SENAST UPPDATERAD: 22 juni 2021

Tillägg för databehandling

Detta tillägg för databehandling (“**DPA**”) är ett tillägg till Lincoln Electric Company Licens för slutanvändare avtalet(“**EULA**”) och är tillämplig mellan Lincoln Electric Company (” **Databehandlare**”) och den auktoriserade användaren enligt EULA ("**Data registeransvarig**"), (var och en " **Part**" och tillsammans "**Parter** ”).

MEDAN DÄREMOT

EULA reglerar rätten för den auktoriserade användaren att använda den licensierade applikationen och, i tillämpliga fall, andra onlinetjänster som tillhandahålls av Lincoln Electric Company. I syfte att uppfylla sina skyldigheter enligt EULA ska Lincoln Electric Company fungera som databehandlare för den auktoriserade användarens räkning. För att säkerställa att personuppgiftsbestämmelserna överensstämmer har parterna enats om att komplettera EULA för att fastställa de villkor och förutsättningar som gäller för behandling av personuppgifter av databehandlaren för den registeransvariges räkning.

DET ÄR ENIGHET OM

1. DEFINITIONER

1.1 I detta DPA, termer med stora bokstäver ska ha följande betydelser, såvida de inte definieras i EULA eller på annat sätt krävs med tanke på sammanhanget:

”Personuppgiftsansvarig”	betyder den enhet som bestämmer ändamålen och medlen för behandlingen av personuppgifter;
“Databehandlare”	betyder den enhet som behandlar personuppgifter för den data registeransvariges räkning;
“Registrerade personen”	betyder en identifierad eller identifierbar individ vars personuppgifter bearbetas;
“Instruktion”	betyder instruktionerna som tillhandahålls av data registeransvarige till databehandlaren för att behandla personuppgifter i enlighet med tillhandahållande av tjänster i enlighet med EULA;
“Personuppgifter”	betyder all information som avser en identifierad eller identifierbar person. En identifierbar person är en som kan identifieras, direkt eller indirekt, särskilt med hänvisning till en identifierare som ett namn, ett identifieringsnummer, lokaliseringsdata, en online -identifierare eller en eller flera faktorer som är specifika för hans eller hennes fysiska, fysiologiska, genetiska, mentala, ekonomiska, kulturella eller sociala identitet;
“Kränkning av personuppgifter”	innebär ett säkerhetsbrott som leder till oavsiktlig eller olaglig förstörelse, förlust, ändring, obehörigt avslöjande av eller tillgång till, personuppgifter som överförs, lagras eller på annat sätt behandlas;
“Bearbeta”/“Bearbetning” /“Bearbetad”	betyder alla åtgärder som utförs på personuppgifter såsom insamling, registrering, organisation, lagring, anpassning eller ändring, hämtning, samråd, användning, avslöjande genom överföring, spridning, överföring eller på annat sätt göra tillgänglig, justering eller kombination, begränsning, radering eller förstörelse;
“Bearbetningstjänster”	innebär bearbetning av personuppgifter av databehandlaren i samband med EULA;
”Särskilda kategorier av personuppgifter”	betyder alla personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiösa eller filosofiska övertygelser, eller medlemskap i fackföreningar, föreningar eller stiftelser, utseende, brottmålsdomar och säkerhetsåtgärder, finans- och egendomsinformation, information om uppehållsort, eller kreditinformation och behandling av genetiska data, biometriska data i syfte att identifiera en fysisk person på ett unikt sätt, uppgifter om hälsa eller uppgifter om en fysisk persons sexliv eller sexuella läggning eller uppgifter om minderåriga som är 14 år eller yngre;

”Standardavtalsklausuler”	betyder de standardavtalsklausuler som antogs genom EU-kommissionens beslut 2010/87 av den 5 februari 2010 om standardavtalsklausuler för överföring av personuppgifter till behandlare som är etablerade i tredjeländer eller någon annan uppsättning standardklausuler som avtalats mellan parterna. Om den personuppgiftsansvarige är etablerad i en jurisdiktion utanför EU, ska hänvisningarna till medlemsstaterna i de materiella bestämmelserna i standardavtalsklausulerna tolkas som hänvisningar till den jurisdiktion där den personuppgiftsansvarige är etablerad;
“Underentreprenör”	betyder alla entreprenörer som engageras av databehandlaren (eller av någon annan underentreprenör av databehandlaren) för att bearbeta personuppgifter på uppdrag av den personuppgiftsansvarige i enlighet med dess instruktioner och villkoren i det skriftliga underleverantörskontraktet.

