

DATABEHANDLERAVTALE

Denne **Databehandleravtalen** er inngått [dato] mellom:

(1) Elvia AS, Org.nr 980 489 698 ("**Behandlingsansvarlig**"); og

(2) <COMPANYNAME, Org.nr <COMPANYNUMBER ("**Databehandler**"),

heretter hver for seg også referert til som "**Part**", og samlet som "**Partene**".

Denne Databehandleravtalen består av denne generelle avtaleteksten og følgende Bilag:

- Bilag A: Opplysninger om behandlingen
- Bilag B: Liste over godkjente Under-Databehandlere
- Bilag C: Tekniske og organisatoriske sikkerhetstiltak

1 INNLEDNING

Denne Databehandleravtalen regulerer Partenes rettigheter og forpliktelser i henhold til Forordning (EU) 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 ("**GDPR**"), og norske lov som gjennomfører og supplerer GDPR (heretter samlet "**Personvernlovgivningen**").

I denne Avtalen skal "**personopplysning**", "**behandlingsansvarlig**", "**databehandler**", den "**registrerte**", "**behandling**", "**brudd på personopplysningssikkerhet**" og "**tilsynsmyndighet**", forstås på samme måte som etter Personvernlovgivningen.

2 FORMÅL OG BEHANDLINGSAKTIVITETER

Databehandler vil i forbindelse med <CONTRACTDESCRIPTION ("**Hovedavtalen**") behandle personopplysninger på vegne av Behandlingsansvarlig. Ved motstrid mellom Hovedavtalen og denne Databehandleravtalen, skal Databehandleravtalen ha forrang, dersom motstriden gjelder forhold vedrørende behandling av personopplysninger.

Kategoriene av personopplysninger og registrerte, aktuelle behandlingsaktiviteter, samt formålet og arten av behandlingen som gjennomføres på vegne av den Behandlingsansvarlige er nærmere beskrevet i Bilag A (Opplysninger om behandlingen) til denne Databehandleravtalen.

Databehandleren skal ikke behandle, bruke, oppdatere, lagre eller endre personopplysningene omfattet av denne Databehandleravtalen i større utstrekning eller til andre formål enn det som er nødvendig for at Databehandleren skal kunne oppfylle sine forpliktelser etter denne Databehandleravtalen, Hovedavtalen og Personvernlovgivningen. Databehandleren kan ikke bruke disse personopplysningene til andre formål uten den Behandlingsansvarliges skriftlige samtykke.

3 KRAV TIL BEHANDLINGEN

3.1 Generelle krav

Databehandleren skal kun behandle personopplysninger i samsvar med Hovedavtalen, Databehandleravtalen, den Behandlingsansvarliges instruksjer og Personvernlovgivningen, og skal ikke behandle personopplysningene for andre formål.

Den foregående begrensningen gjelder imidlertid ikke i den utstrekning Databehandleren etter EU-/EØS-medlemstatenes lovgivning er forpliktet til å behandle personopplysningene på en annen måte. Dersom en slik forpliktelse oppstår, skal Databehandleren umiddelbart varsle den Behandlingsansvarlige om dette, med mindre et slik varsel vil være lovstridig, jf. GDPR artikkel 28 nr. 3 bokstav a.

Dersom den Behandlingsansvarliges instruksjer, etter Databehandlerens mening, er i strid med Personvernlovgivningen eller annen lovgivning vedrørende personvern, skal Databehandleren informere den Behandlingsansvarlige om dette uten ugrunnet opphold, jf. GDPR artikkel 28 nr. 3 siste punkt.

Databehandleren skal sørge for at det gjennomføres egnede tiltak, for å sikre at behandlingen av personopplysninger kun utføres i samsvar med Personvernlovgivningens krav til *konfidensialitet* (dvs. at det ikke gis uautorisert innsyn i personopplysninger), *integritet* (dvs. at det ikke utføres uautorisert endring av personopplysninger) og *tilgjengelighet* (dvs. at det sikres tilgang til personopplysninger hvor tilgjengelighet er nødvendig).

Med mindre annet er avtalt, skal alle personopplysninger Databehandleren mottar, samler inn eller på annen måte behandler i henhold til Databehandleravtalen behandles konfidensielt. Denne taushetsplikten skal også gjelde etter Databehandleravtalens opphør.

