("DPA") er et tillæg til Lincoln Electric Company Slutbrugerlicens Aftale ("EULA") og er gældende mellem Lincoln Electric Company ("Data Processor") og den autoriserede bruger i henhold til EULA (den "Dataansvarlige"), (hvert "Parti", Og få "Parterne sammen").

### I BETRAGTNING

EULA regulerer retten for den autoriserede bruger med hensyn til brug af den licenserede applikation og, efter behov, andre onlinetjenester leveret af The Lincoln Electric Company. For at opfylde forpligtelser i henhold til EULA, fungerer Lincoln Electric Company som en databehandler på vegne af den autoriserede bruger. For at sikre overholdelse af persondataforordningen har parterne aftalt at supplere EULA for fastsættelse af de vilkår og betingelser, der gælder for behandling af personoplysninger af databehandleren på vegne af den dataansvarlige.

### DET ER AFTALT AT

#### 1. DEFINITIONER

1.1 I denne DPA skal store bogstaver have følgende betydninger, medmindre de er defineret i EULA eller det på anden måde er krævet givet konteksten:

|  |   |
|--|---|
| <b>"Dataansvarlig"</b>                           | betyder den enhed, der bestemmer formålene og midlerne til behandlingen af personoplysninger;   |
| <b>"Databehandler"</b>                           | betyder den enhed, der behandler personoplysninger på vegne af den dataansvarlige;  |
| <b>"Dataemne"</b>                                | betyder en identificeret eller identificerbar person, hvis personoplysninger bliver behandlet;  |
| <b>"Instruktion"</b>                             | betyder at instruktionerne fra den dataansvarlige til databehandleren vedrørende behandling af personoplysninger i henhold til levering af tjenester i overensstemmelse med EULA;   |
| <b>"Personlig data"</b>                          | betyder enhver information vedrørende et identificeret eller identificerbart individ. En identificerbar person er en, der kan identificeres direkte eller indirekte, især ved henvisning til en identifikator, f.eks. et navn, et identifikationsnummer, lokationsdata, en online -identifikator eller til en eller flere faktorer, der er specifikke for hans eller hendes fysiske, fysiologisk, genetisk, mental, økonomisk, kulturel eller social identitet;   |
| <b>"Personlig Data Brud"</b>                     | betyder et brud på sikkerheden, der fører til utilsigtet eller ulovlig ødelæggelse, tab, modifikation, uautoriseret videregivelse eller adgang til, Overførte personoplysninger, lagret eller på anden måde behandlet;  |
| <b>"Proces" / "Processing" / "Behandlet"</b>     | betyder enhver handling, der er gjort på personoplysninger, såsom indsamling, registrering, organisation, lagring, tilpasning eller ændring, hentning, konsultation, brug, videregivelse ved transmission, formidling, overførsel eller på anden måde gjort tilgængelig, justering eller kombination, begrænsning, ødelæggelse;   |
| <b>"Behandlingstjenester"</b>                    | betyder behandling af personoplysninger af databehandleren i forbindelse med EULA;  |
| <b>"Særlige kategorier af personoplysninger"</b> | betyder enhver personoplysninger, der har at race eller etnisk oprindelse, politiske meninger, religiøs eller filosofisk overbevisning eller medlemskab af fagforening, foreninger eller fonde, udseende, straffedomme og sikkerhedsforanstaltninger, finansielle og ejendomsoplysninger, oplysninger om opholdssted, eller kreditoplysninger og behandling af genetiske data, biometriske data med det formål at identificere en fysisk person, data vedrørende sundhed eller data vedrørende en fysisk persons sexliv eller seksuel orientering eller data vedrørende mindreårige i alderen 14 år eller derunder; |

