Avtale for databehandling

mellom

……..

– behandlingsansvarlig - heretter kalt kunden -

og

ALSO AS

Tassebekkveien 354

3160 Stokke

– Databehandler - heretter kalt leverandøren

1. Kontraktsinnhold og varighet av bestillingen eller kontrakten

(1) Emne

For ordren eller kontrakten innebærer behandling av data gjennomføring av følgende tjenester eller oppgaver av leverandøren: Teknisk support, ordrebehandling, IT-tjenester, kundeservice, skytjenester.

(2) Varighet

Varigheten til denne kontrakten tilsvarer avtalens betingelser innenfor rammen av de respektive produkt-, tjeneste-, kjøps- og/eller arbeidsavtalene.

2. Spesifisering av ordren eller kontraktdetaljer

(1) Arten av og hensikten med den tilsiktede behandlingen av data

Detaljert beskrivelse av kontrakstgjenstanden med hensyn til arten av og hensikten med tjenestene som tilbys av leverandøren:

Dataens art	Hensikten med behandlingen	Den registrerte
Personopplysninger: Navn, adresse, kontaktopplysninger, bankkontoopplysninger	Ordrebehandling, teknisk support, IT-tjenester, kundeservice, skytjenester	Ansatte hos behandlingsansvarlig, samarbeidspartner, kunde, leverandør, interessenter

Gjennomføring av kontraktsmessig avtalt behandling av opplysninger skal utføres utelukkende innenfor en EU-medlemsstat, i en medlemsstat i Det europeiske økonomiske samarbeidsområde (EØS) eller i et land som er omfattet av EU-kommisjonens tilstrekkelighetsbeslutning. Enhver overføring av opplysninger til en stat som ikke er et medlem av enten EU eller EØS krever kundens forhåndsgodkjennelse og skal kun skje dersom de spesifikke vilkårene i artikkel 44 flg. GDPR oppfylles. Tilstrekkelige beskyttelsesnivå i et land som ikke er medlem av EU, bør garanteres i henhold til EUs standard kontraktsbestemmelser. (Art 46 Abs 2 lit c og d EU-GDPR)

(2) Type opplysninger

Behandlingen av personopplysninger omfatter følgende opplysningstyper / kategorier: Personlige hovedopplysninger (nøkkelopplysninger), kontaktopplysninger, hovedkontraktsopplysninger (kontraktsmessige/juridiske forhold, kontraktsmessige eller produktinteresser), kundehistorikk, kontraktsfaktura- og betalingsopplysninger, offentliggjort informasjon (fra tredjeparter, f.eks. kredittopplysningsbyråer eller offentlige registre), informasjon om systemkonfigurasjon og kundemiljø.

(3) Kategorier for den registrerte

Kategoriene for den registrerte omfatter: Ansatte hos behandlingsansvarlig, samarbeidspartnere, kunder, potensielle kunder, abonnenter, ansatte, leverandører, kontaktpersoner.

3. Tekniske og organisatoriske tiltak

(1) Før behandlingen av opplysninger påbegynnes skal leverandøren kunne dokumentere utførelsen av nødvendige tekniske og organisatoriske tiltak som er fastsatt før tildeling av ordren eller kontrakten (spesielt med hensyn til den detaljerte gjennomføringen av kontrakten), og skal fremlegge disse dokumenterte tiltakene til kunden for gjennomgang. De dokumenterte tiltakene vil gjelde som grunnlag for kontrakten ved aksept fra kunden. Dersom kundens gjennomgang/revisjon av tiltakene viser behov for endringer, skal slike endringer implementeres ved gjensidig enighet.

(2) Leverandøren skal etablere sikkerhetstiltak i samsvar med artikkel 28 avsnitt 3 punkt c og artikkel 32 GDPR, særlig i forbindelse med artikkel 5 avsnitt 1 og avsnitt 2 i GDPR. Tiltakene som skal innføres, er tiltak for datasikkerhet og tiltak som sikrer et sikkerhetsnivå som er passende for risiko knyttet til systemenes konfidensialitet, integritet, tilgjengelighet og robusthet. Det må tas hensyn til dagens tekniske status, implementeringskostnader, arten, omfanget og formålene med databehandlingen, samt sannsynligheten for forekomster og alvorlighetsgraden av risikoen for fysiske personers rettigheter og friheter i henhold til artikkel 32 avsnitt 1 i GDPR. [Detaljer i vedlegg 1]

(3) De tekniske og organisatoriske tiltakene er underlagt teknisk utvikling og videreutvikling. I denne forbindelse er det tillatt for leverandøren å gjennomføre alternative tilstrekkelige tiltak. Sikkerhetsnivået for de definerte tiltakene må imidlertid ikke reduseres. Vesentlige endringer må dokumenteres.

