SIST OPPDATERT: 22. juni 2021

Tillegg for databehandlingsvilkår

Dette tillegget for databehandling ("**DPA**") er et tillegg til The Lincoln Electric Company-sluttbrukerlisensavtalen ("**EULA**") og gjelder mellom The Lincoln Electric Company ("**Databehandleren**") og den autoriserte brukeren i henhold til EULA ("**Datakontrolløren**"), (hver en "**Part**", og sammen "**Partene**").

HVORVED

EULA regulerer retten for den autoriserte brukeren til å bruke den lisensierte applikasjonen og, etter behov, andre online tjenester som leveres av Lincoln Electric Company. For å oppfylle sine forpliktelser i henhold til EULA, skal Lincoln Electric Company fungere som databehandler på vegne av den autoriserte brukeren. For å sikre overholdelse av personopplysningsforskriftene har partene blitt enige om å supplere EULA for å angi vilkårene og betingelsene som gjelder for behandling av personopplysninger av databehandleren på vegne av den behandlingsansvarlige.

PARTENE BLE ENIGE OM FØLGENDE

1. DEFINISJONER

1.1 I dette databehandlingstillegget skal definisjoner med store bokstaver ha følgende betydninger, med mindre de er definert i EULA eller på annen måte kreves gitt konteksten:

"**Datakontrollør"**	betyr enheten som bestemmer formålene og midlene for behandling av personopplysninger;
"Databehandler"	betyr enheten som behandler personopplysninger på vegne av datakontrolløren;
"Registrert person"	betyr en identifisert eller identifiserbar person hvis personopplysninger blir behandlet;
"Instruksjon"	betyr instruksjonene fra datakontrolløren til databehandleren for å behandle personopplysninger i henhold til levering av tjenester i samsvar med EULA;
"Personopplysninger"	betyr all informasjon knyttet til et identifisert eller identifiserbart individ; en identifiserbar person er en som kan identifiseres, direkte eller indirekte, spesielt ved henvisning til en identifikator, for eksempel et navn, et identifikasjonsnummer, plasseringsdata, en elektronisk identifikator eller en eller flere faktorer som er spesifikke for hans eller hennes fysisk, fysiologisk, genetisk, mental, økonomisk, kulturell eller sosial identitet;
"Brudd på personopplysninger"	betyr brudd på sikkerheten som fører til utilsiktet eller ulovlig ødeleggelse, tap, endring, uautorisert avsløring eller tilgang til, Personopplysninger som overføres, lagres eller behandles på annen måte;
"Behandle" /"Behandling" /"Behandlet"	betyr enhver handling som utføres med personopplysninger som innsamling, registrering, organisering, lagring, tilpasning eller endring, henting, konsultasjon, bruk, avsløring ved overføring, formidling, overføring eller på annen måte tilgjengeliggjøring, justering eller kombinasjon, begrensning, sletting eller ødeleggelse;
"Behandlingstjenester"	betyr behandling av personopplysninger av databehandleren i forbindelse med EULA;
"Spesielle kategorier av personopplysninger"	betyr alle personopplysninger som avslører rasemessig eller etnisk opprinnelse, politiske meninger, religiøs eller filosofisk overbevisning, eller medlemskap i fagforening, foreninger eller stiftelser, utseende, straffbare kriminalsaker og sikkerhetstiltak, finansiell og eiendomsinformasjon, informasjon om oppholdssted eller kredittinformasjon og behandling av genetiske data, biometriske data for å identifisere en fysisk person på en unik måte, data om helse eller data om en fysisk persons seksualliv eller seksuell orientering eller data om mindreårige i alderen 14 år eller yngre;

"Standard kontraktsklausuler"	betyr standard kontraktsklausuler vedtatt av EU-kommisjonens beslutning 2010/87 av 5. februar 2010 om standard kontraktsklausuler for overføring av personopplysninger til behandlere etablert i tredjeland eller et annet sett med standardklausuler som avtales mellom partene. Når den behandlingsansvarlige er etablert i en jurisdiksjon utenfor EU, skal henvisningene til medlemslandene i de materielle bestemmelsene i standardavtaleklausulene tolkes som henvisninger til jurisdiksjonen der den behandlingsansvarlige er etablert;
"Underbehandler"	betyr enhver behandler som er engasjert av databehandleren (eller av en annen underbehandler til databehandleren) for å behandle personopplysninger på vegne av datakontrolløren i samsvar med instruksjonene og vilkårene i den skriftlige underkontrakten.

