Databehandleraftale

mellem

.....

– den dataansvarlige – herefter kaldet klienten –

og

ALSO A/S

Helgeshøj Allé 8

2630 Tåstrup

– databehandleren – herefter kaldet leverandøren

1. Ordrens eller kontraktens genstand og varighed

(1) Genstand

Genstanden for ordren eller kontrakten vedrørende behandlingen af data er leverandørens udførelse af følgende tjenester eller opgaver: Teknisk support, ordrebehandling, IT-tjenester, kundeservice, skybaserede tjenester.

(2) Varighed

Denne ordres varighed (periode) svarer til serviceaftalens periode inden for rammerne af de respektive produkt-, service-, indkøbs- og/eller arbejdskontrakter.

2. Præcisering af ordrens eller kontraktens detaljer

(1) Den planlagte databehandlings karakter og formål

Detaljeret beskrivelse af genstanden i forbindelse med karakteren af og formålet med de af leverandøren leverede tjenester:

Dataenes art	Behandlingens formål	De registrerede
Personoplysninger: Navn, adresse, kontaktoplysninger, bankkontooplysninger	Ordrebehandling, teknisk support, IT-tjenester, kundeservice, skybaserede tjenester	Medarbejdere hos databehandler, forretningspartner, kunde, sælger, interessenter

Den kontraktligt aftalte databehandling skal udelukkende udføres i et medlemsland i Den Europæiske Union (EU), i et medlemsland i Det Europæiske Økonomiske Samarbejdsområde (EØS) eller i et land, der er omfattet af Europa-Kommissionens beslutning om et tilstrækkeligt beskyttelsesniveau. Hver enkelt overførsel af personoplysninger til et land, der ikke er et medlemsland i enten EU eller EØS, kræver klientens forudgående samtykke og må udelukkende finde sted, hvis de særlige betingelser i artikel 44 ff. i GDPR er opfyldt. Et tilstrækkeligt beskyttelsesniveau i et land, der ikke er et medlemsland i EU, skal garanteres af EU's standardkontraktbestemmelser (artikel 46 stk. 2, litra b og d i EU's GDPR).

(2) Typer af personoplysninger

Genstanden for behandlingen af personoplysninger omfatter følgende typer/kategorier af personoplysninger: Personlige masterdata (primære personoplysninger), kontaktoplysninger, primære kontraktoplysninger (kontraktlige/juridiske forhold, kontrakt- eller produktinteresser), kundehistorik, oplysninger om kontraktfakturering og -betalinger, videregivet information (fra tredjemand, f.eks. kreditoplysningskontorer eller fra offentlige fortegnelser), oplysninger om systemkonfiguration og kundemiljø.

(3) Kategorier af registrerede

Kategorierne af registrerede omfatter: Medarbejdere hos den dataansvarlige, forretningspartneren, kunder, potentielle kunder, abonnenter, medarbejdere, leverandører, kontaktpersoner.

3. Tekniske og organisatoriske foranstaltninger

(1) Før påbegyndelsen af behandlingen skal leverandøren dokumentere, at de nødvendige tekniske og organisatoriske foranstaltninger er blevet gennemført, som er fastsat forud for tildelingen af ordren eller kontrakten, navnlig i forbindelse med den detaljerede udførelse af kontrakten, og skal forelægge disse dokumenterede foranstaltninger for klienten med henblik på inspektion. Ved klientens accept udgør de dokumenterede foranstaltninger kontraktgrundlaget. Såfremt klientens inspektion/revision viser, at der er behov for ændringer, skal sådanne ændringer implementeres efter gensidig aftale.

(2) Leverandøren skal iværksætte sikkerheden i overensstemmelse med artikel 28, stk. 3, litra c og artikel 32 i GDPR navnlig sammenholdt med artikel 5, stk. 1 og stk. 2 i GDPR. De foranstaltninger, der skal gennemføres, er foranstaltninger vedrørende datasikkerhed, og foranstaltninger, der garanterer et passende beskyttelsesniveau i forhold til risikoen vedrørende fortrolighed, integritet, tilgængelighed og systemernes robusthed. Der skal tages hensyn til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder som omhandlet i artikel 32, stk. 1 i GDPR [Detaljer i Bilag 1].