**”Standard  
aftaleklausuler”**

betyder de standardkontraktklausuler der vedtages ved EU -Kommissionens afgørelse 2010/87 af 5. februar 2010 om standardkontraktbestemmelser for overførsel af personoplysninger til databehandlere, der er etableret i tredjelande, eller ethvert andet sæt af standardklausuler, der er aftalt mellem parterne. Hvis den dataansvarlige er placeret i en jurisdiktion uden for Den Europæiske Union, skal henvisningerne til medlemsstaterne i de materielle bestemmelser i standardkontraktbestemmelserne skal forstås som henvisninger til den jurisdiktion, hvor den dataansvarlige er placeret;

**”underprocessor”**

betyder enhver processor, der er engageret af databehandleren (eller af enhver anden underprocessor i databehandleren) til behandling af personoplysninger på vegne af den dataansvarlige i overensstemmelse med dens instruktioner og vilkårene i den skriftlige underentreprise.

- 1.2 Alle anvendte billedtekster og sektionsoverskrifter bruges udelukkende med henblik på reference og bekvemmelighed, er ikke en del af denne DPA og må ikke bruges til fortolkning af denne DPA.

**2. ANVENDELSESOMRÅDE OG ANVENDELSE AF DENNE DPA**

- 2.1 Denne DPA supplerer kun bestemmelserne af denne EULA i forbindelse til de behandlingstjenester, som databehandleren leverer til den dataansvarlige i henhold til EULA.

**3. DATABEHANDLING**

- 3.1 Databehandleren accepterer at behandle personoplysningerne i overensstemmelse med de vilkår og betingelser, der er beskrevet i denne DPA, og især databehandleren forpligter sig til:

- 3.1.1 til kun at behandle personlige data på vegne af den dataansvarlige og på alle tidspunkter i overensstemmelse med den dataansvarliges instruktioner som defineret i denne DPA og alle gældende databeskyttelseslove;
- 3.1.2 at sikre, at enhver person, der er betroet behandlingstjenesterne, har forpligtet sig til tavshedspligt eller er underlagt en lovpligtig tavshedspligt ;
- 3.1.3 at træffe tekniske, fysiske og organisatoriske foranstaltninger for at sikre sikkerhed og fortrolighed af personoplysninger og en passende beskyttelse af personoplysninger behandlet på den dataansvarliges vegne mod misbrug og tab, som angivet i skema 2 i denne DPA;
- 3.1.4 at den dataansvarlige straks vil blive underrettet vedrørende: (a) enhver juridisk bindende anmodning om offentliggørelse af personoplysningerne fra en offentlig myndighed, medmindre andet er forbudt, f.eks. et forbud i henhold til straffelovgivningen for at bevare fortroligheden af en retshåndhævelse eller efterretningsundersøgelse, tvang eller efterretningsundersøgelse, (b) ethvert brud på persondata, der har en påvirkning på de personoplysninger, der behandles på vegne af den dataansvarlige, (c) enhver anmodning modtaget direkte fra de registrerede (herunder adgang til, berigtigelse, sletning, indsigelse, begrænsning, data overførsel og retten til ikke at blive underlagt en afgørelse, der udelukkende er baseret på automatiseret behandling, herunder profilering); databehandleren (i) vil ikke svare direkte på denne anmodning, undtagen for at meddele den registrerede, at der handles på den dataansvarliges vegne og at give den registrerede kontaktoplysninger fra den dataansvarlige, og (ii) under hensyntagen til behandlingens art, vil hjælpe den dataansvarlige med passende teknisk, fysisk og organisatoriske foranstaltninger, for så vidt dette er muligt, for at opfylde den dataansvarliges forpligtelse at besvare anmodninger vedrørende udøvelse af den registreredes rettigheder;
- 3.1.5 at levere kommercielt rimeligt samarbejde til den dataansvarlige for at hjælpe den dataansvarlige med at overholde dennes juridiske forpligtelser i forbindelse med persondatasikkerhed, såsom: notifikation af et brud på persondata til den kompetente tilsynsmyndighed, kommunikation af sådanne krænkelse af personoplysninger til de berørte registrerede og, hvor det er relevant, implementering af konsekvensanalyser af databeskyttelse og forudgående konsultationer med

tilsynsmyndigheder under hensyntagen til karakteren af Behandlingen og de oplysninger, der er tilgængelige for Databehandleren;