1.2 Tekstene og avsnittoverskrifter er kun ment som referanse og for bekvemmelighet, er ikke en del av dette databehandlingstillegget og skal ikke brukes til å tolke dette databehandlingstillegget.

2. OMFANG OG BRUK AV DETTE DATABEHANDLINGSTILLEGGET

2.1 Denne DPA kompletterer bare bestemmelsene i EULA i forhold til behandlingstjenestene som leveres av databehandleren til datakontrolløren i henhold til EULA.

3. DATABEHANDLING

3.1 Databehandleren godtar å behandle personopplysningene i samsvar med vilkårene og betingelsene i dette databehandlingstillegget, og spesielt betyr at databehandleren:

3.1.1 behandler personopplysningene kun på vegne av datakontrolløren og til enhver tid i samsvar med databehandlerens instruksjoner som definert i dette databehandlingstillegget, og alle gjeldende databeskyttelseslover;

3.1.2 sikrer at alt personell som er betrodd behandlingstjenestene har forpliktet seg til taushetsplikt eller er underlagt en lovfestet taushetsplikt;

3.1.3 tar tekniske, fysiske og organisatoriske tiltak for å sikre sikkerheten og konfidensialiteten til personopplysningene og på en passende måte beskytte personopplysninger som behandles på vegne av datakontrolløren mot misbruk og tap, som angitt i tillegg 2 til dette databehandlingstillegget;

3.1.4 straks vil varsle den behandlingsansvarlige om: (a) enhver juridisk bindende forespørsel om offentliggjøring av personopplysningene fra en myndighet med mindre annet er forbudt, for eksempel et forbud i henhold til straffeloven for å bevare konfidensialiteten til en rettshåndhevelse eller undersøkelse av immateriell eiendom, (b) ethvert brudd på personopplysninger som påvirker personopplysningene som behandles på vegne av den behandlingsansvarlige, (c) enhver forespørsel mottatt direkte fra de registrerte (inkludert rettigheter til tilgang, retting, sletting, innsigelse, begrensning, dataoverføring og rettighet ikke å bli objekt for en beslutning som utelukkende er basert på automatisert behandling, inkludert profilering); Databehandleren (i) vil ikke svare direkte på forespørselen, bortsett fra å varsle den registrerte at den handler på vegne av den behandlingsansvarlige og å gi den registrerte kontaktinformasjonen til den behandlingsansvarlige, og (ii) ta under hensyn til behandlingens art, vil hjelpe den behandlingsansvarlige med passende tekniske, fysiske og organisatoriske tiltak, så langt dette er mulig, for å oppfylle den dataansvarliges forpliktelse til å svare på forespørsler om utøvelse av den registrertes rettigheter;

3.1.5 tilbyr kommersielt rimelig samarbeid til datakontrolløren for å hjelpe datakontrolløren med å overholde sine egne juridiske forpliktelser knyttet til personopplysningssikkerhet, for eksempel: melding om et brudd på personopplysninger til den kompetente tilsynsmyndigheten, kommunikasjon av slike brudd på personopplysninger til berørte personer og, hvor det er aktuelt, implementering av konsekvensanalyser av databeskyttelse og tidligere konsultasjoner med tilsynsmyndigheter, under hensyntagen til behandlingens art og informasjonen som er tilgjengelig for databehandleren;

3.1.6 gjør tilgjengelig for datakontrolløren all informasjon som er nødvendig for å bevise overholdelse av forpliktelsene i denne databeskyttelsesforordningen og tillate og bidra til revisjoner, inkludert inspeksjoner, utført av datakontrolløren eller en annen revisor som er pålagt av datakontrolløren som angitt i avsnitt 6; og,

3.1.7 at alle behandlingstjenester utført av en underbehandler vil bli utført i samsvar med avsnitt 7.

