

Bilag 1 - Databehandleravtale

1 PARTER OG AVTALENS HENSIKT

- 1.1 Aimz AS omtales her som «**Databehandler**» og Kunden (som definert i Kontrakten) omtales som «**Behandlingsansvarlig**».
- 1.2 Denne Databehandleravtalens («**Avtalen**») hensikt er å regulere partenes rettigheter og plikter etter gjeldende personvernregelverk, herunder personopplysningsloven av 2018 som inkorporerer EUs Personvernforordning 2016/679 (GDPR) (heretter samlet benevnt som «personvernregelverket»).

2 GENERELT

- 2.1 Formålet med denne Avtalen er å regulere Databehandlers bruk av personopplysninger på vegne av Behandlingsansvarlig som Databehandler får tilgang til i forbindelse med levering av tjenester under Lisensavtale for bruk av AIMZ («**Kontrakten**»), i samsvar med GDPR artikkel 28.
- 2.2 Vedlegg A og B til denne Databehandleravtalen utgjør en integrert del av avtalen, og inneholder henholdsvis nærmere opplysninger om behandlingen av personopplysninger og liste over godkjente underdatabehandlere
- 2.3 Avtalen har forrang i relasjon til eventuelle tilsvarende personvernrettslige bestemmelser i andre avtaler mellom partene, herunder i Kontrakten.
- 2.4 Denne Avtalen fritar ikke Databehandleren fra plikter som Databehandleren er pålagt etter personvernregelverket eller annen lovgivning. Denne Avtalen regulerer kun Databehandlers behandling på vegne av Behandlingsansvarlig i tilknytning til Løsningen. For personopplysninger som Databehandler behandler som egen behandlingsansvarlig (f.eks. CRM, fakturering, leverandør- og supportkanaler utenfor Løsningen), gjelder Databehandlers egne personverndokumenter og ikke denne Avtalen.

3 DEN BEHANDLINGSANSVARLIGES RETTIGHETER OG PLIKTER

- 3.1 Den Behandlingsansvarlige er ansvarlig for å sikre at behandlingen av personopplysninger skjer i overensstemmelse med personvernregelverket.
- 3.2 Den Behandlingsansvarlige har rett og plikt til å bestemme formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes. Den Behandlingsansvarlige er videre ansvarlig for å sikre at det foreligger et behandlingsgrunnlag for behandlingen av personopplysninger som Databehandler er instruert om å gjøre.

4 DATABEHANDLERENS PLIKTER

- 4.1 **Instrukser:** Databehandler skal bare behandle personopplysninger etter dokumenterte instruksjoner fra den Behandlingsansvarlige, med mindre noe annet kreves av nasjonal eller europeisk rett. Databehandler skal omgående underrette den Behandlingsansvarlige dersom Databehandler er av den oppfatning at en instruks er i strid med personvernregelverket.
- 4.2 **Konfidensialitet:** Databehandler kan bare gi tilgang til personopplysninger som behandles på vegne av den Behandlingsansvarlige til personer som er underlagt Databehandlers instruksjonsmyndighet og som har forpliktet seg til konfidensialitet eller er underlagt en passende lovbestemt taushetsplikt, og kun i nødvendig omfang.

Databehandleren skal etter anmodning fra den Behandlingsansvarlige kunne påvise at de aktuelle personene underlagt Databehandlerens instruksjonsmyndighet er underlagt ovennevnte taushetsplikt.

- 4.3 **Sikkerhet:** Databehandler skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, jf. GDPR artikkel 32. Databehandler skal også bistå den Behandlingsansvarlige med å overholde den Behandlingsansvarliges plikter etter GDPR artikkel 32, blant annet ved å stille nødvendig informasjon til rådighet for den Behandlingsansvarlige.

Den Behandlingsansvarlige skal på samme måte stille nødvendig informasjon til rådighet for Databehandleren som gjør vedkommende i stand til å identifisere og vurdere risikoer i samsvar med GDPR artikkel 32.

