

DATABEHANDLERAVTALE

1. Avtalens bakgrunn og hensikt

Denne databehandleravtalen ("**Databehandleravtalen**") er inngått mellom kunden ("**Behandlingsansvarlig**") og Tradesolution AS (org nr. 968 788 434) ("**Databehandleren**"), i fellesskap omtalt som "**Partene**". Med Databehandleravtalen menes denne generelle avtaleteksten med vedlegg.

Databehandleren samler inn, registrerer, lagrer eller på andre måter behandler personopplysninger på vegne av data behandlingsansvarlig for å levere de avtalte tjenestene etter Partenes avtale om leveranse av tjenester ("**Tjenesteavtalen**").

Formålet med denne Databehandleravtalen er å:

- a) regulere Partenes roller og ansvar ved behandling av personopplysninger etter personopplysningslovgivningen og GDPR artikkel 28 (3) i forbindelse med gjennomføringen av Oppdragsavtalen og
- b) sikre at personopplysninger om De registrerte ikke brukes urettmessig eller kommer uberettigede i hende.

Bestemmelsene i denne Databehandleravtalen skal ved motstrid gå foran tilsvarende bestemmelser i andre avtaler mellom Partene, herunder i Tjenesteavtalen.

2. Definisjoner

Følgende definisjoner gjelder for denne Databehandleravtalen:

"**Databehandleravtalen**" betyr de bestemmelser som fremgår av denne databehandleravtalen med vedlegg.

"**Personopplysning**" betyr enhver opplysning eller informasjon om De registrerte. Dette omfatter, men er ikke begrenset til, de opplysningene som fremgår av Vedlegg 1.

"**Behandling**" (av Personopplysninger) betyr enhver bruk av Personopplysninger, for eksempel innsamling, lagring, organisering, endring eller tilpasning, utlevering og/eller overføring.

"**GDPR**" betyr EU-forordning 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (slik denne er implementert i norsk rett).

"**Personvernlovgivning**" betyr lov om behandling av personopplysninger av 15. juni 2016 nr. 38 med tilførende forskrift og annen lovgivning som implementerer GDPR. .

"**Lov**" betyr enhver annen gjeldende lovgivning som Partene er underlagt.

"**Underleverandør**" betyr andre databehandlere som Databehandleren bruker til å behandle Personopplysningene.

"De registrerte" betyr enhver identifisert eller identifiserbar fysisk person.

3. Generelt

Partene skal Behandle Personopplysninger i samsvar med Personvernlovgivningen, GDPR og denne Avtalen.

Partene skal umiddelbart underrette hverandre hvis en av Partene mener at instruksene eller kravene fra den andre Part utgjør et brudd på Personvernlovgivningen eller GDPR.

Databehandler kan behandle de Personopplysningene som er nødvendige for å levere de avtalte tjenestene samt administrere avtaleforholdet.

Vedlegg 1 beskriver hvilke typer personopplysninger Databehandleren behandler og formålet med behandlingen. Databehandler skal ikke behandle personopplysninger for andre formål enn det som fremgår her.

4. Den Behandlingsansvarliges rettigheter og plikter

Den Behandlingsansvarlige skal fastsette formålene og midlene med behandlingen av Personopplysninger.

Den Behandlingsansvarlige er ansvarlig for at personopplysninger behandles i henhold til kravene i Personvernlovgivningen og GDPR.

Den Behandlingsansvarlige må blant annet sikre at det finnes et lovlig grunnlag for behandlingen av Personopplysningene.

Den Behandlingsansvarlige har rett til å si opp denne Databehandleravtalen dersom Databehandleren ikke handler i tråd med Personvernlovgivningen eller GDPR.

Med mindre noe annet er avtalt eller følger av Lov, har den Behandlingsansvarlige rett til tilgang til og innsyn i de Personopplysningene Databehandleren behandler og de systemene Databehandleren bruker til dette formålet. Databehandler skal gi nødvendig bistand til dette.

5. Instruksjer til Databehandleren

Databehandleren skal kun behandle Personopplysninger etter dokumenterte instruksjer fra den Behandlingsansvarlige, med mindre den behandlingsansvarlige er pålagt å behandle Personopplysninger i henhold til Lov som Databehandleren er underlagt. I et slikt tilfelle skal Databehandleren varsle den Behandlingsansvarlige om den rettslige plikten før behandlingen, med mindre loven forbyr slik at slik informasjon gis av hensyn til allmenn interesse.