3.2 Når det gjelder behandlingstjenestene, vil datakontrolløren være ansvarlig for å overholde alle krav som gjelder for den i henhold til gjeldende lov om behandling av personopplysninger og instruksjonene den gir til databehandleren. Spesielt, men med forbehold for det generelle i det ovennevnte, anerkjenner og godtar den behandlingsansvarlige at den er eneansvarlig for følgende: (i) nøyaktigheten, kvaliteten og lovligheten av personopplysninger; (ii) overholdelse av alle nødvendige krav til åpenhet og lovlighet under gjeldende lov for innsamling og bruk av personopplysningene, inkludert innhenting av nødvendige samtykker og autorisasjoner fra registrerte eller på annen måte; (iii) å sikre at den behandlingsansvarlige har rett til å overføre, eller gi tilgang til, personopplysningene til databehandleren og at den behandlingsansvarlige har gitt alle nødvendige varsler og innhentet nødvendige samtykker og/eller autorisasjoner i forbindelse med overføringen eller tilgang og, mer generelt, for behandling i samsvar med vilkårene i EULA (inkludert denne DPA); og (iv) sikre at instruksjonene er i samsvar med gjeldende lover. På forespørsel fra databehandleren skal datakontrolløren innen tre (3) virkedager levere databehandleren skriftlig bevis på slike varsler, samtykker og autorisasjoner. Datakontrolløren vil ikke legge inn noen spesielle kategorier av personopplysninger i behandlingstjenestene, eller på annen måte gi databehandleren, med mindre annet er skriftlig avtalt separat av datakontrolløren. Datakontrolløren vil informere databehandleren umiddelbart og uten unødig forsinkelse hvis datakontrolløren ikke er i stand til å overholde sine ansvar i dette databehandlingstillegget. Den autoriserte brukeren er eneansvarlig for å gjennomgå behandlingstjenestene, inkludert tilgjengelig sikkerhetsdokumentasjon og funksjoner, for å avgjøre om de tilfredsstiller den Autoriserte brukerens krav, forretningsbehov og juridiske forpliktelser.

3.3 Datakontrolløren gir databehandleren fullmakt til å anonymisere personopplysningene som behandles i henhold til EULA for å utlede analysedata knyttet til bruk av lisensiert applikasjon og Lincoln-produkter og utstyr. Videre bruk av de resulterende statistiske dataene fra databehandleren er ikke betinget av forhåndsgodkjenning fra datakontrolløren.

4. INTERNASJONALE DATAOVERFØRINGER

4.1 Datakontrolløren erkjenner og godtar herved at databehandleren for overføring av behandlingstjenestene i henhold til EULA kan overføre og beholde personopplysninger i USA, og ethvert annet land der databehandleren befinner seg, med det formål å levere behandlingstjenestene. Derfor, i løpet av levering av behandlingstjenestene, kan det være nødvendig å overføre personopplysninger til databehandleren som befinner seg utenfor landet der datakontrolløren er etablert. Hvis datakontrolløren er lokalisert i Det europeiske økonomiske samarbeidsområdet eller i Sveits, forplikter partene seg til å anvende bestemmelsene i standardavtaleklausulene for overføring av personopplysninger fra datakontrolløren (opptrer som dataeksportør i henhold til standardavtaleklausulene) til databehandleren (opptrer som dataimportør i henhold til standardavtaleklausulene).

4.2 Hvis den behandlingsansvarlige befinner seg utenfor Det europeiske økonomiske samarbeidsområdet og Sveits, forplikter partene seg også til å anvende bestemmelsene i standardavtaleklausulene for overføring av personopplysninger fra den behandlingsansvarlige (som handler som dataeksportør i henhold til standardavtaleklausulene) til databehandleren (handler som dataimportør i henhold til standardavtaleklausulene), forutsatt at standardavtaleklausulene er lovpålagt og tilstrekkelig for å oppfylle kravene i de gjeldende databeskyttelsesforskriftene for overføring av personopplysninger fra den behandlingsansvarlige til Databehandler i henhold til EULA.

4.3 Hvis partene anvender standardavtaleklausulene i henhold til avsnitt 4.1 eller 4.2 i dette databehandlingstillegget:

4.3.1 Vedlegg 1 til standardavtaleklausulene skal brukes på følgende grunnlag: (a) Dataeksportør: den behandlingsansvarlige, (b) Dataimportøren: databehandleren, (c) den registrerte: personell til den behandlingsansvarlige (den autoriserte brukeren), (d) Datakategorier: data knyttet til bruk av produkter og utstyr som eies, lisensieres eller administreres av databehandleren, som overvåket av den lisensierte applikasjonen i henhold til EULA, inkludert registreringsdata (dvs. brukernavn og passord) ,

(e) Spesielle kategorier av personopplysninger: I/A, og (f) Behandlingsoperasjoner: innsamling, kopiering, overføring, lagring, endring, sletting og andre operasjoner som er nødvendige for behandlingstjenestene i henhold til EULA.