5 UNDERDATABEHANDLERE

- 5.1 Databehandler skal oppfylle kravene som følger av GDPR artikkel 28 nummer 2 og 4 i tilfeller hvor Databehandler benytter en annen databehandler (en «**underdatabehandler**»).
- 5.2 Den Behandlingsansvarlige gir en generell godkjenning til at Databehandler kan benytte underdatabehandlere. Databehandler skal føre en til enhver tid oppdatert liste over gjeldende underdatabehandlere på sin nettside. Endringer i listen (tilføyelse eller utskiftning av underdatabehandlere) vil bli publisert på Databehandlers nettside. Databehandler kan i tillegg varsle den Behandlingsansvarlige per e-post, men dette er ikke et krav for at endringen skal være gyldig. Den Behandlingsansvarlige kan innen tretti (30) dager etter publisert endring fremsette saklig begrunnede innvendinger mot en ny underdatabehandler. Dersom partene ikke kommer til enighet, kan den Behandlingsansvarlige si opp Kontrakten med virkning fra den dato den nye underdatabehandleren skulle tas i bruk. Fortsett bruk av Tjenesten etter utløpet av innsigelsesfristen anses som aksept av den nye underdatabehandleren. Listen over underdatabehandlere som den Behandlingsansvarlige allerede har godkjent fremgår av vedlegg B.
- 5.3 Ved engasjering av underdatabehandlere skal underdatabehandleren som et minimum pålegges tilsvarende forpliktelser med hensyn til vern av personopplysninger som er fastsatt i denne Avtalen. En kopi av underdatabehandleravtale og eventuelle etterfølgende endringer skal – ved den Behandlingsansvarliges anmodning – sendes til den Behandlingsansvarlige, som på denne måten har mulighet til å sørge for at underdatabehandleren er pålagt de samme forpliktelsene med hensyn til vern av personopplysninger som er fastsatt i denne Avtalen. Kommersielle bestemmelser som ikke påvirker det personopplysningsvernrettslige innholdet av underdatabehandleravtalen, er ikke underlagt kravet om kopi til den Behandlingsansvarlige.
- 5.4 Databehandler skal være fullt ut ansvarlig for underdatabehandlerens eventuelle manglende oppfyllelse av sine personvernrettslige forpliktelser.

6 OVERFØRING TIL TREDJELAND ELLER INTERNASJONALE ORGANISASJONER

- 6.1 Databehandler kan kun overføre personopplysninger til tredjeland eller internasjonale organisasjoner etter dokumenterte instruks fra den Behandlingsansvarlige, med mindre overføring kreves i henhold til nasjonal eller europeisk rett. I så fall skal den Behandlingsansvarlige underrettes om nevnte rettslige krav med mindre allmenne interesser er til hinder for dette. For å unngå tvil, vil en overføring til tredjeland i forbindelse med bruken av godkjente underleverandører, iht. punkt 5 over, alltid regnes som en overføring etter dokumentert instruks fra den Behandlingsansvarlige. Enhver overføring skal alltid skje i overensstemmelse med GDPR kapittel V, herunder være underlagt et lovlig overføringsgrunnlag. Overføringsgrunnlag ved tredjeland. For overføringer av personopplysninger til tredjeland (herunder USA) skal Databehandler sikre at overføringen skjer i samsvar med GDPR kapittel V, herunder ved bruk av EUs standard kontraktsklausuler (EU SCC 2021/914) og gjennomføring av en Transfer Impact Assessment (TIA) med nødvendige tilleggstiltak. Databehandler skal på forespørsel fra Behandlingsansvarlig gjøre tilgjengelig overordnet dokumentasjon som bekrefter gyldig overføringsgrunnlag.
- 6.2 Denne Avtalen skal ikke forveksles med standard personvernbestemmelser som omhandlet i GDPR artikkel 46 nummer 2 bokstav c og d, og denne Avtalen kan ikke utgjøre et grunnlag for overføring av personopplysninger under GDPR kapittel V.

7 BISTAND TIL DEN BEHANDLINGSANSVARLIGE

- 7.1 I den grad det er mulig, skal Databehandler bistå den Behandlingsansvarlige med å besvare anmodninger fra registrerte om oppfyllelse av deres rettigheter, bistå med informasjon og varsling i tilfeller av kvalifiserte brudd på personopplysningssikkerheten, bistå med vurdering av personvernkonsekvenser samt bistå i forbindelse med forhåndsdrøftelser med Datatilsynet.

- 7.2 Ved brudd på personopplysningssikkerheten skal Databehandleren underrette den Behandlingsansvarlige om bruddet uten ugrunnet opphold etter å ha fått kjennskap til det, slik at den Behandlingsansvarlige kan overholde sin forpliktelse til å melde bruddet til den kompetente tilsynsmyndigheten (i Norge: *Datatilsynet*), jf. GDPR artikkel 33.