Den Behandlingsansvarliges instruksjer til Databehandleren er beskrevet i denne Databehandleravtalen med vedlegg. Den Behandlingsansvarlige kan gi Databehandleren etterfølgende instruksjer så lenge Databehandleren behandler Personopplysninger på vegne av den Behandlingsansvarlige. Slike etterfølgende instruksjer skal alltid gis Databehandleren skriftlig og må være dokumentert.

6. Konfidensialitet

Databehandleren skal holde alle Personopplysninger konfidensiell.

Databehandleren skal bare gi tilgang til Personopplysninger som behandles på vegne av den Behandlingsansvarlige til personer under Databehandlerens myndighet som har behov for innsyn i Personopplysningene, og som er forpliktet til konfidensialitet i form av en konfidensialitetsavtale eller er pålagt lovbestemt konfidensialitet.

Databehandleren skal ha oversikt over hvilke personer som har fått tilgang til Personopplysningene og oppdatere oversikten jevnlig. På bakgrunn av disse gjennomgangene kan tilgangen til personopplysninger trekkes tilbake, dersom tilgang ikke lenger er nødvendig. Personopplysningene vil ikke lenger være tilgjengelig for disse personene.

7. Personvernsikkerhet ved behandlingen av personopplysninger

Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen i tråd med GDPR artikkel 32, herunder blant annet, alt etter hva som er egnet:

- a) pseudonymisering og kryptering av personopplysninger;
- b) evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene;
- c) evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse;
- d) en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.

De tekniske og organisatoriske sikkerhet som er egnet for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, er beskrevet i vedlegg 2.

Databehandleren skal gjøre rimelige anstrengelser for å hjelpe den Behandlingsansvarlige med å sikre at kravene til å etablere et egnet sikkerhetsnivå er i samsvar med GDPR artiklene 35-36.

8. Databehandlerens bruk av underdatabehandlere

Databehandleren skal oppfylle de kravene som er spesifisert i GDPR artikkel 28 nr. 2 og 4 når de engasjerer en annen databehandler.

Databehandleren har gitt den Behandlingsansvarlige en generelle tillatelse til å engasjere en annen databehandler.

Databehandleren skal underrette den Behandlingsansvarlige skriftlig gjennom nettsiden <http://tradesolution.no> om endringer i eller utskiftning av andre databehandlere minst to uker i forveien slik at den Behandlingsansvarlige har mulighet til å motsette seg slik endringer før den/de aktuelle databehandleren/databehandlerne engasjeres. Lengre frister for forhåndsvarsling for særskilte kategorier databehandlere kan gis i Vedlegg 3.

De andre databehandlerne som den Behandlingsansvarlige har godkjent ved inngåelsen av denne Databehandleravtalen fremgår av Vedlegg 3.

Dersom Databehandleren engasjerer en annen databehandler for å utføre spesifikke behandlingsaktiviteter på vegne av den Behandlingsansvarlige, skal nevnte andre databehandler pålegges de samme forpliktelsene med hensyn til vern av personopplysninger som er fastsatt i denne Databehandleravtalen gjennom en avtale eller et annet rettslig dokument.

9. Databehandlerens overføring av personopplysninger til tredjestater og internasjonale organisasjoner

Databehandleren kan overføre de Personopplysningene Databehandleren behandler på vegne av den Behandlingsansvarlige til de land der Databehandleren og Underleverandørene driver sin virksomhet og lagre dem der.

Den Behandlingsansvarlige godtar denne overføringen og lagringen så lenge den er nødvendig for å gjennomføre de avtalte leveransene.

Databehandler skal ikke overføre Personopplysninger til land utenfor EØS eller internasjonale organisasjoner uten et forutgående skriftlig samtykke fra den Behandlingsansvarlige, med mindre EU-kommisjonen har fastslått at tredjestaten, territoriet eller en eller flere spesifiserte sektorer i tredjestaten eller den aktuelle internasjonale organisasjonen sikrer et tilstrekkelig beskyttelsesnivå.

Dersom den Behandlingsansvarlige godtar en slik overføring av Personopplysninger til en tredjestat utenfor EØS eller en internasjonal organisasjon, skal Databehandleren sørge for at kravene for overføring av Personopplysninger til tredjestater eller internasjonale organisasjoner som følger av GDPR kapittel V blir fulgt.