3.2 Overføring av personopplysninger til Tredjeland

Med mindre det aktuelle landet av EU-kommisjonen anerkjennes som et land som sikrer et tilstrekkelig beskyttelsesnivå etter Personvernlovgivningen, skal Databehandleren ikke overføre personopplysninger til land utenfor EØS ("**Tredjeland**") uten den Behandlingsansvarliges skriftlige forhåndssamtykke. Med overføring til Tredjeland menes også fjerntilgang til personopplysninger fra Tredjeland.

Dersom den Behandlingsansvarlige gir et slikt samtykke, er Databehandleren ansvarlig for å sørge for at overføringen til Tredjeland utføres i samsvar med kravene i GDPR kapittel V, herunder (men ikke begrenset til) at overføringer skjer med et gyldig overføringsgrunnlag. Databehandleren skal dokumentere tiltakene Databehandleren har gjennomført for å overholde forpliktelsene i dette punkt 3.2. Denne dokumentasjonen skal utformes i samsvar med Det europeiske personvernrådet og Datatilsynets anbefalinger og retningslinjer. Dokumentasjonen skal, på anmodning, gjøres tilgjengelig for den Behandlingsansvarlige.

3.3 Krav til personell

Databehandleren skal sørge for at personopplysninger kun behandles av personell som er:

- a) Kjent med Personvernlovgivningens krav og Databehandlerens forpliktelser etter Databehandleravtalen;
- b) Regelmessig opplært til å håndtere og beskytte personopplysninger;

- c) Autorisert til å behandle personopplysninger, og da kun i henhold til Databehandleravtalens formål og på "need-to-know"-basis; og
- d) Underlagt enten lovpålagt eller avtalemessig taushetsplikt, jf. GDPR artikkel 28 nr. 3 bokstav b.

4 SIKKERHET

4.1 Informasjonssikkerhet ved behandling av personopplysninger

Databehandleren skal i samsvar med GDPR artikkel 32 gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et tilstrekkelig sikkerhetsnivå ved behandlingen av personopplysningene, herunder for å beskytte personopplysningene mot utilsiktet eller ulovlig tilintetgjøring, tap, endring eller uautorisert utlevering av eller tilgang til personopplysninger, og ethvert annet brudd på personopplysningssikkerheten.

Omfanget av tiltakene beskrevet under punkt ovenfor, skal bedømmes ut fra den tekniske utviklingen, implementeringskostnadene, behandlingens art, omfang, formål og sammenhengen den utføres i, samt risiko. Eksempel på slike tiltak er blant annet:

- a) Pseudonymisering og kryptering av personopplysningene;
- b) Tiltak som sikrer evnen til å bevare vedvarende fortrolighet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene;
- c) Tiltak som sikrer evnen til å gjenopprette tilgjengeligheten og tilgangen til personopplysningene i rett tid dersom det oppstår en fysisk eller teknisk hendelse; og
- d) En prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.

Databehandleren skal i tillegg gjennomføre sikkerhetstiltakene nærmere beskrevet i Bilag C (Tekniske og organisatoriske sikkerhetstiltak) til denne Databehandleravtalen.

Databehandleren skal dokumentere sikkerhetstiltakene og rutinene som Databehandleren har gjennomført for å overholde forpliktelsene i dette punkt 4.1. Dokumentasjonen skal være tilgjengelig for den Behandlingsansvarlige, ved den Behandlingsansvarliges anmodning.

4.2 Brudd på personopplysningssikkerhet

Dersom det forekommer et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysningene, skal Databehandleren umiddelbart og senest innen 24 timer varsle den Behandlingsansvarlige og gi nødvendig informasjon og bistand slik at den Behandlingsansvarlige kan oppfylle sine rapporteringsplikter etter Personvernlovgivningen (se GDPR artikkel 4 nr. 12 og GDPR artikkel 33 nr. 2).

Databehandleren skal videre iverksette nødvendige tiltak for å begrense virkningen av, og rette sikkerhetsbruddet.