1.2 Bildtexterna och avsnittsrubrikerna som används är endast avsedda för referens och bekvämlighets skull, är inte en del av denna DPA, och ska inte användas för att tolka denna DPA.

2. OMFATTNING OCH TILLÄMPNING AV DENNA DPA

2.1 Denna DPA kompletterar endast bestämmelserna i EULA i förhållande till de bearbetningstjänster som tillhandahålls av databehandlaren till den personuppgiftsansvarige i enlighet med EULA.

3. PERSONUPPGIFTBEARBETNING

3.1 Databehandlaren samtycker till att behandla personuppgifterna i enlighet med villkoren och förutsättningarna i denna DPA, och databehandlaren åtar sig särskilt:

3.1.1 att behandla personuppgifterna endast för den personuppgiftsansvariges räkning och alltid i enlighet med den personuppgiftsansvariges instruktioner enligt definitionen i denna DPA och alla tillämpliga dataskyddslagar;

3.1.2 att säkerställa att all personal som anförtrotts bearbetningstjänsterna har förbundit sig till sekretess eller är under en lämplig lagstadgad tystnadsplikt;

3.1.3 att vidta tekniska, fysiska och organisatoriska åtgärder för att säkerställa personuppgifternas säkerhet och sekretess och på lämpligt sätt skydda personuppgifter som behandlas för den personuppgiftsansvariges räkning mot missbruk och förlust, enligt schema 2 i denna DPA;

3.1.4 att den omedelbart kommer att meddela den personuppgiftsansvarige om: (a) varje juridiskt bindande begäran om offentliggörande av personuppgifter från en statlig myndighet om inte annat är förbjudet, såsom ett straffrättsligt förbud för att bevara sekretessen för polismyndighet eller underrättelseutredning, (b) varje personuppgiftsöverträdelse som påverkar de personuppgifter som behandlas för den personuppgiftsansvariges räkning, (c) varje begäran som tas emot direkt från de registrerade personen (inklusive rätt till åtkomst, rättelse, radering, invändning, begränsning, dataöverföring och rätten att inte bli föremål för ett beslut som enbart grundas på automatisk bearbetning, inklusive profilering); Databehandlaren (i) kommer inte att svara direkt på den begäran, förutom att meddela den registrerade personen att den agerar på den personuppgiftsansvariges vägnar och för att förse den registrerade personen med kontaktuppgifterna för den personuppgiftsansvarige, och (ii) med hänsyn till behandlingens karaktär, kommer att hjälpa den personuppgiftsansvarige med lämpliga tekniska, fysiska och organisatoriska åtgärder, i den mån detta är möjligt, för att uppfylla den personuppgiftsansvariges skyldighet att svara på förfrågningar om att utöva den registrerade personens rättigheter;

3.1.5 att tillhandahålla affärsmässigt rimligt samarbete till den personuppgiftsansvarige för att hjälpa den personuppgiftsansvarige att uppfylla sina egna rättsliga skyldigheter relaterade till säkerheten för personuppgifter, till exempel: anmälan av ett personuppgiftskränkning till den behöriga tillsynsmyndigheten, kommunikation av sådana kränkningar av personuppgifter till de berörda registrerade personer och i tillämpliga fall, genomförande av konsekvensanalyser av dataskydd och tidigare samråd med tillsynsmyndigheter, med beaktande av behandlingens art och den information som finns tillgänglig för databehandlaren;

3.1.6 att tillhandahålla till den personuppgiftsansvarige all information som är nödvändig för att bevisa att de skyldigheter som anges i denna DPA överensstämmer och möjliggöra och bidra till revisioner, inklusive inspektioner, utförda av den personuppgiftsansvarige eller en annan revisor på uppdrag av den personuppgiftsansvarige enligt avsnitt 6; och

3.1.7 att alla bearbetningstjänster som utförs av en underentreprenör kommer att utföras i enlighet med avsnitt 7.