10. Bistand til den Behandlingsansvarlige

Den Behandlingsansvarlige skal fungere som De registrertes kontaktpunkt og gi all nødvendig informasjon om behandlingen av Personopplysninger.

Den Behandlingsansvarlige er ansvarlig for håndteringen av De registrertes anmodninger om innsyn, retting, sletting, begrensning, dataportabilitet etc., samt sikre at slike forespørsler imøtekommes.

Under hensyntagen til behandlingens art, skal Databehandleren hjelpe den Behandlingsansvarlige ved passende tekniske og organisatoriske tiltak, i den grad dette er nødvendig og rimelig for oppfyllelse av den Behandlingsansvarliges forpliktelser til å svare på forespørsler knyttet til De registrertes rettigheter som følger av GDPR kapittel III.

Dersom Databehandleren mottar en forespørsel fra en Registrert, skal den snarest mulig varsle den Behandlingsansvarlige.

11. Partenes ansvar for avvikshåndtering og varsling

Enhver uautorisert behandling av Personopplysninger i strid med GDPR artikkel 32, de fastlagte rutinene for Databehandleren henhold til GDPR artikkel 32, den Behandlingsansvarliges

instruksjer eller Personvernlovgivningen, skal håndteres som et avvik.

Partene skal etablere og opprettholde rutiner og systematiske tiltak for oppfølging av avvik, herunder tiltak for gjenoppretting av normaltilstand, fjerning av årsaken til avviket og hindre gjentakelse.

Partene skal, så snart de får kunnskap om et avvik, uten ugrunnet opphold informere hverandre og umiddelbart iverksette alle nødvendige og hensiktsmessige tiltak for å gjenopprette normaltilstand.

Den Behandlingsansvarlige er ansvarlig for å sende avviksmelding til Datatilsynet og/eller De registrerte i samsvar med GDPR artikkel 33 og 34.

Databehandleren skal, om nødvendig, bistå den Behandlingsansvarlige med å sikre at GDPR artikkel 33 og 34 overholdes.

For at den Behandlingsansvarlige skal kunne varsle Datatilsynet og/eller de Registrerte i samsvar med GDPR artikkel 33 og 34, er Databehandleren pålagt å hjelpe den Behandlingsansvarlige med å innhente all nødvendig informasjon for å informere Datatilsynet og/eller De registrerte i tråd med kravene under GDPR artikkel 33 og 34.

12. Revisjon og inspeksjon

Databehandleren skal gjøre tilgjengelig for den Behandlingsansvarlige all informasjon som er nødvendig for å påvise overholdelse av Databehandlerens forpliktelser i henhold til Personvernlovgivningen, GDPR og denne Databehandleravtalen.

Databehandleren skal jevnlig revidere systemene som brukes for å behandle Personopplysninger. Revisjonen kan omfatte gjennomgang av rutiner, tilfeldige kontroller og andre passende tiltak.

Dersom den Behandlingsansvarlige ber om det, skal Databehandleren, muliggjøre og gjøre rimelige anstrengelser for å bistå til revisjoner av Behandlingsansvarlig eller av en uavhengig revisor med fullmakt fra den Behandlingsansvarlige.

Databehandleren skal muliggjøre og bidra til revisjoner, herunder inspeksjoner, som gjennomføres av den Behandlingsansvarlige eller en annen inspektør på fullmakt fra den Behandlingsansvarlige av Databehandlerens overholdelse av GDPR, gjeldende EU- eller medlemslands Personvernlovgivning og denne Databehandleravtalen. Den Behandlingsansvarlige har selv det direkte ansvaret for kontakt og kommunikasjon med aktuelle tilsynsmyndigheter, herunder Datatilsynet.

Den Behandlingsansvarlige skal dekke kostnadene ved slike revisjoner.

13. Avtalens varighet

Avtalen gjelder så lenge Databehandleren behandler Personopplysninger på vegne av den Behandlingsansvarlige.

14. Opphør

Når denne Databehandleravtalen opphører, skal Databehandleren slette alle Personopplysninger som omfattes av Databehandleravtalen, med mindre gjeldende lover krever

at Personopplysningene lagres

Personopplysningene skal kun slettes etter skriftlig instruks fra den Behandlingsansvarlige.


Partene avtaler nærmere hvordan overføring eller sletting konkret skal skje.

Databehandleren skal skriftlig dokumentere at sletting er foretatt i henhold til avtalen innen rimelig tid etter Databehandleravtalen opphører.