5 VURDERING AV PERSONVERNKONSEKVENSER

Dersom Databehandleren er eller blir oppmerksom på at behandlingen av personopplysningene vil medføre en høy risiko for de registrertes personvern, skal Databehandleren uten unødig opphold informere den Behandlingsansvarlige om dette og gi nødvendig bistand slik at den

Behandlingsansvarlige kan gjennomføre en vurdering av personvernkonsekvensene, samt rådføre seg med den relevante tilsynsmyndigheten om nødvendig (se GDPR artikkel 35 og artikkel 36).

6 SAMARBEID MED DEN BEHANDLINGSANSVARLIGE OG TILSYNSMYNDIGHETENE

Databehandleren skal for egen regning bistå, inkludert ved hjelp av egnede tekniske og organisatoriske tiltak, den Behandlingsansvarlige med å svare på og gjennomføre (i) enhver henvendelse fra den registrerte vedrørende den registreres rettigheter etter GDPR kapittel III (inkludert men ikke begrenset til den registrertes rett til innsyn, korrigering, begrensnings, innsigelse, sletting og dataportabilitet); samt (ii) enhver annen henvendelse fra den registrerte, tilsynsmyndigheter og andre tredjeparter vedrørende behandling av personopplysninger. Dersom en slik henvendelse, klage eller annen kommunikasjon blir sendt direkte til Databehandleren, skal Databehandleren uten ugrunnet opphold videreformidle henvendelsen til den Behandlingsansvarlige og informere om alle forhold ved henvendelsen/klagen.

Databehandleren skal håndtere henvendelser fra Behandlingsansvarlig knyttet til Databehandlerens behandling av personopplysninger, uten ugrunnet opphold. Databehandleren skal videre til enhver tid kunne fremvise dokumentasjon som viser at Databehandleren oppfyller Personvernlovgivningens krav.

7 INNSYN OG REVISJON

Databehandleren skal etablere, holde vedlike og kunne dokumentere tilstrekkelige internkontrollrutiner vedrørende Databehandlerens behandling av personopplysninger under denne Databehandleravtalen, i henhold til Personvernlovgivningen eller som påkrevet av den Behandlingsansvarlige. Databehandleren skal også etablere og holde vedlike en oversikt/protokoll over behandlingsaktiviteter den foretar på vegne av den Behandlingsansvarlige, jf. GDPR artikkel 30 nr. 2.

Databehandleren skal gjøre tilgjengelig for den Behandlingsansvarlige all informasjon som er nødvendig for å påvise at forpliktelsene fastsatt i denne Databehandleravtalen er oppfylt, samt på andre måter bistå den Behandlingsansvarlige med å oppfylle sine forpliktelser etter Personvernlovgivningen.

Med mindre annet er avtalt eller følger av Personvernlovgivningen, skal den Behandlingsansvarlige gis tilgang til personopplysninger som behandles i medhold av denne Databehandleravtalen, og Databehandlerens systemer som benyttes til dette formålet.

Databehandleren skal også muliggjøre og bidra til revisjoner, herunder inspeksjoner, som gjennomføres av den Behandlingsansvarlige (eller tredjepart som representerer den Behandlingsansvarlige) eller myndigheter for å kontrollere at Databehandleren overholder sine forpliktelser etter denne Databehandleravtalen, jf. GDPR artikkel 28 nr. 3 bokstav h.

8 BRUK AV UNDER-DATABEHANDLERE

Databehandleren skal ikke bruke eller på annen måte engasjere tredjeparter til å bistå med eller sette bort behandlingen av personopplysningene under denne Databehandleravtalen ("**Under-Databehandler**"), uten den Behandlingsansvarliges skriftlige forhåndssamtykke. Dersom Databehandleren i samsvar med dette punkt 8 engasjerer en Under-Databehandler, skal Databehandleren sørge for at Under-Databehandleren pålegges tilsvarende forpliktelser som Databehandleren er pålagt i henhold til Databehandleravtalen.

En liste over Under-Databehandlere som er godkjent av den Behandlingsansvarlige er inntatt i Bilag B. Endring av dette bilaget krever skriftlig samtykke fra den Behandlingsansvarlige.

Databehandlerens bruk av Under-Databehandlere skal ikke redusere eller begrense Databehandlerens ansvar og forpliktelser etter denne Databehandleravtalen.