- 3.1.6 at stille den dataansvarlige til rådighed for alle oplysninger, der er nødvendige for at bevise overholdelse af forpligtelserne i denne databeskyttelsesforordning og give mulighed for og bidrage til revisioner, herunder inspektioner, foretaget af den dataansvarlige eller en anden revisor, bemyndiget af den dataansvarlige som angivet i afsnit 6; og,
- 3.1.7 at alle behandlingstjenester der udføres af en underprocessor vil blive gennemført i overensstemmelse med afsnit 7.

- 3.2 Med hensyn til behandlingstjenesterne vil den dataansvarlige være ansvarlig for at overholde alle krav, der er gældende i henhold til den gældende lov vedrørende behandling af personoplysninger og de instruktioner, den udsender til databehandleren. Især men med forbehold af det foregående generelt, anerkender og accepterer den dataansvarlige, at denne alene er ansvarlig for følgende: (i) nøjagtighed, kvalitet og lovlighed af personoplysninger (ii) overholdelse af alle nødvendige krav til gennemsigtighed og lovlighed i henhold til den gældende lovgivning vedrørende indsamling og brug af personoplysninger, herunder indhentelse af nødvendige samtykker og autorisationer fra registrerede eller på anden måde (iii) sikre, at den dataansvarlige har retten til at overføre eller give adgang til personoplysningerne til databehandleren, og at den dataansvarlige har givet alle nødvendige meddelelser og indhentet de nødvendige samtykker og/eller autorisationer i forbindelse med denne overførsel eller adgang og mere generelt til behandling i overensstemmelse med betingelserne i EULA (herunder denne DPA) og (iv) at sikre, at dens instruktioner overholder gældende love. Efter anmodning fra databehandleren skal den dataansvarlige inden tre (3) arbejdsdage forelægge databehandleren skriftligt bevis for sådanne meddelelser, samtykker og autorisationer. Den dataansvarlige vil ikke indlæse behandlingstjenesterne, eller på anden måde give databehandleren særlige kategorier af personoplysninger, medmindre der er lavet en særskilt skriftligt aftale af den dataansvarlige. Den dataansvarlige skal straks og uden unødige forsinkelse informere databehandleren, hvis den dataansvarlige ikke er i stand til at overholde sit ansvar i denne databeskyttelsesforordning. Den autoriserede bruger er ansvarlig for at gennemgå behandlingstjenesterne, herunder tilgængelig sikkerhedsdokumentation og funktioner, for at bestemme, om den autoriserede brugers krav, forretningsbehov og juridiske forpligtelser er opfyldt. krav, forretningsbehov og juridiske forpligtelser.
- 3.3 Den dataansvarlige bemyndiger databehandleren til at anonymisere de behandlede personoplysninger i henhold til EULA for udledning af analysedata vedrørende brug af licenseret applikation og Lincoln produkter og udstyr. Yderligere brug af de resulterende statistiske data af databehandleren er ikke betinget af forudgående tilladelse fra den dataansvarlige.