3.2 När det gäller bearbetningstjänsterna kommer den personuppgiftsansvarige att ansvara för att uppfylla alla krav som gäller för den enligt tillämplig lag när det gäller behandling av personuppgifter och de instruktioner som den utfärdar för databehandlaren. I synnerhet men utan att det påverkar allmängiltigheten i det föregående, bekräftar och godkänner den personuppgiftsansvarige att den kommer att vara ensam ansvarig för följande: (i) personuppgifternas riktighet, kvalitet och laglighet; (ii) uppfylla alla nödvändiga krav på insyn och laglighet enligt tillämplig lag för insamling och användning av personuppgifterna, inklusive att erhålla nödvändiga samtycken och tillstånd från registrerade personer eller på annat sätt; (iii) säkerställa att den personuppgiftsansvarige har rätt att överföra eller ge tillgång till personuppgifterna till databehandlaren och att den personuppgiftsansvarige har lämnat alla nödvändiga meddelanden och erhållit alla nödvändiga samtycken och/eller auktorisationer i samband med överföringen eller åtkomst och mer allmänt, för bearbetning i enlighet med villkoren i EULA (inklusive denna DPA); och (iv) se till att dess instruktioner överensstämmer med gällande lagar. På begäran av databehandlaren ska den personuppgiftsansvarige inom tre (3) arbetsdagar tillhandahålla databehandlaren skriftliga bevis på sådana meddelanden, samtycken och tillstånd. Den personuppgiftsansvarige kommer inte att mata in till bearbetningstjänsterna eller på annat sätt förse databehandlaren med några särskilda kategorier av personuppgifter, såvida inte annat skriftligen överenskommits separat av den personuppgiftsansvarige. Den personuppgiftsansvarige kommer att informera databehandlaren omedelbart och utan onödigt dröjsmål om den personuppgiftsansvarige inte kan uppfölja sina skyldigheter som anges i denna DPA. Den auktoriserade användaren är ensam ansvarig för att granska bearbetningstjänsterna, inklusive eventuell tillgänglig säkerhetsdokumentation och funktioner, för att avgöra om de uppfyller auktoriserade användares krav, affärsbehov och juridiska skyldigheter.

3.3 Den personuppgiftsansvarige ger databehandlaren tillstånd att anonymisera de personuppgifter som behandlas i enlighet med EULA för att härleda analysdata med avseende på användningen av licensierad applikation och Lincoln produkter och utrustning. Vidare användning av de resulterande statistiska uppgifterna av databehandlaren är inte föremål för förhandsgodkännande från den personuppgiftsansvarige.

4. INTERNATIONELLA DATAÖVERFÖRINGAR

4.1 Den personuppgiftsansvarige bekräftar och godkänner härmed att databehandlaren, för att tillhandahålla bearbetningstjänsterna enligt EULA, kan databehandlaren överföra och behålla personuppgifter i USA, och alla andra länder där databehandlaren är belägen, i syfte att tillhandahålla bearbetningstjänsterna. Under tillhandahållandet av behandlingstjänsterna kan det därför vara nödvändigt att överföra personuppgifter till den databehandlare som befinner sig utanför personuppgiftsansvariges etableringsland. Om den personuppgiftsansvarige är belägen i europeiska ekonomiska samarbetsområdet eller i Schweiz åtar sig parterna att tillämpa bestämmelserna i standardavtalsklausulerna för överföring av personuppgifter från den personuppgiftsansvarige (i egenskap av dataexportör enligt standardavtalsklausulerna) till databehandlaren (i egenskap av dataimportör enligt standardavtalsklausulerna).

4.2 Om den personuppgiftsansvarige befinner sig utanför Europeiska ekonomiska samarbetsområdet och Schweiz förbinder sig parterna också att tillämpa bestämmelserna i standardavtalsklausulerna för överföring av personuppgifter från den personuppgiftsansvarige (i egenskap av dataexportör enligt standardavtalsklausulerna) till databehandlaren (i egenskap av dataimportör enligt standardavtalsklausulerna), förutsatt att standardavtalsklausulerna är lagstadgade och tillräckliga för att uppfylla kraven i tillämpliga dataskyddsbestämmelser för överföring av personuppgifter från den personuppgiftsansvarige till Databehandlare enligt EULA.

4.3 Om parterna tillämpar standardavtalsklausulerna enligt avsnitt 4.1 eller 4.2 i denna DPA:

4.3.1 Bilaga 1 till standardavtalsklausulerna ska tillämpas på följande grundval: (a) Dataexportör: Den personuppgiftsansvarige, (b) Dataimportören: Databehandlaren, (c) De registrerade personerna:

personalen hos den personuppgiftsansvarige (den auktoriserade användaren), (d) Datakategorier: uppgifter om användning av produkter och utrustning som ägs, licensieras eller hanteras av databehandlaren, som övervakas av den licensierade applikationen enligt EULA, inklusive registreringsdata (dvs. användarnamn och lösenord) , (e) Särskilda kategorier av personuppgifter: Ej tillämpligt, och (f) Bearbetningsoperationer: insamling, kopiering, överföring, lagring, ändring, radering och andra åtgärder som är nödvändiga för bearbetningstjänsterna enligt EULA.