4. Korrigering, begrensning og sletting av data

(1) Leverandøren kan ikke på egen hånd korrigere, slette eller begrense behandlingen av data som behandles på vegne av kunden. Dette kan bare skje basert på dokumenterte instruksjoner fra kunden. Dersom den registrerte kontakter leverandøren direkte med hensyn til en korrigering, sletting eller begrensning av behandling, vil leverandøren umiddelbart videresende vedkommendes forespørsel til kunden.

(2) Forutsatt at det inngår i tjenestens omfang, skal leverandørens retningslinjer for sletting, «retten til å glemmes», korrigering, datamobilitet og tilgang sikres av leverandøren i samsvar med dokumenterte instruksjoner fra kunden uten forsinkelse.

5. Kvalitetssikring og andre plikter hos leverandøren

I tillegg til å overholde regler som er angitt i denne ordren eller kontrakten, skal leverandøren også overholde de lovbestemte kravene som er omtalt i artiklene 28 til 33 i GDPR. Leverandøren skal derfor særlig sørge for overholdelse av følgende krav:

a) Utnevne et personvernombud, som utfører sine oppgaver i samsvar med artikkel 38 og 39 i GDPR.

   Hans/hennes nåværende kontaktinformasjon er alltid tilgjengelig og kan enkelt finnes på leverandørens nettsted. Personvernombudet hos ALSO AS kan til enhver tid kontaktes på DPO.NO@ALSO.COM

b) Konfidensialitet i henhold til artikkel 28 i avsnitt 3, 2. setning, punkt b, samt artikkel 29 og 32 avsnitt 4 i GDPR. Leverandøren overlater bare databehandlingen som er skissert i denne kontrakten til ansatte som er underlagt taushetsplikt og som er kjent med personvernbestemmelsene som er relevante for utførelsen av arbeidet. Leverandøren og enhver person som har tilgang til personopplysninger og handler under leverandørens myndighet, skal ikke behandle disse dataene uten instruksjoner fra kunden (beskrevet i denne kontrakten), med mindre det kreves ved lov.

c) Implementering og overholdelse av alle tekniske og organisatoriske tiltak som er nødvendige for denne ordren eller kontrakten i henhold til artikkel 28 i avsnitt 3, 2. setning, punkt c, samt artikkel 32 i GDPR [detaljer i vedlegg 1].

d) Kunden og leverandøren skal ved forespørsel samarbeide med tilsynsmyndighetene ved utførelsen av sine oppgaver.

e) Kunden skal umiddelbart informeres om eventuelle tilsyn og tiltak som utføres av tilsynsmyndighetene, i den grad de gjelder denne ordren eller kontrakten. Dette gjelder også dersom leverandøren er under etterforskning, eller er en part i en etterforskning fra en kompetent myndighet, i forbindelse med overtredelse av sivil- eller straffelov eller administrativ regel eller forskrift om behandling av personopplysninger i forbindelse med behandling av denne ordren eller kontrakten.

f) Leverandøren skal gjøre sitt ytterste for å støtte kunden dersom kunden er under etterforskning av tilsynsmyndighetene for en administrativ eller straffbar handling eller straffesak, et erstatningskrav fra en registrert eller en tredjepart, eller det foreligger et annet krav i forbindelse med ordre- eller kontraktsbehandlingen til leverandøren.

g) Leverandøren skal regelmessig overvåke de interne prosessene og de tekniske og organisatoriske tiltakene for å sikre at behandling innenfor leverandørens ansvarsområde er i samsvar med kravene i gjeldende personvernlov og beskyttelse av rettighetene til den registrerte.

h) Etterprøving av tekniske og organisatoriske tiltak blir utført av kunden som en del av kundens tilsynsmyndighet, som nevnt i punkt 7 i denne kontrakten.

6. Underleverandører

(1) I henhold til denne avtalen skal underleverandører forstås som tjenester som direkte vedrører levering av hovedtjenesten. Dette inkluderer ikke tilleggstjenester, som telekommunikasjonstjenester, post-/transporttjenester, vedlikeholds- og brukerstøttetjenester eller deponering av databærere, samt andre tiltak for å sikre konfidensialitet, tilgjengelighet, integritet og motstandsdyktighet av maskinvare og programvare som blir brukt til databehandlingen. Leverandøren er imidlertid forpliktet til å inngå hensiktsmessige og juridisk bindende avtaler i form av kontrakter og å iverksette passende kontrolltiltak for å sikre personvern og datasikkerhet overfor kundens data, også i tilfelle av outsourcede tilleggstjenester.