#### **4. INTERNATIONALE DATAOVERFØRELSER**

- 4.1 Den dataansvarlige anerkender og accepterer hermed, at vedrørende levering af behandlingstjenesterne i henhold til EULA, kan databehandleren overføre og opbevare personoplysninger i USA og ethvert andet land, hvor databehandleren er placeret, med det formål at levere behandlingstjenesterne. Derfor kan det i løbet af bestemmelsen af behandlingstjenesterne være nødvendigt at overføre personoplysninger til den databehandler, der er placeret uden for det land hvor den dataansvarlige er placeret. Hvis den dataansvarlige er placeret i Det Europæiske Økonomiske Samarbejdsområde eller i Schweiz, forpligter parterne sig til at bruge bestemmelserne i standardkontraktbestemmelserne vedrørende overførsel af personoplysninger fra den dataansvarlige (fungerer som dataeksportør i henhold til standardkontraktbestemmelserne) til databehandleren (fungerer som dataimportør i henhold til standardkontraktbestemmelserne).
- 4.2 Hvis den dataansvarlige er placeret i Det Europæiske Økonomiske Samarbejdsområde eller i Schweiz, forpligter parterne sig til at bruge bestemmelserne i standardkontraktbestemmelserne vedrørende overførsel af personoplysninger fra den dataansvarlige (fungerer som dataeksportør i henhold til standardkontraktbestemmelserne) til databehandleren (fungerer som dataimportør i henhold til standardkontraktbestemmelserne). forudsat at standardkontraktbestemmelserne er påkrævet ved lov og tilstrækkelige til at møde kravene i de gældende databeskyttelsesbestemmelser for overførsel af personoplysninger fra den dataansvarlige til databehandleren i henhold til EULA.
- 4.3 Hvis parterne anvender standardkontraktbestemmelserne i henhold til afsnit 4.1 eller 4.2 i denne DPA:

- 4.3.1 Tillæg 1 af standardkontraktbestemmelserne skal bruges på følgende grundlag: a) Dataeksportør: den dataansvarlige, b) dataimportør: databehandleren, c) registrerede: personale hos den dataansvarlige (den autoriserede bruger), d) Datakategorier: data vedrørende brug af produkter og udstyr, der ejes, licenseres eller er administreret af databehandleren, overvåges af den licenserede ansøgning i henhold til EULA, herunder registreringsdata (dvs. brugernavne og adgangskoder), (e) Særlige kategorier af personoplysninger: Ikke relevant og (f) Behandlingsoperationer: indsamling, kopiering, overførsel, lagring, modifikation, sletning og andre operationer, der er nødvendige for behandlingstjenesterne i henhold til EULA.
- 4.3.2 Beskrivelsen af de tekniske, fysiske og organisatoriske sikkerhedsforanstaltninger, der iværksættes af databehandleren, implementeret af dataimportør i henhold til tillæg 2 til standardkontraktbestemmelserne, er i overensstemmelse med skema 2 i denne DPA.
- 4.4 Hvis standardkontraktklausulerne er gældende mellem parterne i henhold til sektion 4.1 eller 4.2, vil deres bestemmelser blive betragtet som indarbejdet ved henvisning til denne databeskyttelsesforordning, medmindre parterne udfører standardaftaleklausulerne som et selvstændigt dokument i henhold til sektion 4.5.
- 4.5 I det omfang det kræves af de gældende databeskyttelsesregler, skal parterne indgå og udføre standardkontraktbestemmelserne som et separat dokument.

## **5. OPSIGELSE**

- 5.1 Denne DPA vil træde i kraft på ikrafttrædelsesdatoen for denne EULA.
- 5.2 This DPA will terminate automatically upon the later of termination or expiry of (a) the EULA or (b) of the Data Behandlerens forpligtelser i forhold til behandlingstjenesterne og sådan opsigelse vil ikke kræve en domstolsafgørelse eller retssager eller enhver anden handling fra databehandleren, den dataansvarlige eller en anden part for at være effektiv. Hvor det er relevant, ved ophør af nærværende DPA, skal databehandleren vende tilbage til data Behandler eller sletter, efter den dataansvarliges anmodning, alle den dataansvarliges personlige data, som denne besidder eller under dennes kontrol. Efter anmodning fra den dataansvarlige skal databehandleren skriftligt bekræfte overholdelsen af sådanne forpligtelser og slette eksisterende kopier, medmindre en gældende lov kræver lagring eller på anden måde tillader opbevaring af personoplysningerne.
- 5.3 Den dataansvarlige har ret til at opsigte denne DPA ved skriftlig meddelelse til databehandleren, hvis databehandleren er i væsentlig eller et vedvarende brud af denne databeskyttelsesmyndighed, som i tilfælde af et brud, der kan afhjælpes, ikke er blevet afhjulpet inden for tredive (30) arbejdsdage fra datoen for databehandlerens modtagelse af en meddelelse fra den dataansvarlige, der har identificeret bruddet og kræver en afhjælpning.
- 5.4 Den dataansvarlige har ret til at opsigte denne DPA ved skriftlig meddelelse til databehandleren, hvis databehandleren er i væsentlig eller et vedvarende brud af denne databeskyttelsesmyndighed, som i tilfælde af et brud, der kan afhjælpes, ikke er blevet afhjulpet inden for tredive (30) arbejdsdage fra datoen for databehandlerens modtagelse af en meddelelse fra den dataansvarlige, der har identificeret bruddet og kræver en afhjælpning.