9 AVTALENS VARIGHET

Databehandleravtalen gjelder så lenge Databehandleren behandler personopplysninger på vegne av den Behandlingsansvarlige for det formål som er beskrevet i denne Databehandleravtalen og i Hovedavtalen.

Ved Databehandlerens brudd på denne Databehandleravtalen eller Personvernlovgivningen kan den Behandlingsansvarlig pålegge Databehandler å stanse den videre behandlingen av Personopplysningene med øyeblikkelig virkning.

Selv om Hovedavtalen opphører, vil Databehandleravtalen fortsette å gjelde så lenge Databehandleren behandler personopplysninger på vegne av den Behandlingsansvarlige.

10 LAGRING OG SLETTING

Databehandleren skal følge den Behandlingsansvarliges meddelte rutiner og instruksjoner vedrørende sletting og lagring av personopplysninger.

Ved den Behandlingsansvarliges anmodning (jf. GDPR artikkel 28 nr. 3 bokstav g) skal Databehandleren enten:

- a) returnere til Behandlingsansvarlig (eller en tredjepart utpekt av den Behandlingsansvarlige) personopplysningene omfattet av denne Databehandleravtalen i et alminnelig benyttet format; eller
- b) slette alle personopplysninger og tilhørende dokumentasjon (inkludert kopier) omfattet av denne Databehandleravtalen.

Den ovennevnte plikten til å slette eller returnere personopplysninger omfattet av Databehandleravtalen gjelder ikke dersom Databehandleren er pålagt fortsatt lagring av personopplysningene etter preseptorisk lovgivning.

Ved Databehandleravtalens opphør etter punkt 9 skal Databehandleren øyeblikkelig stanse behandlingen av personopplysninger omfattet av denne Databehandleravtalen, samt gi skriftlig bekreftelse på at dette har blitt etterkommet.

11 ANSVAR

Hver Part kan kreve erstattet ethvert direkte tap som denne Parten lider som følge av den andre Partens mislighold av Databehandleravtalen. For å unngå tvil, direkte tap omfatter, men er ikke begrenset til:

- a) kostnader knyttet til rekonstruksjon av skadet eller tapt data, samt andre direkte kostnader den skadelidende Parten pådrar seg som følge av skade på- eller tap av data, og
- b) krav og overtredelsesgebyr fra tilsynsmyndighetene mot den ene Parten som følge av den andre Partens mislighold av Databehandleravtalen.

Den enkelte Parts samlede og maksimale erstatningsansvar under denne Databehandleravtalen er begrenset til det høyeste av følgende beløp:

- a) En sum tilsvarende 2x (to ganger) den skadevoldende Partens maksimale erstatningsansvar under Hovedavtalen, eller
- b) NOK 10 000 000,- (ti millioner kroner).

Har den skadevoldende Part eller noen denne svarer for utvist grov uaktsomhet eller forsett, gjelder ikke de ovennevnte erstatningsbegrensningene.

Partenes erstatningsansvar for krav fra registrerte eller andre fysiske personer for brudd på Personvernlovgivningen, skal utelukkende reguleres av GDPR artikkel 82 (og ikke dette punkt 11).

12 KOSTNADER VED ETTERLEVELSE AV DATABEHANDLERAVTALEN

Hver Part er ansvarlige for egne kostnader som oppstår som følge av Partens etterlevelse av denne Databehandleravtalen.

13 KONTAKTPERSONER HOS DEN BEHANDLINGSANSVARLIGE OG DATABEHANDLEREN

Partene kan kontakte hverandre angående denne Databehandleravtalen via oppgitte kontaktpersoner. Partene forplikter seg til å orientere hverandre løpende om endringer som gjelder kontaktpersoner.