(2) Ordrer kan videresendes til underleverandører innenfor de rammene av aktiviteter som er avtalt i ordren. Underleverandørene vil bli varslet på kundens forespørsel. Leverandøren må velge underleverandører med omhu ut fra deres egnethet, særlig med hensyn til kravene i EU-GDPR, og skal foreta regelmessige inspeksjoner av disse. Videre skal leverandørens avtaler om ordrebehandling med underleverandører være i henhold til denne avtalen. Leverandøren vil informere kunden i forveien om tiltenkt endring med hensyn til involvering eller erstatning av underleverandører, noe som gir kunden muligheten til å protestere mot denne endringen. Dersom ingen innsigelse oppstår innen 14 dager etter melding, skal samtykke til endringen anses som gitt.

(3) Overføringen av personopplysninger fra kunden til underleverandøren, og underleverandørens påbegynnelse av databehandlingen, skal bare foretas etter at alle krav er oppfylt.

(4) Hvis underleverandøren leverer tjenesten utenfor EU, må leverandøren sørge for overholdelse av EUs personvernforskrifter ved hjelp av passende tiltak. Det samme gjelder dersom det skal benyttes tjenesteleverandører, i henhold til avsnitt 1, 2. setning.
(5) Ytterligere outsourcing av underleverandøren krever samtykke fra hovedkunden (minst i tekstformat). Alle kontraktsforskrifter i alle kontrakter må også pålegges den andre underleverandøren.

7. Tilsynsmyndigheten til kunden

(1) Kunden har etter samråd med leverandøren, rett til å utføre inspeksjoner av en person som er pålagt profesjonelt hemmelighold eller å få inspeksjon utført av en revisor som blir utpekt i hvert enkelt tilfelle. Kunden har rett til å få bli overbevist om at leverandøren overholder denne avtalen i sin forretningsvirksomhet ved hjelp av tilfeldige kontroller, som normalt må bli kunngjort i god tid.
(2) Leverandøren skal sikre at kunden er i stand til å bekrefte etterlevelse av leverandøren forpliktelser i samsvar med artikkel 28 i GDPR**.** Leverandøren forplikter seg til å gi kunden nødvendig informasjon på forespørsel og særlig å demonstrere gjennomføringen av de tekniske og organisatoriske tiltakene.
(3) Bevis på slike tiltak, som ikke bare gjelder den spesifikke ordren eller kontrakten, kan gis ved overholdelse av etiske retningslinjer l i henhold til artikkel 40 GDPR; Sertifisering i henhold til en godkjent sertifiseringsprosedyre i samsvar med artikkel 42 GDPR, attester fra nåværende revisor, rapporter eller utdrag fra rapporter fra uavhengige organer (for eksempel revisor, personvernombud, avdeling for IT-sikkerhet, dataregistreringsrevisor, kvalitetsrevisor). En egnet sertifisering av IT-sikkerhet eller datasikkerhetsrevisjon (for eksempel i henhold til BSI-Grundschutz (IT Baseline Protection-sertifisering utviklet av German Federal Office for Security in Information Technology (BSI)) eller ISO/IEC 27001).

(4) Leverandøren kan kreve godtgjørelse for å muliggjøre inspeksjoner fra kunden.

8. Kommunikasjon ved overtredelser fra leverandøren

(1) Leverandøren skal bistå kunden med å oppfylle forpliktelsene vedrørende sikkerheten til personopplysninger, rapporteringskrav for datainnbrudd, konsekvensutredninger for personvern og tidligere konsultasjoner, omtalt i artiklene 32-36 i GDPR. Disse inkluderer:

a) Sikre et passende nivå av beskyttelse gjennom tekniske og organisatoriske tiltak som tar hensyn til omstendighetene og formålene med behandlingen, samt den anslåtte sannsynligheten for og alvorlighetsgraden av en eventuell overtredelse loven som følger av sikkerhetsproblemer og som muliggjør umiddelbar påvisning av relevante overtredelseshendelser.
b) Forpliktelsen til å øyeblikkelig rapportere et datainnbrudd til kunden
c) Plikten til å bistå kunden med hensyn til kundens forpliktelser til å informere den registrerte og å umiddelbart gi kunden all relevant informasjon i denne forbindelsen.
d) Støtte kunden med sin konsekvensutredning av datasikkerhet
e) Støtte kunden med hensyn til forutgående konsultasjoner fra tilsynsmyndighetene

(2) Leverandøren kan kreve kompensasjon for støttetjenester som ikke er inkludert i tjenestebeskrivelsen og som ikke skyldes feil fra leverandørens side.