## **6. REVISIONER OG INFORMATIONSANMODNINGER**

- 6.1 Med for grænsen på en (1) revision om året og med forbehold af meddelelse fra den dataansvarlige med tredive (30) dages varsel, undtagen i tilfælde af en revision anmodet af en tilsynsmyndighed, den dataansvarlige kan i normalåbningstid, uden urimeligt at blande sig i databehandlerens forretningoperationer, personligt revision af databehandleren eller valg af en tredjepartsrevisor, der er underlagt fortrolighedsforpligtelser til at udføre en sådan revision.
- 6.2 Databehandleren skal samarbejde i tilfælde af en revision i henhold til denne sektion 6 og give den dataansvarlige alle oplysninger, der er nødvendige for udførelse af en sådan revision. Den dataansvarlige skal dække de omkostninger og udgifter, der påløber hver part i forbindelse med revisioner i henhold til denne sektion 6.

**7. UDNÆVNELSE AF UNDERPROCESSORER**

- 7.1 Den dataansvarlige giver databehandleren tilladelse til at bruge underprocessorers service, der er angivet på siden, der er tilgængelig på [\[https://www.lincolnelectric.com/en/Legal-Information/Subprocessors\]](https://www.lincolnelectric.com/en/Legal-Information/Subprocessors), udelukkende efter behov for udførelsen af tjenesterne i forbindelse med EULA.
- 7.2 Den dataansvarlige skal give databehandleren tilladelse til at anvende nye underprocessorers service, med forbehold af forudgående meddelelse til den dataansvarlige af databehandleren med en femten (15) dages varsel før ændringen af underprocessoren. Hvis den dataansvarlige gør indsigelse mod ændringen af en underprocessor, hvor dette er blevet underrettet, kan den dataansvarlige i hele opsigelsesperioden afslutte denne DPA skriftligt. Hvis den dataansvarlige ikke stopper inden for opsigelsesperioden, formaliserer dette den dataansvarliges samtykke til den underrettede ændring af underprocessor.
- 7.3 Under alle omstændigheder, hvor databehandleren anvender en underprocessors tjenester, er sidstnævnte ved kontrakt forpligtet til at overholde de samme forpligtelser, som databehandleren er bundet til med hensyn til behandling af personoplysninger i henhold til denne DPA.

**8. DIVERSE BESTEMMELSER**

- 8.1 Ændringer eller tilføjelser til denne DPA skal foretages skriftligt for at den er effektiv. Uanset det foregående kan databehandleren til enhver tid og uden varsel til den dataansvarlige lave ændringer i de tekniske, fysiske og organisatoriske foranstaltninger, der er angivet i skema 2, forudsat at en sådan ændring ikke i væsentlig grad vil påvirke sikkerheden, fortroligheden eller integriteten af personoplysninger .
- 8.2 Henvisninger i denne DPA til "skrivning" eller "skrift" inkluderere-mail-kommunikation og certificeret post.
- 8.3 Hvis en bestemmelse i denne DPA er eller bliver ugyldig, har dette ikke påvirkning på gyldigheden af de resterende vilkår. I tilfælde af ugyldighed af en bestemmelse i denne DPA skal parterne under alle omstændigheder i god tro forsøge at erstatte den ugyldige bestemmelse med en anden, håndhævelig, gyldig og juridisk, der mest muligt i samme omfang har en juridisk indvirkning svarer til eller svarer til den oprindelige bestemmelse.
- 8.4 Denne DPA er underlagt den samme gældende lovgivning som EULA.

