DATABEHANDLERAVTALE

Denne databehandleravtalen («**Databehandleravtalen**») er inngått mellom Kunden («**Behandlingsansvarlige**») og Leverandøren («**Databehandleren**») med vedlagt spesifikasjon («**Vedlegget**») og inngår i Hovedavtalen.

Databehandleren vil som følge av ytelsene etter Hovedavtalen behandle personopplysninger på vegne av Behandlingsansvarlige i henhold til personvernregelverket (GDPR).

Formålet for behandlingen er å utføre ytelsene etter Hovedavtalen som nærmere spesifisert i Vedlegget.

Bistand til Behandlingsansvarlig: Databehandler skal bistå Behandlingsansvarlige med plikter etter GDPR artikkel 32-36, herunder sikkerhet, varsling om brudd på personopplysningssikkerheten, vurdering av personvernkonsekvenser og besvarelse av anmodninger fra registrerte, så langt det er mulig ved hjelp av egnede tekniske og organisatoriske tiltak.

Instrukser fra behandlingsansvarlig: Databehandleren skal kun behandle personopplysningene etter dokumenterte instrukser fra Behandlingsansvarlige og i overensstemmelse med personvernregelverket. Databehandler skal underrette Behandlingsansvarlige dersom Databehandler mener at en instruks er i strid med personvernregelverket. Krever Behandlingsansvarlig at behandlingen skal fortsette, er dette Behandlingsansvarliges ansvar.

Konfidensialitetsplikt: Databehandler skal sikre at personer som er autorisert til å behandle personopplysningene hos Databehandleren har forpliktet seg til å behandle opplysningene konfidensielt eller er underlagt en egnet lovfestet taushetsplikt. Se også punkt **Error! Reference source not found.** i Hovedavtalen.

Informasjonsplikt: Databehandler skal gjøre tilgjengelig for Behandlingsansvarlige all nødvendig informasjon, herunder dokumentasjon av sikkerhetstiltak, behandlingsaktiviteter, og annen informasjon som er nødvendig for å påvise etterlevelse etter GDPR artikkel 28.

Sikkerhetstiltak: Databehandleren skal gjennomføre tilstrekkelige tekniske og organisatoriske tiltak etter GDPR artikkel 32. Spesifikke tiltak er beskrevet i Vedlegget.

Underdatabehandlere: Databehandleren kan bruke de leverandører som er beskrevet i Vedlegget til å utføre ytelser som omfatter behandling av Behandlingsansvarliges personopplysninger (underdatabehandler) som er godkjent av Behandlingsansvarlig ved inngåelsen av Databehandleravtalen.

Skal Databehandleren engasjere eller bytte ut underdatabehandlere, skal Behandlingsansvarlige varsles minst fire uker før endringen slik at Behandlingsansvarlige får anledning til å motsette seg endringen. Databehandleren har rett til å si opp Hovedavtalen med to ukers varsel fra utløp av nevnte fire ukers frist om endringen av underdatabehandler har vesentlig betydning for ytelsene etter Hovedavtalen, samt at endringen er nødvendig for tjenestens levering og partene ikke kommer til enighet om alternativ løsning.

Databehandleren skal inngå avtale med underdatabehandler som pålegger disse de samme forpliktelsene for behandling av personopplysninger som Databehandleren har etter Databehandleravtalen, og Databehandleren er ansvarlig for at underdatabehandler oppfyller disse pliktene.

Overføring av personopplysninger til tredjeland: Databehandler skal ikke overføre personopplysninger til land utenfor EØS uten godkjenning fra Behandlingsansvarlig eller ved godkjent underdatabehandler i tredjeland. Det skal alltid foreligge lovlig overføringsgrunnlag etter GDPR kapittel V.

Revisjon/inspeksjon: Databehandler skal muliggjøre og bidra til revisjoner/inspeksjoner fra Behandlingsansvarlige/annen med fullmakt fra Behandlingsansvarlige. Revisjon kan gjennomføres én gang i året om det ikke foreligger særlige forhold, som brudd på Databehandleravtalen eller personvernbrudd som skyldes Databehandler. Tidspunkt og omfang av revisjonen skal varsles med minst 14 dagers skriftlig varsel. Databehandler dekker egne kostnader ved revisjon. Revisjoner ut over nevnte skal Behandlingsansvarlig dekke.

Varsling: Databehandler skal uten ugrunnet opphold underrette Behandlingsansvarlige ved brudd på personopplysningssikkerheten etter å ha fått kjennskap til bruddet. Varslingen skal så langt mulig inneholde opplysningene som kreves etter artikkel 33(3).