4.3.2 Beskrivelsen av de tekniske, fysiske og organisatoriske sikkerhetstiltakene som iverksettes av databehandleren som opptrer som dataimportør i henhold til vedlegg 2 i standardavtaleklausulene, skal være som angitt i tillegg 2 til denne databeskyttelsesforordningen.

4.4 Hvis standardavtaleklausulene er gjeldende mellom partene i henhold til avsnitt 4.1 eller 4.2, vil deres bestemmelser bli ansett som inkorporert ved henvisning til dette databehandlingstillegget, med mindre partene utfører standardavtaleklausulene som et frittstående dokument i henhold til avsnitt 4.5.

4.5 I den grad det kreves av gjeldende databeskyttelsesforskrift, skal partene inngå og utføre standard kontraktsklausuler som et eget dokument.

5. AVSLUTNING

5.1 Dette databehandlingstillegget trer i kraft på ikrafttredelsesdatoen for EULA.

5.2 Denne databeskyttelsesavtalen avsluttes automatisk ved senere avslutning eller utløp av (a) EULA eller (b) av databehandlerens forpliktelser i forhold til behandlingstjenestene, og slik oppsigelse krever ikke rettskjennelse eller rettslig behandling eller andre handlinger for databehandleren, datakontrolløren eller en annen part for å tre i kraft. Når det er aktuelt, ved opphør av dette databehandlingstillegget, skal databehandleren returnere til datakontrolløren eller slette, etter datakontrollørens forespørsel, alle datakontrollørens personopplysninger som er i besittelse eller under dens kontroll. På forespørsel fra datakontrolløren skal databehandleren skriftlig bekrefte overholdelsen av slike forpliktelser og slette alle eksisterende kopier, med mindre gjeldende lov krever lagring eller på annen måte tillater oppbevaring av personopplysningene.

5.3 Datakontrolløren har rett til å avslutte denne databehandlingsvilkår ved skriftlig melding til databehandleren hvis databehandleren har gjort et vesentlig eller vedvarende brudd på denne databehandlingsvilkår, som i tilfelle brudd skaper grunnlag for rettelse, ikke skal ha blitt rettet innen tretti (30) virkedager fra datoen for databehandlerens mottak av et varsel fra datakontrolløren som identifiserer bruddet og krever at det blir rettet.

5.4 Databehandleren har rett til å avslutte denne databehandlingsvilkår ved skriftlig melding til datakontrolløren hvis datakontrolløren har gjort et vesentlig eller vedvarende brudd på denne databehandlingsvilkår, som i tilfelle brudd skaper grunnlag for rettelse, ikke skal ha blitt rettet innen tretti (30) virkedager fra datoen for datakontrollørens mottak av et varsel fra databehandleren som identifiserer bruddet og krever at det blir rettet.

6. REVISJONER OG INFORMASJONSFORSKRIFTER

6.1. Innen begrensning på en (1) revisjon per år og underlagt varsel fra datakontrolløren med en tretti (30) dagers forhåndsvarsel, unntatt i tilfelle en revisjon som en tilsynsmyndighet ber om, kan datakontrolløren under vanlige åpningstimer, uten å urimelig forstyrre databehandlerens forretningsdrift, personlig revidere databehandleren eller oppnevne en tredjepartsrevisor som er underlagt taushetsplikt for å utføre slik revisjon.

6.2. Databehandleren skal samarbeide ved revisjon i henhold til dette avsnitt 6 og gi datakontrolløren all informasjon som er nødvendig for å utføre slik revisjon. Datakontrolløren skal dekke kostnadene og utgiftene som hver part påløper i forbindelse med revisjoner i henhold til dette avsnitt 6.

7. VALG AV UNDERBEHANDLERE

7.1 Datakontrolløren gir databehandleren fullmakt til å bruke tjenesten til underbehandlere som er oppført på siden som er tilgjengelig på [https://www.lincolnelectric.com/en/Legal-Information/Subprocessors], utelukkende etter behov for utførelsen av tjenestene i forbindelse med EULA.