**TIDSPLAN 1 - JURISDIKTION SÆRLIGE BETINGELSER**

Når den dataansvarlige er placeret i en af de jurisdiktioner, der er anført i dette skema 1, gælder de følgende vilkår for DPA, og i tilfælde af konflikt vil sådanne vilkår erstatte og kontrollere de andre bestemmelser i DPA. Alle vilkår i denne EULA, der ikke er specifikt ændret af de gældende jurisdiktionsspecifikke vilkår i dette skema 1, vil forblive uændrede og i fuld kraft og effekt.

**Brasilien:**

Parterne anerkender og er enige om, at følgende ændring af databeskyttelsesforordningen skal anvendes:

- a) Alle forekomster af "Særlige kategorier af personoplysninger" i databeskyttelsesforordningen erstattes af "Følsomme personoplysninger".

**Mexico:**

Parterne anerkender og er enige om, at følgende ændring af databeskyttelsesforordningen skal anvendes:

- a) Alle forekomster af "Særlige kategorier af personoplysninger" i DPA skal erstattes af "Følsomme personoplysninger";
- b) For applikationen af standardkontraktbestemmelserne skal alle henvisninger til "overførsler" af personoplysninger fortolkes som eftergivelser af personoplysninger i henhold til Mexicansk føderal lov vedrørende beskyttelse af personoplysninger i besiddelse af de private parter ("Ley Federal de Protección de Datos Personales en Posesión de los Particulares").

**Rusland:**

Ud over bestemmelserne i databeskyttelsesmyndigheden forpligter parterne på følgende måde:

- a) Databehandleren bekræfter hermed, at være fuldt ud klar over, at formålet med personoplysningsbehandlingsaktiviteterne i henhold til databeskyttelsesmyndigheden kun er at levere behandlingstjenesterne og kun behandle personoplysningerne til det formål, hvortil personoplysningerne videregives, og den dataansvarlige kræver det fra databehandleren. Desuden skal databehandleren straks skriftligt bekræfte, at denne regel overholdes, hvis dette anmodes fra den dataansvarlige.
- b) Inden videregivelse af de personoplysninger, der kommer fra russiske statsborgere til databehandleren, skal den dataansvarlige sikre, at alle sådanne personoplysninger er blevet registreret, systemiseret, akkumuleret, gemt, afklaret (opdateret, ændret) og ekstraheret med brug af databaser, der er lokaliseret på Den Russiske Føderations område, når personoplysninger er indsamlet, herunder gælder også internettet.
- c) Hvis den dataansvarlige registrerer en ulovlig behandling eller unøjagtighed af personoplysningerne, skal den dataansvarlige straks instruere databehandleren om en blokering af disse personoplysninger og starte en inspektion. De berørte personoplysninger skal være blokeret gennem hele inspektionsperioden. Hvis inspektionen bekræfter unøjagtigheden af personoplysningerne, skal den dataansvarlige anmode den relevante registrerede (dennes repræsentant) eller databeskyttelsesmyndigheden (hvis relevant) vedrørende ændringerne og videresende dem til databehandleren. Unøjagtige personoplysninger skal ændres inden for kort tid og senest inden for syv (7) arbejdsdage fra den dag, hvor ændringerne blev leveret til databehandleren. Blokeringen af Personoplysningerne skal fjernes straks ved ændringer.
- d) Hvis det opdages, at personoplysningerne er behandlet på ulovlig måde, skal den dataansvarlige instruere databehandleren om at stoppe en sådan ulovlig behandling inden for tre (3) arbejdsdage fra datoen for afsløringen. Hvis det viser sig at være umuligt at fjerne overtrædelserne og sikre lovligheden af behandling af personoplysninger, skal den dataansvarlige instruere databehandleren om at ødelægge de ulovligt behandlede personoplysninger inden for ti (10) arbejdsdage efter datoen for afsløringen. Den dataansvarlige er også forpligtet til at underrette den relevante registrerede (hans/hendes repræsentant) og, når det kræves ved lov, til databeskyttelsesmyndigheden vedrørende eliminering af overtrædelserne.
- e) Hvis en registreret tilbagekalder hans/hendes samtykke vedrørende behandling af personoplysninger, skal den dataansvarlige straks underrette databehandleren, og databehandleren skal stoppe behandlingen og ødelægge den registreredes personoplysninger inden for tredive (30) dage fra den dato, hvor den dataansvarlige har modtaget annulleringsmeddelelsen.
- f) Hvis det ikke er muligt at overholde de tidsperioder, der er angivet i klausul d) og e) her ovenfor, skal databehandleren blokere de relevante personoplysninger efter anmodning fra den dataansvarlige i højst seks (6) måneder og ødelægge denne personlige Data inden for samme periode, medmindre gældende lov foreskriver noget andet.