9. Kundens myndighet til å gi instruksjoner

(1) Kunden skal umiddelbart bekrefte muntlige instruksjoner (i det minste i tekstform).
(2) Leverandøren skal umiddelbart informere kunden dersom en instruksjon anses som brudd på personvernforskrifter. Leverandøren har da rett til å innstille gjennomføringen av instruksjonene frem til kunden bekrefter eller endrer dem.

10. Sletting og retur av personopplysninger

(1) Kopier eller duplikater av dataene skal aldri opprettes uten kundens viten, med unntak av sikkerhetskopier i den grad de er nødvendige for å sikre at databehandling foregår på en ordentlig måte, samt data som kreves for å oppfylle myndighetskrav om datalagring.

(2) Etter ferdigstillelse av det avtalte arbeidet, eller tidligere ved forespørsel fra kunden men senest ved oppsigelse av tjenestesavtalen, skal leverandøren overføre data til kunden eller (med forbehold om tidligere samtykke) på en forsvarlig måte ødelegge alle dokumenter, bearbeidings- og bruksresultater, og datasett som leverandøren er i bestittelse av og som er knyttet til kontrakten. Det samme gjelder for alle tilhørende tester, avfall, overflødig og kassert materiale. Logg for ødeleggelse eller sletting skal gis ved forespørsel.
(3) Dokumentasjon som brukes til å demonstrere ryddig databehandling i samsvar med ordren eller kontrakten, skal lagres av leverandøren etter kontraktens utløp i henhold til respektive oppbevaringsperioder. Slik dokumentasjon kan overleveres til kunden ved kontraktsperiodens utløp for å løse leverandøren fra denne kontraktsforpliktelsen.

Vedlegg - Tekniske og organisatoriske tiltak

Bedrift: ALSO AS
Sted: Norge

1.Konfidensialitet (Art. 32 avsnitt 1, punkt B i EU-GDPR)
Kontroll av fysisk tilgang
Ingen uautorisert fysisk tilgang til databehandlingssystemer.

Formål: Dette tiltaket skal sikre at ingen uautoriserte personer har fysisk tilgang til databehandlingssystemer som behandler personopplysninger.

Vedtatte tiltak:

Tilgjengelig	Tiltak
x	Adgangskontrollsystem (ID-kortleser, låsesystem med nøkkel)
x	Tiltak for objektsikkerhet
x	Barrierer
x	Sikkerhetsdører, sikkerhetsvinduer
x	Dørsikkerhet (nøkkellåsing, kodelås, biometrisk tilgangskontroll, sikkerhetslåser)
x	Fysisk nøkkelhåndtering / Dokumentasjon av fysisk nøkkelutdeling
x	Sikring på grunn av kontortid ved fabrikkens sikkerhetstjeneste og / eller alarmsystem.
x	Spesielle sikkerhetstiltak for serverrom

Kontroll av tilgang:
Ingen uautorisert fysisk tilgang til databehandlingssystemer.

Formål: Dette tiltaket skal sikre at kun autoriserte personer har tilgang til databehandlingssystemer og at systemene kun kan benyttes av disse.

Vedtatte tiltak:

Tilgjengelig	Tiltak
x	Personlig og individuell bruker ved innlogging i databehandlingssystemer og bedriftsnettverk
x	Retningslinjer for passord
x	Multifaktorautorisering
x	Ekstra systeminnlogginger for enkelte applikasjoner
x	Tildeling av bestemte klienter utelukkende til definerte roller.
x	Automatisk låsing av klienter på grunn av inaktivitet uten brukerinteraksjon. (Passordbeskyttet skjermsparer eller automatisk registrering av pauser)
x	Elektronisk dokumentasjon av passord (ingen brukerpassord) og kryptering av denne dokumentasjonen for å forhindre uautorisert tilgang.
x	Bruk av systemer som oppdager innbrudd
x	Bruk av antivirus- og antimalwareprogramvare
x	Bruk av brannmurer
x	Tilgangskontroll for nettverk (NAC)
x	Tildeling av brukerprofiler til IT-systemer
x	Bruk av VPN-teknologi
x	Bruk av krypteringsmekanismer for filer
x	Ingen enheter uten passord eller låsekode har tilgang til bedriftsdata.
x	Brukernes forpliktelser til personvern. Art. 28 avsnitt 3, punkt b i EU-DSGVO
x	Retningslinjer for privat bruk av firmaets utstyr.
x	Retningslinjer for BYOD (ta med eget utstyr)
x	Retningslinjer for mobilt arbeid (f.eks. bærbar datamaskin)