(3) De tekniske og organisatoriske foranstaltninger er underlagt tekniske fremskridt og yderligere udvikling. I den forbindelse er det tilladt leverandøren at implementere alternative passende foranstaltninger. Ved en sådan implementering må de definerede foranstaltningers sikkerhedsniveau ikke reduceres. Væsentlige ændringer skal dokumenteres.

4. Berigtigelse, begrænsning og sletning af personoplysninger

(1) Leverandøren må kun berigtige, slette eller begrænse behandlingen af de personoplysninger, der behandles på vegne af klienten, hvis der foreligger dokumenterede instrukser fra klienten.
Såfremt en registreret kontakter leverandøren direkte vedrørende en berigtigelse, sletning eller begrænsning af behandlingen, skal leverandøren straks fremsende den registreredes anmodning til klienten.

(2) Såfremt det indgår i tjenesternes omfang skal sletningspolitikken, "retten til at blive glemt", berigtigelse, dataoverførbarhed og adgang uden ugrundet ophold sikres af leverandøren i overensstemmelse med dokumenterede instrukser fra klienten.

5. Kvalitetssikring og øvrige forpligtelser, der påhviler leverandøren

Ud over at overholde bestemmelserne i nærværende ordre eller kontrakt skal leverandøren overholde de lovkrav, der henvises til i artikel 28-33 i GDPR. Tilsvarende skal leverandøren navnlig sikre overholdelse af følgende krav:

a) Udpeget databeskyttelsesrådgiver, som varetager sine forpligtelser i overensstemmelse med artikel 38 og 39 i GDPR.

   Databeskyttelsesrådgiverens kontaktoplysninger skal altid være tilgængelige og lette at finde på leverandørens websted. ALSO A/S' databeskyttelsesrådgiver kan altid kontaktes på DPO.DK@ALSO.COM

b) Fortrolighed i overensstemmelse med artikel 28, stk. 3, 2. punktum, litra b, artikel 29 og 32 stk. 4 i GDPR. Leverandøren overdrager kun den i nærværende kontrakt anførte databehandling til medarbejdere, som er underlagt fortrolighed, og som tidligere er blevet gjort bekendt med de databeskyttelsesbestemmelser, der er relevante for deres arbejde. Leverandøren og enhver person, som handler på dennes vegne, og som har adgang til personoplysninger, må ikke behandle de pågældende personoplysninger, medmindre det sker efter instruks fra klienten, hvilket omfatter beføjelserne givet i nærværende kontrakt, eller medmindre det er påbudt ved lov.

c) Implementering og overholdelse af alle tekniske og organisatoriske foranstaltninger, der er nødvendige for nærværende ordre eller kontrakt, i medfør af artikel 28, stk. 3, 2. punktum, litra c og artikel 32 i GDPR [detaljer i Bilag 1].

d) Klienten og leverandøren skal, efter anmodning, samarbejde med tilsynsmyndigheden i udførelsen af dennes opgaver.

e) Klienten skal straks underrettes om alle inspektioner og foranstaltninger udført af tilsynsmyndigheden, hvis de vedrører nærværende ordre eller kontrakt. Dette gælder også, hvis leverandøren undersøges eller er part i en undersøgelse, der udføres af en kompetent myndighed i forbindelse med overtrædelser af civil- eller strafferetlige bestemmelser eller administrative regler eller forordninger vedrørende behandlingen af personoplysninger i forbindelse med behandlingen af nærværende ordre eller kontrakt.

f) Hvis klienten er genstand for en af tilsynsmyndigheden udført inspektion, en administrativ eller mindre alvorlig lovovertrædelse eller en strafferetlig procedure, et erstatningskrav fremsat af en registreret eller en tredjemand eller ethvert andet krav i forbindelse med leverandørens databehandling i medfør af ordren eller kontrakten, skal leverandøren gøre sit yderste for at støtte klienten.

g) Leverandøren skal periodisk overvåge de interne processer og de tekniske og organisatoriske foranstaltninger for at sikre, at behandlingen inden for dennes ansvarsområde er i overensstemmelse med kravene i den gældende databeskyttelseslovgivning og beskyttelsen af den registreredes rettigheder.

h) Verificerbarhed af de tekniske og organisatoriske foranstaltninger gennemført af klienten som en del af klientens tilsynsbeføjelser iht. punkt 7 i nærværende kontrakt.