15. Lovvalg og verneting

Databehandleravtalen er underlagt norsk rett. Partene vedtar Oslo Tingrett som rett verneting for enhver tvist om denne Databehandleravtalen.

Vi ber om at avtalen signeres og returneres til Tradesolution AS på følgende e-post adresse: regnskap@tradesolution.no. Husk at avtalen må undertegnes av den som er autorisert til å representere selskapet.

Behandlingsansvarlig (signatur): Tradesolution AS	Databehandler (signatur):
Signatur: 	Navn og tittel:
Navn og tittel: Sigmund Berle Jensen, CEO	Place & date:

Vedlegg 1 – Informasjon om Personopplysningene og formålet med behandlingen

Formålet med behandlingen	Kategorier av personopplysninger	Kategorier av De registrerte	Varigheten av behandlingen
Utførelse av tjenestene angitt i Oppdragsavtalen	Kontaktinformasjon (mobilnummer, e-postadresse, postadresse etc.)	Kunder av den Behandlingsansvarlige	I samsvar med Oppdragsavtalens varighet
Utførelse av tjenestene angitt i Oppdragsavtalen	Personopplysninger (navn, alder, stilling, kjønn etc.)	Kunder av den Behandlingsansvarlige	I samsvar med Oppdragsavtalens varighet

Vedlegg 2 - Beskrivelse av tekniske og organisatoriske tiltak

Skybaserte tjenester:

Databehandler skal til enhver tid benytte de beste egnede sikkerhetsløsning som er tilgjengelig i Microsoft Azure på en optimal måte hensyntatt risikoen.

Autentisering 1:

Databehandler skal benytte to-faktorautentisering for gjestebbrukere (for eksempel konsulenter).

Autentisering 2:

Databehandler skal sikre at ingen ansatte får tilgang til passordet til kundenes brukere. Dette håndteres innad i Azure.

Autorisering:

Adminportalen (internt kundesystem) sikrer at alle kunder og deres brukere kun har tilgang til korrekte data og tjenester.

Single Sign On (SSO):

Databehandler tilbyr SSO til alle kunder som ønsker dette. Det betyr at kunde selv kan legge til og fjerne egne brukeres tilgang til våre tjenester.

Hardware:

Databehandler skal installere Intune eller tilsvarende programvare på all maskinvare (herunder ansattes PCer, smarttelefoner og nettbrett) som meldes inn i domenet. Programvaren overvåker at korrekt sikkerhetspolicy overholdes (passord/pin-koder, VPN-tuneller, e-postlagring og dokumenter).

Intern sikkerhetsinstruks:

Alle ansatte skal lese, forstå og undertegne konfidensialitetsavtaler og vår sikkerhetsinstruks. Sikkerhetsinstruksen oppdateres jevnlig og hver ansatt må re-signere hvert år.

Logging og overvåking av tjenestene:

Databehandler skal overvåke systemer både på bruker- og tjenestenivå samt spore aktivitet for å avdekke, motvirke og håndtere sikkerhetsbrudd.

Databehandler skal etablere gode rutiner for back-up og gjennomføre jevnlig øvelser i disaster recovery for å sikre at data ikke går tapt.

Vedlegg 3 – Oversikt over databehandlerens underdatabehandlere

Selskap	Organisasjonsnummer	Adresse	Kontakt opplysninger	Lagring og behandlingstid (land)
Microsoft Ireland Operation LTD	IE8256796U	Sandyford Business-Estate 1885008, Dublin D 18, IRLAND		Nederland (Azure) Back-up in Ireland
Lime Technologies Norway AS	989 711 393	Inkognitogata 33, 0256 Oslo, Norway	Info.no@lime.tech	Ireland (Amazon)
Nitschke & Borgting AS	962 077 447	Henrik-Ibsensgate 60A 0255 OSLO 8001 Bodø, Norway	+ 47 22 94 25 50	Nederland (Azure). Back-up in Ireland. Store-and-forward operation – servers in Bodø and Trondheim.
Coretrek AS	984 587 406	Nordre Kullerød 1 3241 SANDEFJORD	Info@coretrek.no	Back up in Norway
Lindorff AS	835 302 202	PB. 7055 3007 Drammen, Norway	+ 47 23 21 10 00	Finland (Fujitsu)
Evry Norge AS	933 012 867	Snarøyveien 30A, 1360 Fornebu, Norway	+ 47 23 14 50 00	Processing within the EU/EEA