4.3.2 Beskrivningen av de tekniska, fysiska och organisatoriska säkerhetsåtgärder som genomförts av databehandlaren i egenskap av dataimportör i enlighet med tillägg 2 till standardavtalsklausulerna ska vara i enlighet med schema 2 i denna DPA.

4.4 Om standardavtalsklausulerna är tillämpliga mellan parterna enligt avsnitt 4.1 eller 4.2, kommer deras bestämmelser att anses införlivade genom hänvisning till denna DPA, såvida inte parterna utför standardavtalsklausulerna som ett fristående dokument enligt avsnitt 4.5.

4.5 I den utsträckning som krävs av tillämpliga dataskyddsföreskrifter ska parterna komma överens om och verkställa standardavtalsklausulerna som ett separat dokument.

5. UPPSÄGNING

5.1 Denna DPA kommer att träda i kraft vid ikraftträdandedatumet av EULA.

5.2 Denna DPA upphör automatiskt vid senare upphörande eller utgång av (a) EULA eller (b) av Data behandlarens skyldigheter i förhållande till bearbetningstjänsterna, och sådan uppsägning kräver inte en domstols beslut eller rättsliga förfaranden eller andra åtgärder från databehandlaren, personuppgiftsansvarige eller någon annan part för att vara ändamålsenligt. I förekommande fall, ska databehandlaren vid uppsägning av denna DPA återvända till personuppgiftsansvarige eller radera, på den personuppgiftsansvariges begäran, alla personuppgiftsansvariges personuppgifter i dess besittning eller under dess kontroll. På begäran av den personuppgiftsansvarige ska databehandlaren skriftligen bekräfta överensstämmelse av sådana skyldigheter och radera alla befintliga kopior, om inte tillämplig lag kräver lagring eller på annat sätt tillåter bibehållande av personuppgifterna.

5.3 Den personuppgiftsansvarige har rätt att säga upp denna DPA genom skriftligt meddelande till databehandlaren om databehandlaren är i ett väsentligt eller långvarigt avtalsbrott mot denna DPA, som i händelse av ett brott som kan åtgärdas, inte ska ha åtgärdats inom trettio (30) arbetsdagar från dagen då databehandlaren mottog ett meddelande från den personuppgiftsansvarige som identifierar överträdelsen och kräver att den åtgärdas.

5.4 Databehandlaren har rätt att säga upp denna DPA genom skriftligt meddelande till den personuppgiftsansvarige om den personuppgiftsansvarige har ett väsentligt eller långvarigt avtalsbrott mot denna DPA, som i händelse av ett brott som kan åtgärdas, inte ska ha åtgärdats inom trettio (30) arbetsdagar från dagen då personuppgiftsansvarige mottog ett meddelande från den databehandlare som identifierar överträdelsen och kräver att den åtgärdas.

6. REVISIONER OCH INFORMATIONSFÖRFRÅGNINGAR

6.1. Inom ramen för en (1) revision per år och med förbehåll för underrättelse från den personuppgiftsansvarige med ett trettio (30) dagars förvarning, med undantag för en revision som begärts av en tillsynsmyndighet, den personuppgiftsansvarige kan under ordinarie kontorstid , utan att på ett oskäligt sätt störa databehandlarens affärs verksamhet, personligen granska databehandlaren eller utse en tredjepartsrevisor som är föremål för sekretess för att utföra en sådan revision.

6.2. Databehandlaren ska samarbeta vid en revision enligt detta avsnitt 6 och förse den personuppgiftsansvarige med all information som är nödvändig för att utföra en sådan revision. Den personuppgiftsansvarige ska täcka de kostnader och utgifter som varje part ådrar sig i samband med revisioner enligt detta avsnitt 6.

7. UTNÄMNING AV UNDERENTREPRENÖRER

7.1 Den personuppgiftsansvarige auktoriserar databehandlaren att använda tjänsten av underentreprenörer som listas på sidan tillgänglig på [https://www.lincolnelectric.com/en/Legal-Information/Subprocessors], endast som krävs för utförandet av tjänsterna i samband med EULA.