#### **Sydafrika:**

Parterne anerkender og er enige om, at de følgende ændringer af DPA finder anvendelse med hensyn til definitionerne i sektion 1 i databeskyttelsesforordningen:

- a) "Den registrerede" betyder en person, hvis personoplysninger bliver behandlet.
- b) "Personlige data" betyder personlige oplysninger som defineret i POPIA, inkluderet oplysninger om en identificeret eller identificerbar person.
- c) "POPIA" betyder den sydafrikanske lov vedrørende beskyttelse af personoplysninger 4 fra 2013 og enhver bindende regulering, direktiv, kendelse, bekendtgørelse eller retningslinje offentliggjort under POPIA.

#### **Forenede Stater:**

Ud over bestemmelserne i databeskyttelsesmyndigheden forpligter parterne på følgende måde:

- a) Hver part anerkender og accepterer, at indsamling og videregivelse af personoplysninger, der overføres til behandlingstjenesterne (i), ikke udgør og ikke er en af parternes hensigt med en sådan aktivitet at udgøre et salg af personoplysninger, og (ii) hvis værdifulde vederlag, monetære eller på anden måde, bliver leveret af autoriseret bruger til databehandleren, er sådanne værdifulde vederlag, monetære eller på anden måde, givet til brug for behandlingstjenesterne og ikke til videregivelse af personoplysninger. Databehandleren må ikke opbevare, bruge, videregive eller sælge personoplysninger til andre formål end til det specifikke formål at udføre behandlingstjenesterne, eller som på anden måde er tilladt ved lov eller denne EULA. For at undgå tvivl må databehandleren ikke sælge personoplysninger eller autorisere eller på anden måde tillade nogen underprocessor at foretage det samme, medmindre andet er tilladt af EULA eller ved gældende lov.

## Skema 2 - Sikkerhedsforanstaltninger implementeret af databehandleren

### 1. Fysisk adgangskontrol til lokaler og faciliteter

Databehandleren vil implementere tekniske og organisatoriske foranstaltninger til en kontrol af adgang til lokaler og faciliteter, især for at kontrollere autorisation for at sikre forebyggelse af uautoriseret adgang.

Specifikt:

- Adgangskontrolsystem
- ID læser, magnetkort, chipkort
- Udstedelse af nøgler
- Dørlåsning
- Sikkerhedspersonale, vagter
- Overvågningsfaciliteter
- Alarmsystem, video/CCTV skærm

### 2. Adgangskontrol til systemer

Databehandleren vil implementere tekniske (ID/adgangskode sikkerhed) og organisatoriske foranstaltninger til brugeridentifikation og godkendelse for at forhindre at der forekommer uautoriseret adgang til IT systemer.