6. Brug af underdatabehandlere

(1) Brug af underdatabehandlere med henblik på opfyldelsen af nærværende aftale skal forstås som tjenesteydelser, der relaterer direkte til leveringen af hovedydelsen. Dette omfatter ikke accessoriske tjenesteydelser såsom telekommunikationstjenester, post-/transporttjenester, vedligeholdelses- og brugersupporttjenester eller bortskaffelse af databærere samt andre foranstaltninger, der skal sikre fortroligheden, tilgængeligheden, integriteten og robustheden af databehandlingsudstyrets hardware og software. Leverandøren er dog forpligtet til at indgå relevante og juridisk bindende kontraktlige arrangementer og gennemføre relevante inspektionsforanstaltninger for at sikre databeskyttelsen og datasikkerheden forbundet med klientens data også i tilfælde af outsourcede accessoriske tjenesteydelser.

(2) Ordrer kan videregives til underdatabehandlere inden for rammerne af de aktiviteter, der er aftalt i ordren. Leverandøren skal omhyggeligt udvælge underdatabehandlere ud fra deres egnethed, navnlig hvad angår kravene i EU's GDPR, og skal inspicere dem regelmæssigt. Endvidere skal leverandøren indgå en aftale med underdatabehandlere om ordrebehandling i overensstemmelse med nærværende aftale. Leverandøren vil give klienten forhåndsinformation om forventede ændringer i forhold til eksisterende eller nye underdatabehandlere, hvilket giver kunden mulighed for at gøre indsigelse i mod dette. Hvis der ikke er gjort indsigelse indenfor 14 dage efter informationen er givet, opfattes dette som stiltiende accept.
(3) Overførsel af personoplysninger fra klienten til underdatabehandleren og underdatabehandlernes påbegyndelse af databehandlingen kan først igangsættes, når alle krav er opfyldt.
(4) Hvis underdatabehandleren leverer den aftalte tjenesteydelse uden for EU, skal leverandøren ved hjælp af egnede foranstaltninger sikre, at dette sker i overensstemmelse med EU's databeskyttelsesregler. Det samme gælder, hvis tjenesteydere skal benyttes inden for betydningen af stk. 1, andet punktum.
(5) Hvis underdatabehandleren outsourcer yderligere, kræver dette hovedkundens samtykke (som minimum skriftligt). Alle aftaleforhold i kontraktkæden skal også pålægges den anden underdatabehandler.

7. Klientens tilsynsbeføjelser

(1) Klienten har ret til, efter rådføring med leverandøren, at lade en person, der er underlagt professionel tavshedspligt, foretage inspektioner, eller at få inspektionerne foretaget af en revisor, som skal udpeges i hvert enkelt tilfælde. Klienten har ret til at kontrollere, at leverandøren i sin forretningsførelse overholder nærværende aftale, ved hjælp af vilkårlige kontroller, som sædvanligvis skal annonceres i god tid.
(2) Leverandøren skal sikre, at klienten kan kontrollere overholdelse af leverandørens forpligtelser i overensstemmelse med artikel 28 i GDPR**.** Leverandøren forpligter sig til at give klienten den nødvendige information på anmodning og navnlig at demonstrere gennemførelsen af de tekniske og organisatoriske foranstaltninger.
(3) Dokumentation for sådanne foranstaltninger, som ikke kun vedrører den specifikke ordre eller kontrakt, kan være overholdelse af godkendte adfærdskodekser som omhandlet i artikel 40 i GDPR, certificering i henhold til en godkendt certificeringsprocedure som omhandlet i artikel 42 i GDPR, den nuværende revisors påtegninger, rapporter eller uddrag fra rapporter leveret af uafhængige organer (f.eks. revisor, databeskyttelsesrådgiver, IT-sikkerhedsafdeling, databeskyttelsesrevisor, kvalitetsrevisor). En egnet certificering opnået på grundlag af IT-sikkerheds- eller