7.2 Den personuppgiftsansvarige auktoriserar databehandlaren att använda tjänsterna av nya underentreprenörer, med förbehåll för förhandsanmälan till den personuppgiftsansvarige av databehandlaren med ett femton (15) dagars varsel före byte av underentreprenör. Om den personuppgiftsansvarige motsätter sig ändringen av underentreprenören som meddelats, kan den personuppgiftsansvarige under hela uppsägningstiden säga upp denna DPA skriftligen. Om den personuppgiftsansvarige inte upphör inom uppsägningstiden, formaliserar detta den personuppgiftsansvariges samtycke till den meddelade ändringen av underentreprenören.

7.3 Under alla omständigheter, där databehandlaren använder tjänster från en underentreprenör, ska den senare genom kontrakt vara skyldig att uppfylla samma skyldigheter som databehandlaren är bunden till när det gäller personuppgiftsbehandling enligt denna DPA.

8. ÖVRIGA BESTÄMMELSER

8.1 Rättelser eller tillägg till denna DPA måste göras skriftligen för att vara verkningsfulla. Trots det föregående kan databehandlaren när som helst och utan föregående meddelande till den personuppgiftsansvarige, ändra de tekniska, fysiska och organisatoriska åtgärderna i schema 2, förutsatt att en sådan rättelse inte påverkar väsentligt säkerheten, sekretessen eller integriteten av personuppgifter.

8.2. Hänvisningar i denna DPA till "skrift" eller "skrivna" inkluderar e-postkommunikationer och certifierad post.

8.3 Om någon bestämmelse i denna DPA är eller blir ogiltig, ska detta inte påverka giltigheten av de återstående villkoren. I händelse av ogiltigförklaring av en bestämmelse i denna DPA ska parterna under alla omständigheter i god tro sträva efter att ersätta den ogiltigförklarade bestämmelsen med en annan, verkställbar, giltig och laglig, som har i största möjliga utsträckning en rättslig inverkan lika eller motsvarande den i den ursprungliga bestämmelsen.

8.4 Denna DPA regleras av samma styrande lag som EULA.

SCHEMA 1 - JURISDIKTIONSSPECIFIKA VILLKOR

När den personuppgiftsansvarige är etablerad i en av de jurisdiktioner som anges i detta schema 1 gäller följande villkor för DPA, och sådana villkor ska ersätta och kontrollera, i händelse av konflikt med de andra bestämmelserna i dataskyddsförordningen. Alla villkor i EULA som inte är specifikt modifierade av de tillämpliga jurisdiktionsspecifika villkoren i detta schema förblir oförändrade och i full kraft och verkan.

Brasilien:

Parterna bekräftar och är överens om att följande ändring av DPA ska gälla:

a) Alla förekomster av "Särskilda kategorier av personuppgifter" i DPA ska ersättas med "känsliga personuppgifter".

Mexiko:

Parterna bekräftar och är överens om att följande ändringar av DPA ska gälla:

a) Alla förekomster av "Särskilda kategorier av personuppgifter" i DPA ska ersättas med "känsliga personuppgifter";
b) För tillämpning av standardavtalsklausulerna ska alla hänvisningar till "överföringar" av personuppgifter tolkas som eftergifter av personuppgifter i enlighet med mexikansk federal lag om skydd av personuppgifter som innehas av de privata parterna (*"Ley Federal de Protección de Datos Personales en Posesión de los Particulares"*).

Ryssland:

Utöver bestämmelserna i DPA förbinder sig parterna på följande sätt:

a) Databehandlaren bekräftar härmed att han är fullt medveten om att syftet med personuppgiftsbearbetningen enligt DPA endast är att tillhandahålla bearbetningstjänsterna och ska behandla personuppgifterna endast för det ändamål för vilket personuppgifterna lämnas ut och personuppgiftsansvarige kräver det från databehandlaren. Dessutom ska databehandlaren omedelbart skriftligen bekräfta att denna regel iakttas på begäran av den personuppgiftsansvarige.
b) Innan personuppgifterna från ryska medborgare avslöjas för databehandlaren ska den personuppgiftsansvarige se till att alla sådana personuppgifter har registrerats, systematiserats, ackumulerats, lagrats, förtydligats (uppdaterats, ändrats) och extraherats med användning av databaser som finns på ryska federationens territorium när sådana personuppgifter samlades in på något sätt, inklusive via Internet.
c) Om den personuppgiftsansvarige upptäcker olaglig behandling eller felaktigheter i personuppgifterna, ska den personuppgiftsansvarige omedelbart instruera databehandlaren att blockera dessa personuppgifter och inleda en inspektion. De berörda personuppgifterna ska blockeras under hela inspektionsperioden. Om inspektionen bekräftar att personuppgifterna är felaktiga, ska den personuppgiftsansvarige begära den berörda registrerade personen (vederbörandes representant) eller dataskyddsmyndigheten (om tillämpligt) för rättelserna och vidarebefordra dem till databehandlaren. Felaktiga personuppgifter ska rättas inom kort, och senast inom sju (7) arbetsdagar, från den dag då rättelserna lämnades till databehandlaren. Blockering av personuppgifterna ska hävas omedelbart vid rättelse.
d) Om det upptäcks att personuppgifterna behandlas olagligt, ska den personuppgiftsansvarige instruera databehandlaren att stoppa sådan olaglig behandling inom tre (3) arbetsdagar från detekteringsdatumet. Om det verkar vara omöjligt att eliminera överträdelserna och säkerställa lagligheten av personuppgiftsbehandlingen, ska den personuppgiftsansvarige instruera databehandlaren att förstöra de olagligt behandlade personuppgifterna inom tio (10) arbetsdagar från detekteringsdatumet. Den personuppgiftsansvarige är också skyldig att underrätta den berörda registrerade personen (vederbörandes representant) och när det krävs enligt lag, dataskyddsmyndigheten om eliminering av kränkningarna.
e) Om en registrerad återkallar sitt samtycke till personuppgiftsbehandlingen, ska den personuppgiftsansvarige omedelbart meddela databehandlaren och databehandlaren ska stoppa behandlingen och förstöra personuppgifterna för den registrerade personen inom trettio (30) dagar från datumet personuppgiftsansvarige mottog meddelandet om annullering.
f) Om det är omöjligt att följa tidsperioderna som anges i klausulerna d) och e) här ovan, ska databehandlaren blockera relevanta personuppgifter på begäran av den personuppgiftsansvarige i högst sex (6) månader och förstöra dessa personuppgifter inom samma period om inte tillämplig lag föreskriver annat.

Sydafrika:
Parterna bekräftar och är överens om att följande ändringar i DPA ska tillämpas med avseende på definitionerna försedda i avsnitt 1 i DPA:

a) Med ”registrerad person” avses en person vars personuppgifter behandlas.
b) ”Personuppgifter” avser personlig information enligt definitionen i POPIA, inklusive all information som rör en identifierad eller identifierbar individ.
c) ”POPIA” betyder Sydafrikanskt skydd av personuppgifter lag 4 från 2013 och alla bindande föreskrifter, direktiv, beslut, förordningar eller riktlinjer som publiceras under POPIA.

USA:
Utöver bestämmelserna i DPA förbinder sig parterna på följande sätt:

a) Varje part bekräftar och samtycker till att insamling och utlämnande av personuppgifter som överförs till bearbetningstjänsterna (i) utgör inte och är inte avsikten av endera parten att sådan verksamhet ska utgöra en försäljning av personuppgifter, och (ii) om ersättning, monetär eller på annat sätt, tillhandahålls av den auktoriserade användaren till databehandlaren, sådan ersättning, monetär eller på annat sätt, tillhandahålls så för användning av bearbetningstjänsterna och inte för utlämnande av personuppgifter. Databehandlaren får inte behålla, använda, avslöja eller sälja personuppgifter för något annat ändamål än för det specifika syftet att utföra bearbetningstjänsterna, eller på annat sätt tillåtet enligt lag eller EULA. För att undanröja alla tvivel ska databehandlaren inte sälja personuppgifter eller auktorisera eller på annat sätt tillåta någon underentreprenör att utföra samma sak, om inte annat tillåts av EULA eller tillämplig lag.

Schema 2 - Säkerhetsåtgärder som genomförs av databehandlaren

1. Fysisk tillträdeskontroll till lokaler och anläggningar

Databehandlaren kommer att genomföra tekniska och organisatoriska åtgärder för att kontrollera åtkomst till lokaler och anläggningar, särskilt för att kontrollera tillstånd och säkra förhindrandet av obehörig åtkomst.