Specifikt:

- Adgangskodeprocedurer (inkl. Specialtegn, minimumslængde, ændring af adgangskode)
- Automatisk blokering (f.eks. Adgangskode eller timeout)
- Kryptering af datamedier, herunder flytbare og bærbare.

### 3. Logisk adgangskontrol til data

Databehandler vil sikre, at aktiviteter i it-systemer, der ikke er dækket af de tildelte adgangsrettigheder, forhindres ved at anvende en kravbaseret definition af godkendelsesordningen og adgangsrettigheder og overvågning og logning af adgang.

Specifikt:

- Rollebaserede adgangsrettigheder (profiler, roller, transaktioner og objekter)
- Brug af en kommerciel Privilegeret Kontostyring løsning til at lette sikker godkendelse af administrative konti til systemer til vedligeholdelse eller andre administrative formål
- Automatiserede rapporter, der regelmæssigt gennemgås og følges op for uregelmæssig eller mistænkelig aktivitet
- Adgang ved hjælp af en model med mindst privilegium til kun at tillade adgang til systemer og/eller data baseret på behov for at vide

### 4. Offentliggørelse og databeskyttelseskontrol

Databehandleren vil kontrollere videregivelse af personoplysninger ved at inkorporere foranstaltninger til transport, overførsel og kommunikation eller lagring af data på datamedier (manuel eller elektronisk) og til efterfølgende kontrol via elektronisk overførsel, datatransport og transmissionskontrol.

Specifikt:

- Kryptering/tunneling
- Elektronisk underskrift
- Logning og en løbende overvågning af sikkerhedshændelser og advarsler
- Transportsikkerhed til at kryptere data under forsendelse
- Kryptering af data i hvile
- En regelmæssig rotation af krypteringsnøgler
- Begrænsning af adgang til krypteringsnøgler til begrænsede personer
- Adgangskodekompleksitet aktiveret, med tofaktorautenticering påkrævet til alle fjernadgangssessioner

### 5. Indgangskontrol

Databehandleren vil bevare fuld dokumentation for datastyring og vedligeholdelse skal vedligeholdes, herunder foranstaltninger til efterfølgende kontrol af, om data er blevet indtastet, ændret eller fjernet (slettet), og af hvem:

Specifikt:

- Logning og rapporteringssystemer



## 6. Jobkontrol

Databehandleren vil behandle personoplysninger i henhold til den dataansvarliges instruktioner og vil acceptere foranstaltninger (teknisk/organisatorisk) for at adskille ansvaret mellem den dataansvarlige og databehandleren: Specifikt:

- Entydig formulering af kontrakten
- Formel idriftsættelse (anmodningsformular)
- Kriterier vedrørende valg af databehandler
- Overvågning af kontraktens udførelse

## 7. Tilgængelighedskontrol

Databehandleren vil sikre, at data vil blive beskyttet mod utilsigtet eller ondsindet ødelæggelse eller tab ved at træffe foranstaltninger til at sikre dataens fysiske og logiske sikkerhed.

Specifikt:

- Backup procedurer
- Spejling af harddiske, f.eks. RAID -teknologi
- Nødstrømsforsyning (UPS)
- Fjernbetjening eller disk-baseret lagring, der replikeres til alternative datacentre
- Antivirus- og/eller anti-malware-software, der bliver opdateret regelmæssigt og applikationsbevidste firewall-systemer konfigureret med standard-nægtelseserklæringer, hvilket kun tillader trafik, der eksplicit er tilladt til forretningsformål
- Forretningskontinuitet og Plan for genopretning af katastrofer

## 8. Adskillelseskontrol

Databehandleren vil søge at sikre, at data, der er indsamlet til forskellige formål vil blive behandlet hver for sig og ikke bliver blandet med andre kundedata ved at gennemføre specifikke foranstaltninger til at sørge for separat Behandling (opbevaring, ændring, sletning, transmission) af data til forskellige formål:

Specifikt:

- "Intern klient" koncept / begrænsning af brug
- Funktionsopdeling (produktion/test)