8 ANSVAR

- 8.1 Hver part er ansvarlig for ethvert økonomisk tap den påfører den andre parten ved mislighold av denne Avtalen. Ansvarsbegrensningene i Kontrakten gjelder også her.
- 8.2 Hver part er ansvarlig overfor den registrerte som har lidd materiell eller ikke-materiell skade hvis skaden er forårsaket av at parten har opptrådt utenfor eller i strid med denne Avtalen eller personvernregelverket, jf. GDPR artikkel 82 nummer 1.

9 SLETTING OG RETURNERING AV PERSONOPPLYSNINGER

- 9.1 Ved opphør av databehandlertjenestene skal Databehandler, etter den Behandlingsansvarliges valg, slette alle personopplysninger som er blitt behandlet på vegne av den Behandlingsansvarlige eller levere tilbake alle personopplysninger og slette eksisterende kopier, med mindre nasjonal eller europeisk rett er til hinder for dette, eller annet er avtalt i Kontrakten. Databehandleren forplikter seg til å utelukkende behandle personopplysningene til de(t) formål, med den varighet og under de betingelsene som disse reglene fastsetter.
- 9.2 Sletting hos underdatabehandlere. Databehandler skal ved opphør instruere relevante underdatabehandlere om sletting eller retur av personopplysninger som behandles på vegne av Behandlingsansvarlig. Databehandler skal bekrefte gjennomført sletting/retur innen rimelig tid (normalt innen 30–90 dager) etter opphør, med mindre annen frist følger av lov.

10 REVISJONER, HERUNDER INSPEKSJONER

- 10.1 Databehandler skal stille til den Behandlingsansvarliges disposisjon all informasjon som er nødvendig for å påvise etterlevelse av forpliktelsene etter personvernregelverket og denne Avtalen. Videre skal Databehandler muliggjøre og bidra til revisjoner, herunder inspeksjoner, som utføres av den Behandlingsansvarlige eller en annen revisor som er bemyndiget av den Behandlingsansvarlige.

11 IKRAFTTREDELSE OG OPPHØR

- 11.1 Avtalen trer i kraft på samme dato som Kontrakten.
- 11.2 Avtalen gjelder så lenge databehandlertjenestene varer og kan da ikke sies opp, med mindre partene avtaler andre vilkår som regulerer levering av databehandlertjenestene i samsvar med gjeldende personvernregelverk.
- 11.3 Dersom Kontrakten eller leveringen av databehandlertjenestene opphører, og personopplysningene er slettet eller returnert til den Behandlingsansvarlige i overensstemmelse med punkt 9.1 over, opphører denne Avtalen.

VEDLEGG A TIL DATABASEHANDLERAVTALE: BESKRIVELSE AV BEHANDLINGEN

1. Formålet med Databehandlers behandling av personopplysninger på vegne av den Behandlingsansvarlige er:

Formålet med Databehandlers behandling av personopplysninger på vegne av Behandlingsansvarlig er å levere Aimz' digitale tjeneste for økonomi- og prosjektstyring i bygge- og anleggsprosjekter, herunder funksjonalitet for fakturaimport, prognoseoppfølging og rapportering.

Databehandlingen skjer utelukkende for å muliggjøre Behandlingsansvarliges bruk av Løsningen og for å støtte driften av denne.

2. Databehandlers behandling av personopplysninger på vegne av den Behandlingsansvarlige skal primært dreie seg om (behandlingens art):

Behandlingen vil omfatte innhenting og tilgang til relevante opplysninger fra Behandlingsansvarliges systemer, registrering, organisering, strukturering, sammenstilling og samkjøring av data, analyse, beregning av KPI-er, utarbeidelse og tilgjengeliggjøring av rapporter og dashboards, lagring, gjenfinning, bruk og rådgivning, samt begrensning og sletting ved opphør. Databehandler utfører i tillegg teknisk støtte, feilsøking og håndtering av nødvendige drifts- og tilgangsløgger knyttet til tjenesten.