Specifikt:

- Åtkomstkontrollsystem
- ID -läsare, magnetkort, chipkort
- Utfärdande av nycklar
- Dörrlåsning
- Säkerhetspersonal, vakter
- Övervakningsanläggningar
- Larmsystem, video/CCTV -monitor

2. Åtkomstkontroll till system

Databehandlaren kommer att genomföra tekniska (ID/lösenordsäkerhet) och organisatoriska åtgärder för användaridentifiering och autentisering för att förhindra obehörig åtkomst till IT -system.

Specifikt:

- Lösenordsprocedurer (inkl. specialtecken, minsta längd, byte av lösenord)
- Automatisk blockering (till exempel lösenord eller timeout)
- Kryptering av datamedier, inklusive flyttbara och bärbara.

3. Logisk åtkomstkontroll till data

Databehandlaren kommer att säkerställa att aktiviteter i IT-system som inte omfattas av de tilldelade åtkomsträttigheterna kommer att förhindras genom att använda kravstyrd definition av auktoriseringsschemat och åtkomsträttigheter, och övervakning och loggning av åtkomster.

Specifikt:

- Rollbaserade åtkomsträttigheter (profiler, roller, transaktioner och objekt)
- Användning av en kommersiell privilegierad kontohantering lösning för att underlätta säker autentisering av administrativa konton till system för underhåll eller andra administrativa ändamål
- Automatiserade rapporter som regelbundet granskas och följs upp för avvikande eller misstänkt aktivitet
- Åtkomst, med hjälp av en modell med minst privilegier för att endast tillåta åtkomst till system och/eller data baserat på behov att veta

4. Avslöjande och dataskyddskontroll

Databehandlaren kommer att kontrollera avslöjande av personuppgifter genom att införliva åtgärder för att transportera, överföra och kommunicera eller lagra data på datamedier (manuellt eller elektroniskt) och för efterföljande kontroll via elektronisk överföring, datatransport och överföringskontroll.

Specifikt:

- Kryptering/tunneling
- Elektronisk signatur
- Loggning och kontinuerlig övervakning av säkerhetshändelser och varningar
- Transportsäkerhet för att kryptera data i transit
- Kryptering av data i vila
- Regelbunden rotation av krypteringsnycklar
- Begränsning av åtkomst till krypteringsnycklar för begränsade personer
- Lösenordskomplexitet aktiverat, med tvåfaktorsautentisering som krävs för alla fjärråtkomstsessioner

5. Indatakontroll

Databehandlaren kommer att behålla fullständig dokumentation av datahantering och underhåll måste upprätthållas, inklusive åtgärder för efterföljande kontroll av om data har matats in, ändrats eller tagits bort (raderats), och av vem:

Specifikt:

- Loggning och rapporteringssystem

6. Jobbkontroll

Databehandlaren kommer att behandla personuppgifter enligt den personuppgiftsansvariges instruktioner och för att överensstämma med åtgärder (tekniska/organisatoriska) för att separera ansvaret mellan den personuppgiftsansvarige och databehandlaren: Specifikt:

- Otvetydig formulering av kontraktet
- Formell driftsättning (begäran)
- Kriterier för att välja databehandlare
- Övervakning av kontrakt prestanda

7. Tillgänglighetskontroll

Databehandlaren kommer att se till att data skyddas mot oavsiktlig eller skadlig förstörelse eller förlust genom att vidta åtgärder för att säkerställa den fysiska och logiska säkerheten av data.

Specifikt:

- Säkerhetskopieringsprocedurer
- Spegling av hårddiskar, till exempel RAID -teknik
- Avbrottsfri strömförsörjning (UPS)
- Fjärr- eller diskbaserad lagring som replikeras till alternativa datacenter
- Antivirus- och/eller anti-malware-programvara som uppdateras regelbundet och applikationsmedvetna brandväggssystem konfigurerade med standard förnekande uttalanden, vilket endast tillåter trafik som uttryckligen är tillåten för affärsändamål
- Affärs kontinuitet och katastrofåterhämtningsplan

8. Segregeringskontroll

Databehandlaren kommer att försöka se till att data som samlas in för olika ändamål kommer att behandlas separat och inte blandas med andra kunddata genom att genomföra specifika åtgärder för separat behandling (lagring, rättning, radering, överföring) av data för olika ändamål:

Specifikt:

- ”Intern klient” -koncept / användningsbegränsning
- Funktionssegregering (produktion/testning)