7.2 Datakontrolløren gir databehandleren fullmakt til å bruke tjenestene til nye underprosessorer, med forbehold om forhåndsvarsel til datakontrolløren av databehandleren med et femten (15) dagers varsel før endring av underprosessor. Hvis datakontrolløren protesterer mot endringen av underprosessoren som er varslet, kan datakontrolløren i hele varslingsperioden avslutte denne DPA skriftlig. Hvis datakontrolløren ikke avslutter

avtalen innen avslutningstiden, formaliserer dette samtykke fra datakontrolløren til den varslede endringen av underbehandleren.

7.3 Under alle omstendigheter, der databehandleren bruker tjenestene til en underbehandler, skal denne i henhold til kontrakt binde seg til de samme forpliktelsene som databehandleren er bundet til når det gjelder behandling av personopplysninger i henhold til dettee databehandlingstillegget.

8. DIVERSE BESTEMMELSER

8.1 Endringer eller tillegg til denne DPA-avtalen må gjøres skriftlig for å kunne tre i kraft. Uavhengig av det ovennevnte, kan databehandleren når som helst og uten varsel til datakontrolløren endre de tekniske, fysiske og organisatoriske tiltakene som er angitt i tillegg 2, forutsatt at en slik endring ikke vesentlig påvirker sikkerheten, konfidensialiteten eller integriteten til personopplysninger .

8.2. Henvisninger i denne DPA til "skriving" eller "skrift" inkluderer e-postkommunikasjon og sertifisert post.

8.3 Skulle en bestemmelse i denne DPA være eller bli ugyldig, skal dette ikke påvirke gyldigheten av de resterende vilkårene. I tilfelle ugyldighet av en bestemmelse i dette databehandlingstillegget, skal partene uansett i god tro forsøke å erstatte den ugyldige bestemmelsen med en annen, som kan håndheves, er gyldig og lovlig, og i størst mulig grad har juridisk innvirkning lik eller tilsvarende den i den opprinnelige bestemmelsen.

8.4 Denne DPA er underlagt samme gjeldende lov som EULA.

VEDLEGG 1 - SPESIFIKKE VILKÅR FOR JURISDIKSJON

Når datakontrolløren er etablert i en av jurisdiksjonene som er oppført i dette vedlegg 1, gjelder følgende vilkår for DPA, og slike vilkår skal erstatte og overveie i tilfelle konflikt med de andre bestemmelsene i DPA. Alle vilkårene i EULA som ikke er spesifikt endret av de gjeldende jurisdiksjonsspesifikke vilkårene i dette vedlegg, forblir uendret og har full kraft.

Brasil:
Partene erkjenner og er enige om at følgende endring av DPA skal gjelde:

a) Alle forekomster av "Spesielle kategorier av personopplysninger" i DPA skal erstattes med "Sensitive personopplysninger".

Mexico:
Partene erkjenner og er enige om at følgende endring av DPA skal gjelde:

a) Alle forekomster av "Spesielle kategorier av personopplysninger" i DPA skal erstattes med "Sensitive personopplysninger".
b) For anvendelse av standardavtaleklausulene skal alle henvisninger til "overføringer" av personopplysninger tolkes som ettergivelser av personopplysninger i samsvar med meksikansk føderal lov om beskyttelse av personopplysninger som innehas av private parter ("*Ley Federal de Protección de Datos Personales en Posesión de los Particulares ").*

Russland:
I tillegg til bestemmelsene i DPA, forplikter partene seg som følger:

a) Databehandleren bekrefter herved at den er fullstendig klar over at formålet med behandling av personopplysningene i henhold til databeskyttelsesforordningen kun er å tilby behandlingstjenestene og skal behandle personopplysningene bare for det formålet som personopplysningene blir gitt for og datakontrolløren krever det fra databehandleren. I tillegg skal databehandleren umiddelbart skriftlig bekrefte at denne regelen overholdes på forespørsel fra datakontrolløren.
b) Før vi avslører personopplysningene fra russiske statsborgere til databehandleren, skal datakontrolløren sikre at alle slike personopplysninger er registrert, systemisert, akkumulert, lagret, klarlagt (oppdatert, endret) og ekstrahert med bruk av databaser som er lokalisert på den russiske føderasjonens territorium hvis slike personopplysninger ble samlet inn på hvilken som helst måte, inkludert via Internett.
c) Hvis datakontrolløren oppdager ulovlig behandling eller unøyaktighet i personopplysningene, skal datakontrolløren umiddelbart instruere databehandleren om å blokkere disse personopplysningene og starte en inspeksjon. De berørte persons opplysningene skal sperres for hele inspeksjonsperioden. Hvis inspeksjonen bekrefter unøyaktigheten av personopplysningene, skal datakontrolløren be den relevante registrerte personen (hans/hennes representant) eller databeskyttelsesmyndigheten (hvis aktuelt) om endringene og videresende dem til databehandleren. Unøyaktige personopplysninger skal endres innen kort tid, og senest innen syv (7) virkedager, fra dagen da endringene ble levert til databehandleren. Personopplysningene skal avblokkeres umiddelbart etter endring.
d) Hvis det oppdages at personopplysningene behandles ulovlig, skal datakontrolløren instruere databehandleren om å stoppe slik ulovlig behandling innen tre (3) virkedager fra datoen for oppdagelsen. Hvis det ser ut til å være umulig å eliminere bruddene og sikre at personopplysningsbehandlingen er lovlig, skal datakontrolløren instruere databehandleren om å ødelegge de ulovlig behandlede personopplysningene innen ti (10) virkedager fra datoen for oppdagelsen. Datakontrolløren er også forpliktet til å varsle den aktuelle registrerte (hans/hennes representant) og, når loven krever det, databeskyttelsesmyndigheten om eliminering av bruddene.
e) Hvis en registrert person tilbakekaller sitt samtykke til behandling av personopplysninger, skal datakontrolløren umiddelbart varsle databehandleren, og databehandleren skal stoppe behandlingen og ødelegge personopplysningene til denne registrerte personen innen tretti (30) dager fra datoen for mottak av oppsigelsesvarselet.
f) Hvis det er umulig å overholde tidsperiodene angitt i klausulene d) og e) her ovenfor, skal databehandleren blokkere de relevante personopplysningene på forespørsel fra datakontrolløren i høyst seks (6) måneder og ødelegge disse personlige data innen samme periode med mindre gjeldende lov foreskriver noe annet.

Sør-Afrika:

Partene erkjenner og er enige om at følgende endringer i DPA skal gjelde med hensyn til definisjonene i avsnitt 1 i DPA:

a) "Datasubjekt" betyr en person hvis personopplysninger blir behandlet.
b) "Personopplysninger" betyr personlig informasjon som definert i POPIA, inkludert all informasjon knyttet til et identifisert eller identifiserbart individ.
c) "POPIA" betyr sørafrikansk beskyttelse av personopplysningsloven 4 fra 2013, og enhver bindende forskrift, direktiv, kjennelse, pålegg eller retningslinje publisert under POPIA.

USA:

I tillegg til bestemmelsene i DPA, forplikter partene seg som følger:

a) Hver part erkjenner og godtar at innsamling og avsløring av personopplysninger som overføres til behandlingstjenestene (i) ikke utgjør, og danner ikke intensjonen til noen av partene for slik aktivitet, et salg av personopplysninger, og (ii) hvis verdifull vederlag, økonomisk eller på annen måte, blir gitt av autorisert bruker til databehandleren, slik verdifull vederlag, pengemessig eller på annen måte, er gitt for bruk av behandlingstjenestene og ikke for avsløring av personopplysninger. Databehandler skal ikke oppbevare, bruke, avsløre eller selge personopplysninger for andre formål enn for det spesifikke formålet med å utføre behandlingstjenestene, eller på annen måte tillatt ved lov eller EULA. For å unngå tvil, skal databehandler ikke selge personopplysninger eller autorisere eller på annen måte tillate noen underprosessor å påta seg det samme, med mindre annet er tillatt av EULA eller gjeldende lov.

Vedlegg 2 - Sikkerhetstiltak implementert av databehandleren

1. Fysisk tilgangskontroll til lokaler og fasiliteter

Databehandler vil iverksette tekniske og organisatoriske tiltak for å kontrollere tilgang til lokaler og fasiliteter, spesielt for å kontrollere autorisasjon for å sikre forhindring av uautorisert tilgang.