databeskyttelsesaudit (f.eks. iht. BSI-Grundschutz (IT-baselinebeskyttelscertificering udarbejdet af det tyske forbundskontor for IT-sikkerhed (BSI)) eller ISO/IEC 27001).
(4) Leverandøren kan kræve vederlag for muliggørelse af inspektioner foretaget af klienten.

8. Kommunikation i tilfælde af overtrædelser fra leverandørens side

(1) Leverandøren skal bistå klienten i at overholde forpligtelserne vedrørende personoplysningssikkerhed, rapporteringskrav i forbindelse med brud på datasikkerheden, konsekvensanalyser vedrørende databeskyttelse samt forudgående høringer som omhandlet i artikel 32-36 i GDPR. Dette omfatter:

a) At sikre et passende beskyttelsesniveau gennem tekniske og organisatoriske foranstaltninger, som tager højde for omstændighederne og formålene med behandlingen samt den projekterede sandsynlighed og alvor forbundet med en mulig overtrædelse af lovgivningen som følge af sikkerhedsmangler, og som muliggør øjeblikkelig detektering af relevante hændelser forbundet med overtrædelse.
b) Forpligtelse til øjeblikkeligt at rapportere brud på persondatasikkerheden til klienten
c) Pligt til at bistå klienten med at overholde klientens forpligtelse til at underrette den pågældende registrerede og øjeblikkeligt give klienten alle relevante oplysninger herom.
d) At understøtte klienten med konsekvensanalyse vedrørende databeskyttelse
e) At understøtte klienten i forbindelse med forudgående høring over for tilsynsmyndigheden

(2) Leverandøren kan kræve vederlag for supporttjenester, som ikke er omfattet i beskrivelsen af tjenesterne, og som ikke kan tilskrives fejl fra leverandørens side.

9. Klientens beføjelse til at udstede instrukser

(1) Klienten skal straks bekræfte mundtlige instrukser (som minimum skriftligt).
(2) Leverandøren skal straks informere klienten, hvis leverandøren finder, at en instruks er i strid med databeskyttelsesreglerne. Leverandøren skal derefter være berettiget til at ophæve udførelse af de relevante instrukser, indtil klienten bekræfter dette eller ændrer dem.

10. Sletning og tilbagelevering af personoplysninger

(1) Kopier eller dubletter af personoplysningerne må aldrig oprettes uden klientens vidende, med undtagelse af sikkerhedskopier, hvis disse er nødvendige for at sikre en forsvarlig databehandling, og med undtagelse af personoplysninger, der er nødvendige for at opfylde myndighedskrav om opbevaring af personoplysninger.

(2) Efter udførelsen af det aftalte arbejde, eller på et tidligere tidspunkt, hvis klienten anmoder om det, og senest ved serviceaftalens ophør, skal leverandøren give klienten eller – i henhold til forudgående samtykke – tilintetgøre alle dokumenter, behandlings- og anvendelsesresultater samt datasæt relateret til kontrakten, der er kommet i leverandørens besiddelse, på en måde, der er i overensstemmelse med databeskyttelsesreglerne. Det samme gælder alt dermed forbundet materiale, herunder testmateriale, affald, overflødigt og kasseret materiale. Logfilen, der dokumenterer tilintetgørelse eller sletning, skal fremlægges på anmodning.
(3) Dokumentation, der bruges til at påvise forsvarlig databehandling i overensstemmelse med ordren eller kontrakten, skal opbevares af leverandøren efter kontraktens udløb i overensstemmelse med de

respektive perioder, hvori leverandøren har pligt til at opbevare dataene. Leverandøren kan overdrage en sådan dokumentation til klienten ved kontraktperiodens udløb for at fritage leverandøren for dennes kontraktlige forpligtelse.