Kontroll av datatilgang
Ingen uautorisert lesing, kopiering, endring eller sletting av personopplysninger i et databehandlingssystem.
F.eks. Autorisasjonskonsept, behovsbaserte tilgangsrettigheter, tilgangslogging.

Formål: Disse tiltakene skal sikre at kun autoriserte brukere har tilgang til databehandlingssystemet, og tilgangen til personopplysninger er begrenset til tilgangsrettighetene til denne brukeren. Personopplysninger kan ikke behandles eller brukes, og etter lagring av opplysninger kan ikke uautoriserte personer lese, kopiere, endre eller slette opplysninger.

Vedtatte tiltak:

Tilgjengelig	**Tiltak**
x	Administrasjon av rettigheter og roller
x	Differensierte tilgangsrettigheter
x	Profiler
x	Roller
x	Dokumentasjon av tilgangsrettigheter
x	Godkjenningsprosedyre for autorisasjonstildeling
x	Debriefing / Logging
x	Tilsyn / revisjon
x	Kryptering av CD/DVD-ROM, eksterne stasjoner eller bærbare datamaskiner (f.eks. av operativsystem, sikkerhetsbeskyttelse, PGP, Veracrypt, etc.)
x	Fire øyne-prinsippet
x	Ansvarsfordeling
x	Oppgaverelaterte profiler med tilgangsrettigheter
x	Redusere antall personer med administrasjonsrettigheter til et minimum
x	Sletting av datamedier for gjenbruk
x	Bruk av tjenesteleverandør for ødeleggelse av dokumenter
x	Sikkerhetstiltak for datamedier
x	Korrekt ødeleggelse av datamedier
x	Loggføring av ødeleggelse
x	Jevnlig revisjon av tilgangsrettigheter
x	Registrering og analyse av loggfiler (vellykkede og mislykkede innloggingsforsøk)
x	Retningslinjer for pseudonymisering av personopplysninger
x	Fraværsregulering/-retningslinjer. (Tilgang til data for fraværende ansatt)

Separasjonskontroll:
Separat behandling av data som samles inn til ulike formål. (f.eks. prosessisolering, behandling av flere kunder samtidig)

Formål: Formålsrelatert behandling av personopplysninger bør gjennomføres på et teknisk nivå. Data som samles inn til ulike formål, bør behandles atskilt.

Vedtatte tiltak:

Tilgjengelig	**Tiltak**
x	Separerte systemer
x	Separerte databaser
x	Tilgangsrettigheter
x	Separasjon gjennom tilgangsrettigheter

Andre:
Pseudonymisering: (Artikkel 32, avsnitt 1, punkt a i EU-GDPR, artikkel 25, avsnitt 1 i EU-GDPR)
Behandling av personopplysninger gjøres på en måte hvor disse dataene ikke henviser til en bestemt person uten ytterligere opplysninger - i den grad de ytterligere opplysningene lagres separat og er knyttet til tekniske og organisatoriske tiltak.

2. Integritet (Art. 32, avsnitt 1, punkt b i EU-GDPR)
Kontroll ved overføring

Ingen uautorisert lesing, kopiering, endring eller sletting under transport eller elektronisk overføring. (Kryptering, VPN, signatur, etc.)

Formål: Disse tiltakene sikrer at datamedier ikke kan leses, kopieres, endres eller slettes under transport. Tiltakene sjekker og finner ut hvor personopplysninger overføres eller forberedes til overføring. Transport- og datamediekontroll kombineres i overføringskontroll.