Sletting/retur ved opphør av Databehandleravtalen: Databehandler skal etter Behandlingsansvarliges valg slette eller tilbakelevere personopplysningene etter at behandlingen er utført, samt slette kopier, med mindre lagring kreves. Nevnte skal bekreftes av Databehandler på forespørsel. Sletting skjer tidligst 30 dager etter varsel om sletting etter Hovedavtalens opphør, med mindre annet følger av lov eller særskilt avtale.

Varighet av Databehandleravtalen: Denne Databehandleravtalen gjelder så lenge Hovedavtalen gjelder, og inntil Databehandlerens plikt til behandling av personopplysninger opphører.

Denne Databehandleravtalen er vedlegg til og inngås som del av Hovedavtalen.

VEDLEGG: SPESIFIKASJON AV BEHANDLINGEN

Spesifikasjon av behandling av personopplysninger etter Hovedavtalen, herunder behandlingsaktiviteter, behandlingens art og formål: Databehandler skal levere forvaltnings- og konverteringstjenester for behandling av rådatafiler fra 3D skanning som

overføres fra Behandlingsansvarliges eget eller leide utstyr. I forbindelse med tjenestene får Behandlingsansvarlig tilgang til Databehandlerens portal for opplasting av filer og informasjon.

Kategorier personopplysninger: Følgende kategorier personopplysninger vil bli behandlet: Følgende kategorier personopplysninger vil bli behandlet:

- Navn og kontaktopplysninger på ansatte hos Behandlingsansvarlig

- Opplysninger knyttet til adresse for kunder av Behandlingsansvarlig, herunder tegninger av bolig, gnr., bnr., snr. og adresse

- Råfiler fra skanner kan inneholde bilder av personer

Behandlingsansvarlig skal søke å sørge for at bilder ikke inneholder personopplysninger. Behandlingen omfatter ikke særlige kategorier personopplysninger etter GDPR artikkel 9. Behandlingsansvarlig er ansvarlig for å sikre at råfiler ikke inneholder slike opplysninger.

Kategorier registrerte: Følgende kategorier registrerte vil omfattes av behandlingen: Ansatte hos Behandlingsansvarlig og kunder av Behandlingsansvarlig, indirekte via adresse og eventuelt på bilder.

Varighet på behandling og lagring: Personopplysninger om brukere behandles så lenge tjenestene leveres.

Sikkerhetstiltak for behandlingen: Databehandler har implementert følgende tekniske og organisatoriske tiltak i henhold til GDPR artikkel 32:

Tekniske tiltak: To-faktor autentisering, kryptering av data under overføring (TLS 1.2 minimum) og i ro, rollebasert tilgangskontroll, automatisk utlogging ved inaktivitet, brannmurer og nettverkssegmentering i AWS VPC med private subnett, intrusion detection/prevention systemer, antivirus, sårbarhetsskanning, regelmessige krypterte sikkerhetskopier, og logging av all tilgang til personopplysninger.

Organisatoriske tiltak: Begrenset personell med tilgang (tre personer til server/plattform), taushetserklæringer, obligatorisk opplæring i personvern, biometrisk adgangskontroll til lokaler, dokumenterte prosedyrer for håndtering av personvernbrudd med varsling uten ugrunnet opphold, månedlige tilgangslogger, og definerte rutiner for dataminimering og sletting.

Detaljert beskrivelse av sikkerhetstiltak er tilgjengelig for Behandlingsansvarlig på forespørsel.

Underdatabehandlere: Leverandører/underdatabehandlere som vil behandle personopplysninger under Avtalen:

Utvikling av løsning: Tulipsoft AS (org. nr. 934 977 734. Drift av portal, lagring av opplysninger og overføring av råfiler: Amazon Web Services EMEA SARL, filial Sverige, org. nr. 516411-0669, Malmskillnadsgatan 36, 111 57, Stockholm, Sverige. Region: EU-north-1 (Stockholm).

Prosessering av råfiler til Rapporter: Bo3d India.

Råfilene vil behandles av Bo3d i India, slik at personopplysningene vil overføres til India. Dette gjøres ved bruk av Standard kontraktsbestemmelser mellom Databehandler og underleverandøren i India (Processor to Processor. Module 2) med de supplerende tiltak som følger av sikkerhetstiltakene ovenfor, som er tilgjengelig for Behandlingsansvarlig på forespørsel.