Klient: _____

_____
(sted/dato)

_____
(underskrift/stempel)

_____
(navn/underskriverens funktion)

Leverandør: _____

_____
(sted/dato)

_____
(underskrift/stempel)

_____
(navn/underskriverens funktion)

Bilag - Tekniske og organisatoriske foranstaltninger

Virksomhed: ALSO A/S
Sted: Danmark

1. Fortrolighed (artikel 32, stk. 1, litra b i EU's GDPR)
Fysisk adgangskontrol
Ingen uautoriseret fysisk adgang til databehandlingssystemer.

Formål: Denne foranstaltning skal sikre, at ingen uautoriserede personer har fysisk adgang til de databehandlingssystemer, der behandler personoplysninger.

Vedtagne foranstaltninger:

Tilgængelig	Foranstaltning
x	Adgangskontrolsystem (id-kortlæser, nøglelåsningssystem)
x	Foranstaltninger vedrørende genstandes sikkerhed
x	Hegn
x	Sikkerhedsdøre, sikkerhedsvinduer
x	Gitre til vinduer og døre
x	Fabrikssikkerhedsservice, portvagt
x	Kontrol af personer, reception
x	Dokumentation for besøgende
x	Videoovervågning
x	Fotoelektriske stråler, bevægelsessensorer
x	Dørsikkerhed (dørlåsningssystem, kodelås, biometrisk adgangskontrol, sikkerhedslåse)
x	Fysisk nøgleadministration/dokumentation for fordeling af fysiske nøgler
x	Korrekt sikring uden for kontortiden via fabrikssikkerhedsservice og/eller alarmsystem
x	Retningslinje for gæster/besøgende/eksterne personer
x	Id-kort til besøgende
x	Særlige sikkerhedsforanstaltninger for serverrum
x	Medarbejdere har id-kort og autorisationskort (og har pligt til at have dem på sig)
x	Særlige områder, der er underlagt begrænsning
x	Omhyggelig udvælgelse af rengøringspersonale

Adgangskontrol
Ingen uautoriseret adgang til databehandlingssystemer.

Formål: Denne foranstaltning skal sikre, at kun autoriserede personer har adgang til databehandlingssystemer, og at de kun kan bruges af dem.

Vedtagne foranstaltninger:

Tilgængelig	Foranstaltning
x	Personligt og individuelt brugerlogin, når man logger på databehandlingssystemer og virksomhedsnetværk
x	Adgangskodepolitik
x	Multifaktorautentifikation
x	Ekstra systemlogin til visse programmer
x	Tildeling af bestemte klienter udelukkende til definerede roller
x	Automatisk låsning af klienter på grund af inaktivitet uden brugerinteraktion (adgangskodebeskyttet pauseskærm eller automatisk pauseregistrering)
x	Elektronisk dokumentation af adgangskoder (ingen brugeradgangskoder) og kryptering af denne dokumentation for at forhindre uautoriseret adgang
x	Låsning af sager
x	Brug af systemer til registrering af indtrængende
x	Brug af antivirussoftware/antimalwaresoftware
x	Brug af firewalls
x	Netværksadgangskontrol (NAC)
x	Tildeling af brugerprofiler til IT-systemer
x	Brug af VPN-teknologi
x	Brug af krypteringsmekanismer til filer
x	Ingen enheder uden adgangskode eller låsningskode, hvis de giver adgang til virksomhedsdata
x	Brugere er forpligtet til databeskyttelse Artikel 28, stk. 3, litra b i EU's GDPR
x	Retningslinje for privat brug af virksomhedsudstyr
x	Retningslinje for BYOD (Bring Your Own Device)
x	Retningslinje for mobile medarbejdere (f.eks. i forbindelse med bærbare computere)

Fysisk adgangskontrol
Ingen uautoriseret læsning, kopiering, modificering eller sletning af personoplysninger i et databehandlingssystem.
F.eks. Autorisationskoncept, behovsbaserede adgangsrettigheder, logning af adgang.