For den Behandlingsansvarlige:

Navn: [sett inn]
Stilling: [sett inn]
Telefonnummer: [sett inn]
E-postadresse: [sett inn]

For Databehandleren:

Navn: [sett inn]
Stilling: [sett inn]
Telefonnummer: [sett inn]
E-postadresse: [sett inn]

14 LOVVALG OG VERNETING

Partenes rettigheter og plikter etter Databehandleravtalen bestemmes i sin helhet av norsk rett. Dersom tvisteløsning og vernetting er avtalt i Hovedavtalen, skal enhver tvist mellom Partene om tolkningen eller rettsvirkningene av denne Databehandleravtalen løses i samsvar med Hovedavtalens bestemmelser vedrørende tvisteløsning og vernetting. Dersom Hovedavtalen ikke inneholder slike bestemmelser, kan hver av Partene forlange tvisten avgjort med endelig virkning ved norske domstoler, med den Behandlingsansvarliges hjemting som avtalt vernetting.

* * *

Avtalen er utstedt i 2 (to) eksemplarer, hvor Partene har mottatt hvert sitt.

[dato]

Elvia AS

<COMPANYNAME

[sett inn navn]

[sett in stilling]

[sett inn navn]

[sett in stilling]

BILAG A - OPPLYSNINGER OM BEHANDLINGEN

Tabellen nedenfor inneholder en nærmere beskrivelse av Databehandlerens behandling av personopplysninger på vegne av den Behandlingsansvarlige.

Formålet med Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige er:	[beskriv]
Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige skal primært dreie seg om (behandlingens art):	[beskriv]
Behandlingen omfatter følgende typer av personopplysninger om de registrerte:	[beskriv]
Behandlingen omfatter følgende kategorier av registrerte:	[beskriv]
Behandlingen gjennomføres på følgende lokasjon:	[beskriv]
Sletterutiner knyttet til behandlingen:	[beskriv]

BILAG B - LISTE OVER GODKJENTE UNDER-DATABASEHANDLERE

For å kunne levere de tjenester som følger av Hovedavtalen har Databehandler inngått avtaler om tjenesteleveranser fra Under-Databehandlerne listet opp nedenfor.

Navn på Under-Databehandler:	
Org.nr.	
Adresse	
Beskrivelse av tjenesteleveranse	
Lokasjon for utførelse av tjenesteleveranse	
Dersom bruken av Under-Databehandleren medfører overføring av personopplysninger til Tredjeland, oppgi informasjon om: - hvilke personopplysninger som skal overføres; - Tredjelandet personopplysningene skal overføres til; og - hvilket overføringsgrunnlag som vil benyttes.	
Informasjon om Under-databehandlerens etterlevelse av Personvernlovgivningen	
Navn på Under-Databehandler:	
Org.nr.	
Adresse	
Beskrivelse av tjenesteleveranse	
Lokasjon for utførelse av tjenesteleveranse	
Dersom bruken av Under-Databehandleren medfører overføring av personopplysninger til Tredjeland, oppgi informasjon om: - hvilke personopplysninger som skal overføres; - Tredjelandet personopplysningene skal overføres til; og - hvilket overføringsgrunnlag som vil benyttes.	
Informasjon om Under-databehandlerens etterlevelse av Personvernlovgivningen	

BILAG C - TEKNISKE OG ORGANISATORISKE SIKKERHETSTILTAK

Fyll inn hvilke sikkerhetstiltak din virksomhet har utført. Tiltakene opplistet nedenfor er ikke uttømmende. Dersom din virksomhet har gjennomført ytterligere/andre tiltak, bør disse også beskrives.

[beskriv kravene som gjelder pseudonymisering og kryptering av personopplysninger]

[beskriv kravene som gjelder å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemer og -tjenester]

[beskriv kravene som gjelder evnen til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse]

[beskriv kravene som gjelder prosesser for regelmessig testing, vurdering og evaluering av de tekniske og organisatoriske tiltakenes effektivitet når det gjelder å sikre personopplysningsikkerheten]

[beskriv kravene som gjelder tilgang til opplysningene via internett]

[beskriv kravene som gjelder beskyttelse av opplysninger under overføring]

[beskriv kravene som gjelder beskyttelse av opplysninger under oppbevaring]

[beskriv kravene som gjelder fysisk sikring av lokasjoner hvor personopplysninger blir behandlet]

[beskriv kravene som gjelder bruk av hjemme-/fjernarbeidsplasser]

[beskriv kravene som gjelder logging]

[beskriv eventuelle sikkerhetssertifiseringer Databehandleren innehar]