Vedtatte tiltak:

Tilgjengelighet	**Tiltak**
x	Kryptering av CD/DVD-ROM, eksterne stasjoner eller bærbare datamaskiner (f.eks. av operativsystem, sikkerhetsbeskyttelse, PGP, Veracrypt, etc.)
x	Krypterte tilkoblinger (VPN)
x	Loggføring (revisjonslogg)
	Låsing av datamedier og transportbeholdere under transport
x	Sikret WLAN
x	SSL-kryptering for webtilgang
x	Retningslinjer for ødeleggelse av data
x	Korrekt ødeleggelse av datamedier
x	Møysommelig utvelgelse av transportpersonale dersom manuell transport
x	Overføring på en pseudonymisert eller anonymisert måte
x	Registrering av vanlige dataoverføringer
x	Ingen programvare som overfører personopplysninger uten kontraktsbestemmelser til en utenlandsk server. (Facebook, Whatsapp,…)
x	Prosedyrer for å oppdage og beskytte mot ondsinnet programvare
x	Sikret inngang i datasenter
x	Håndtering av datamedier
x	Separat lagring for konfidensielle datamedier
x	Ødeleggelse av datamedier (f.eks. feilprinting, disker,...)
x	Sletting av datamedier før utveksling
x	Sikker utskrift

Kontroll av inngang:
Fastsette om og av hvem personopplysninger har blitt oppført, endret eller fjenet i databehandlingssystemer, f.eks. innlogging, dokumenthåndtering

Formål: Disse tiltakene er utformet for å sikre etterprøvbarheten til en behandlingsoperasjon (oppføring, modifisering, fjerning) av personopplysninger. Dette betyr at forfatteren, innholdet og tidspunktet for datalagringen bør fastslås.

Vedtatte tiltak:

Tilgjengelig	**Tiltak**
x	Tilgangsrettigheter / Autorisasjonskonsept
x	Systemlogging
x	Sikkerhets- eller loggprogramvare
x	Funksjonelt ansvar
x	Forpliktelse overfor personvern

3. Tilgjengelighet og motstandsdyktighet (Art. 32, avsnitt 1, punkt b i EU-GDPR)
Tilgjengelighetskontroll:
Beskyttelse mot utilsiktet eller bevisst ødeleggelse eller tap, f.eks.:
Sikkerhetskopieringskonsept (online/offline, onsite/offsite), uavbrutt strømforsyning, virusbeskyttelse, brannmur, rapporteringskanaler, beredskapsplaner.

Formål: Det må sikres at personopplysningene ikke ødelegges utilsiktet og at de beskyttes mot tap. Det må sikres at systemene som brukes kan gjenopprettes i tilfelle funksjonssvikt.

Vedtatte tiltak:

Tilgjengelig	**Tiltak**
x	Strategi for sikkerhetskopiering
x	Lagringskonsept for sikkerhetskopier
x	Serverrom ikke under vannførende systemer/anlegg
x	Uavbrutt strømforsyning (batteri, diesel)
x	Overvåkning av temperatur og luftfuktighet i serverrom
x	Beskyttelse mot virus/trusler, brannmur
x	Klimaanlegg i IT-rom
x	Brann- og slukningssikkerhet (brannalarmsystemer, brannslukkingsutstyr)
x	Alarmsystemer
x	Egnede arkiveringsrom
x	Nødplan
x	Beredskapsøvelse
x	Feil- og gjenopprettingsplaner
x	Redundant datasenter (internt/eksternt)
x	Redundant datatilkobling av datasenter til bedriftsnettverket
x	Redundant maskinvare
x	Dataspeiling

4. Prosedyre for regelmessig gjennomgang, referanse og evaluering (Art. 32, avsnitt 1, punkt d i EU-GDPR, art. 25, avsnitt 1 i EU-GDPR)

Ordrekontroll:
Ingen behandling av data i henhold til art. 28 EU-GDPR uten tilsvarende instruksjoner fra oppdragsgiver, f.eks. tydelig kontraktsutforming, formalisert ordrebehandling, strengt utvalg av tjenesteleverandøren, forpliktelse til å overbevise på forhånd, oppfølgingskontroller.

Formål: Leverandøren må sørge for at dataene som skal behandles i ordren kun behandles i samsvar med kundens instruksjoner. Kundens plikt å gi instruksjoner til leverandøren er indirekte knyttet til dette.

Vedtatte tiltak:

Tilgjengelig	**Tiltak**
x	Skriftlig kontrakt for ordre av databehandling i henhold til EU-GDPR med forskrifter om leverandørens og kundens rettigheter og forpliktelser
x	Opplæring av alle autoriserte ansatte
x	Jevnlig oppfølging med opplæringskurs
x	Ansatte er forpliktet til å opprettholde konfidensialitet og holde data hemmelig
x	Regelmessige personvernrevisjoner av selskapets personvernombud
x	Nøye valg av leverandør