Formål: Denne foranstaltning skal sikre, at kun autoriserede brugere har adgang til databehandlingssystemet, og at adgangen til personoplysninger er begrænset til den pågældende brugers adgangsrettigheder. Personoplysninger må ikke behandles og bruges, og efter opbevaring må oplysningerne ikke uautoriseret læses, kopieres, modificeres eller slettes.

Vedtagne foranstaltninger:

Tilgængelig	**Foranstaltning**
x	Administration af rettigheder og roller
x	Differentierede adgangsrettigheder
x	Profiler
x	Roller
x	Dokumentation af adgangsrettigheder
x	Godkendelsesprocedure for autorisationstildeling
x	Debriefing/logføring
x	Inspektion/revision
x	Kryptering af CD'er/DVD-ROM'er, eksterne drev eller bærbare computere (f.eks. via operativsystem, Safeguard, PGP, Veracrypt osv.)
x	Fire øjne-princip
x	Adskillelse af funktioner
x	Opgaverelaterede adgangsrettighedsprofiler
x	Reducering af personer med administratorrettigheder til et minimum
x	Sletning af datamedier før genanvendelse
x	Brug af serviceleverandør til tilintetgørelse af dokumenter
x	Sikker opbevaring af datamedier
x	Korrekt tilintetgørelse af datamedier
x	Logning af tilintetgørelse
x	Regelmæssig revision af adgangsrettigheder
x	Registrering og analyse af logfiler (succesfulde og ikke-succesfulde forsøg på login)
x	Retningslinje for pseudonymisering af personoplysninger
x	Retningslinje for regulering af fravær (en fraværende medarbejders adgang til data)

Adskillelseskontrol:
Adskilt behandling af personoplysninger, der indsamles til forskellige formål (f.eks. Sandboxing, Multi Client-funktion)

Formål: Formålsrelateret behandling af personoplysninger skal implementeres på et teknisk niveau. Personoplysninger, der indsamles til forskellige formål, skal behandles adskilt.

Vedtagne foranstaltninger:

Tilgængelig	**Foranstaltning**
x	Adskilte systemer
x	Adskilte databaser
x	Adgangskontrolrettigheder
x	Adskillelse gennem adgangskontrolrettigheder

Andet:
Pseudonymisering: (artikel 32, stk. 1, litra a i EU's GDPR, artikel 25 stk. 1 i EU's GDPR)
Behandling af personoplysninger udføres på en måde, som betyder, at disse personoplysninger ikke uden supplerende oplysninger kan henføres til en fysisk person, hvis de supplerende oplysninger lagres separat og er underlagt tekniske og organisatoriske foranstaltninger.

2. Integritet (artikel 32, stk. 1, litra b i EU's GDPR)
Overførselskontrol

Ingen uautoriseret læsning, kopiering, modificering eller sletning under transport eller elektronisk overførsel (kryptering, VPN, underskrift osv.).

Formål: Denne foranstaltning har til formål at sikre, at datamedier ikke kan læses, kopieres, modificeres eller slettes under transport. Disse foranstaltninger skal kontrollere og finde ud af, hvor personoplysninger overføres eller bliver forberedt til overførsel. Transport- og datamediekontrol er kombineret i overførselskontrol.

Vedtagne foranstaltninger:

Tilgængelig	**Foranstaltning**
x	Kryptering af CD'er/DVD-ROM'er, eksterne drev eller bærbare computere (f.eks. via operativsystem, Safeguard, PGP, Veracrypt osv.)
x	Krypterede forbindelser (VPN)
x	Logning (logning af revision)
	Transportlåsning af datamedier og transportbeholdere
x	Sikret WLAN
x	SSL-kryptering til webadgang
x	Retningslinje for tilintetgørelse af personoplysninger
x	Korrekt tilintetgørelse af datamedier
x	Omhyggelig udvælgelse af transportpersonale ved manuel transport
x	Overførsel på en pseudoanonymiseret eller anonymiseret måde
x	Register over regelmæssige dataoverførsler
x	Ingen software, der overfører personoplysninger til fremmed server uden kontraktbestemmelser (Facebook, Whatsapp,…)
x	Procedurer for detektering af og beskyttelse mod ondsindet software
x	Sikret indgang til datacenter
x	Styring af datamedier
x	Separat lager til fortrolige datamedier
x	Tilintetgørelse af datamedier (f.eks. forkerte udskrifter, disks)
x	Sletning af datamedier før udskiftning
x	Sikker udskrivning