Nærmere bestemt:

- Adgangskontrollsystem
- ID-leser, magnetkort, chipkort
- Utgave av nøkler
- Dørlås
- Sikkerhetspersonell, vakter
- Overvåkingsanlegg
- Alarmsystem, video/CCTV-skjerm

2. Tilgangskontroll til systemer

Databehandler vil implementere tekniske (ID/passord sikkerhet) og organisatoriske tiltak for brukeridentifikasjon og autentisering for å forhindre uautorisert tilgang til IT-systemer.

Nærmere bestemt:

- Passordprosedyrer (inkl. spesialtegn, minimumslengde, endring av passord)
- Automatisk blokkering (f.eks. passord eller timeout)
- Kryptering av datamedier, inkludert flyttbar og bærbar.

3. Logisk tilgangskontroll til data

Databehandler vil sørge for at aktiviteter i IT-systemer som ikke dekkes av de tildelte tilgangsrettighetene, forhindres ved å bruke kravdrevet definisjon av autorisasjonsordningen og tilgangsrettigheter, og overvåking og logging av tilganger.

Nærmere bestemt:

- Rollebaserte tilgangsrettigheter (profiler, roller, transaksjoner og objekter)
- Bruk av en kommersiell privilegert kontoadministrasjonsløsning for å lette sikker autentisering av administrative kontoer til systemer for vedlikehold eller andre administrative formål
- Automatiserte rapporter som regelmessig gjennomgås og følges opp for unormal eller mistenkelig aktivitet
- Tilgang, ved hjelp av en modell med minst privilegium for å bare tillate tilgang til systemer og/eller data basert på behov-for-tilgang

4. Avsløring og databeskyttelseskontroll

Databehandler vil kontrollere avsløring av personopplysninger ved å inkorporere tiltak for å transportere, overføre og kommunisere eller lagre data på datamedier (manuelt eller elektronisk) og for senere kontroll via elektronisk overføring, datatransport og overføringskontroll.

Nærmere bestemt:

- Kryptering/tunneling
- Elektronisk signatur
- Logging og kontinuerlig overvåking av sikkerhetshendelser og varsler
- Transportsikkerhet for å kryptere data under transport
- Kryptering av lagrede data
- Regelmessig rotasjon av krypteringsnøkler
- Begrensning for tilgang til krypteringsnøkler for begrensede personer
- Passordkompleksitet aktivert, med tofaktorautentisering påkrevd for alle økter med ekstern tilgang

5. Inndata-kontroll

Databehandler vil opprettholde full dokumentasjon av datahåndtering og vedlikehold, inkludert tiltak for senere kontroll av om data er lagt inn, endret eller fjernet (slettet), og av hvem:

Nærmere bestemt:

- Loggings- og rapporteringssystemer

6. Jobbkontroll

Databehandler vil behandle personopplysninger i henhold til datakontrollørens instruksjoner og godta tiltak (tekniske/organisatoriske) for å skille ansvaret mellom datakontrolløren og databehandleren: Nærmere bestemt:

- Entydig formulering av kontrakten
- Formell igangkjøring (forespørselsskjema)
- Kriterier for valg av databehandler
- Overvåking av kontraktsutførelse

7. Tilgjengelighetskontroll

Databehandler vil sikre at data vil bli beskyttet mot utilsiktet eller ondsinnet ødeleggelse eller tap ved å treffe tiltak for å sikre den fysiske og logiske sikkerheten til dataene.

Nærmere bestemt:

- Sikkerhetskopieringsprosedyrer
- Speiling av harddisker, f.eks. med RAID-teknologi
- Avbruddsfri strømforsyning (UPS)
- Ekstern eller diskbasert lagring som replikeres til alternative datasentre
- Anti-virus og/eller anti-malware programvare som oppdateres regelmessig og applikasjonsbevisste brannmursystemer konfigurert med standard nekteserklæringer, slik at bare trafikk eksplisitt er tillatt for forretningsformål
- Forretningskontinuitet og gjenopprettingsplan for katastrofer

8. Segregeringskontroll

Databehandler vil prøve å sikre at data som samles inn for forskjellige formål blir behandlet separat og ikke blandet med andre kundedata ved å implementere spesifikke tiltak for å sørge for separat behandling (lagring, endring, sletting, overføring) av data til forskjellige formål:

Nærmere bestemt:

- "Intern klient" konsept / begrensning av bruk
- Funksjonssegregering (produksjon/testing)