AI-behandling: Behandlingen kan omfatte bruk av AI-funksjonalitet for analyse, prediksjon og generering av forslag relatert til økonomi- og prosjektstyring (f.eks. indikatorer/health score, innsikter og forslag til oppfølging). AI-funksjoner skal ikke trenes på Behandlingsansvarliges data, med mindre annet er særskilt avtalt skriftlig. Databehandler skal sikre at AI-leverandører kun behandler data i samsvar med denne Avtalen, og innenfor avtalt region der dette er relevant.

Lagring og drift: Løsningen driftes i Microsoft Azure i EU/EØS. Databehandler skal sikre at all data som behandles for Behandlingsansvarlig lagres i EU/EØS, med mindre annet er avtalt i samsvar med §6.

3. Behandlingen omfatter følgende typer av personopplysninger om de registrerte:

Behandlingsansvarlig vil normalt behandle, herunder ha tilgang til, følgende personopplysninger:

Kontakt- og identitetsdata: navn, stilling/rolle, avdeling, e-post, telefon.

Arbeids-/organisasjonsdata: organisatorisk tilknytning, kostnadssted/prosjekt, brukerattributter (tilgangsrolle/ID i relevante systemer).

Transaksjons- og økonomidata som kan knyttes til personer: reiseregninger/utlegg (ikke vedlegg med særlige kategorier), ordre-/fakturareferanser med kontaktfelt, timelister knyttet til prosjekt/ressurs (der dette inngår i økonomidata).

System-/driftslogger knyttet til leveransen: støtte-/hendelseslogger, tilgangsløgger (minimert til det nødvendige, typisk 90 dager oppbevaring).

Support- og kommunikasjonshenvendelser: navn, e-post, innhold i henvendelser (inkl. vedlegg dersom tilsendt), tekniske metadata (tidspunkt, nettleser/IP) i den grad nødvendig for å yte støtte til Løsningen.

Den Behandlingsansvarlige vil som hovedregel ikke behandle særlige kategorier av (sensitive) personopplysninger, jf. GDPR artikkel 9 nr. 1 under denne Avtalen.

4. Behandlingen omfatter følgende kategorier av registrerte:

Behandlingen omfatter ansatte hos Behandlingsansvarlig, herunder ledere og andre personer med roller som er relevante for økonomi- og prosjektoppfølging, samt kontaktpersoner hos Behandlingsansvarliges kunder og leverandører som fremgår av økonomi- og fakturadata. Behandlingen kan også omfatte innleide konsulenter og oppdragstakere dersom personopplysninger om disse inngår i prosjekt- eller økonomidata.

5. Databehandlers behandling av personopplysninger på vegne av den Behandlingsansvarlige har følgende varighet:

Databehandler vil behandle personopplysninger så lenge Kontrakten består.

VEDLEGG B TIL DATABEHANDLERAVTALE: UNDERDATABEHANDLERE

Godkjente underdatabehandlere

Ved Avtalens ikrafttredelse har den Behandlingsansvarlige godkjent bruken av undernevnte underdatabehandlere for den behandlingsaktiviteten som er beskrevet for vedkommende underdatabehandler. Databehandleren kan ikke – uten den Behandlingsansvarliges godkjennelse – benytte en underdatabehandler til en annen behandlingsaktivitet enn den som er avtalt for vedkommende eller bruke en annen underdatabehandler til den beskrevne behandlingsaktiviteten.

LEVERANDØR	TJENESTE/ROLLE	LOKASJON	BESKRIVELSE AV BEHANDLINGEN
Fronted	IT-konsulentselskap	EEA	Tilbyr fulltids systemutviklere som bistår AIMZ i programvareutvikling
Microsoft	Hosting (Azure) og admin (365)	EEA	Lagring og behandling av applikasjonsdata, e-post, videokonferanse, databaser, backup, drift og overvåking.
Hubspot	CRM	EEA	Administrasjon av kundens brukere/kontakter og aktivitetsmønstre for oppfølging, onboarding og helseindikatorer.
Intercom	Kundestøtte/Chat	US	Navn, e-post, henvendelsesinnhold og tekniske metadata for brukerstøtte knyttet til Løsningen. Overføringsgrunnlag: EU SCC (2021/914) + TIA; sletting ved opphør iht. §9.
PostHog	Produktanalyse	EEA	Hendelser/brugeratferd, pseudonyme ID-er og teknisk metadata for analyse og produktforbedring.
OpenAI	Produktberikelse	US	Analyse og forslag Overføringsgrunnlag: EU SCC (2021/914) + TIA; sletting ved opphør iht. §9.