Inputkontrol:
Mulighed for at fastslå, om og af hvem personoplysninger er blevet indtastet, ændret eller fjernet i databehandlingssystemer, f.eks. logning, dokumentstyring

Formål: Disse foranstaltninger er udarbejdet for at sikre behandlingsprocessens verificerbarhed (indtastning, modificering, fjernelse) af personoplysninger. Det betyder, at forfatteren, indholdet og tidspunktet for datalagringen skal kunne fastslås.

Vedtagne foranstaltninger:

Tilgængelig	**Foranstaltning**
x	Adgangsrettigheder/autorisationskoncept
x	Systemmæssig logføring
x	Logføringssoftwarens sikkerhed
x	Funktionelt ansvar
x	Forpligtelse til databeskyttelse

3. Tilgængelighed og robusthed (artikel 32, stk. 1, litra b i EU's GDPR)
Tilgængelighedskontrol:
Beskyttelse mod hændelig eller forsætlig tilintetgørelse eller hændeligt eller forsætligt tab, f.eks.: koncept for sikkerhedskopiering (online/offline, i virksomheden/uden for virksomheden), nødstrømsforsyning, virusbeskyttelse, firewall, rapporteringskanaler, nødplaner.

Formål: Det skal sikres, at personoplysninger ikke tilintetgøres ved et uheld, og at de beskyttes mod tab. Det skal sikres, at de anvendte systemer kan gendannes i tilfælde af fejlfunktion.

Vedtagne foranstaltninger:

Tilgængelig	**Foranstaltning**
x	Strategi for sikkerhedskopiering
x	Lagringskoncept for sikkerhedskopier
x	Serverrum må ikke være placeret under vandbærende systemer/faciliteter
x	Nødstrømsforsyning (batteri, diesel)
x	Overvågning af temperatur og luftfugtighed i serverrum
x	Beskyttelse mod virus/trusler, firewall
x	Aircondition i IT-rum
x	Brandsikring (brandalarmsystemer, brandslukningsudstyr)
x	Alarmsystemer
x	Egnede arkivrum
x	Nødplan
x	Nødberedskabsøvelser
x	Planer vedrørende svigt og gendannelse
x	Redundant datacenter (internt/eksternt)
x	Redundant dataforbindelse fra datacenter til virksomhedens netværk
x	Redundant hardware
x	Dataspejling

4. Procedure for regelmæssig gennemgang, benchmarking og evaluering (artikel 32, stk. 1, litra d i EU's GDPR; artikel 25, stk. 1 i EU's GDPR)

Ordrekontrol:
Ingen databehandling i betydningen af artikel 28 i EU's GDPR uden tilsvarende instruktioner fra den ordregivende myndighed, f.eks. tydelig kontraktudformning, formaliseret ordrestyring, streng udvælgelse af serviceleverandøren, forpligtelse til at overbevise på forhånd, opfølgende kontroller.

Formål: Ordremodtageren skal sikre, at de data, der skal behandles i ordren, udelukkende behandles i overensstemmelse med klientens instrukser. Indirekte forbundet hermed er kundens forpligtelse til at give ordremodtagerne instrukser.

Vedtagne foranstaltninger:

Tilgængelig	**Foranstaltning**
x	Skriftlig kontrakt vedrørende ordredatabehandling i henhold til EU's GDPR med bestemmelser om ordremodtagerens og ordregiverens rettigheder og forpligtelser.
x	Uddannelse af alle autoriserede medarbejdere
x	Regelmæssige opfølgende uddannelseskurser
x	Medarbejdere er underlagt tavshedspligt og datafortrolighed
x	Regelmæssige revisioner af databeskyttelse udført af virksomhedens databeskyttelsesrådgiver
x	Omhyggelig udvælgelse af ordremodtageren