VEDLEGG X - DATABEHANDLERAVTALE ("DATABEHANDLERAVTALE")

1. ROLLER OG ANSVAR

Partene har inngått en tjenesteavtale om leveranser av QuineCore tjenesten («Tjenesteavtalen»), der Quine er leverandør og kunden er mottager av tjenestene. Denne Databehandleravtalen er et vedlegg til Tjenesteavtalen, og er underlagt bestemmelsene der. Ved motstrid skal Databehandleravtalen går foran Tjenesteavtalen.

For at **leverandøren («Quine» eller «Leverandør»)** skal kunne levere QuineCore («Tjenesten»), et samhandlingssystem for mediaproduksjoner og slik som beskrevet i Tjenesteavtalen, vil det være nødvendig å behandle personopplysninger som **databehandler**.

Kunden («Høyskolen i Innlandet» eller «Kunden») vil være **behandlingsansvarlig** når Quine behandler personopplysninger på vegne av Kunden. Kundens innledende instruksjoner og ytterligere behandlingsdetaljer er beskrevet nedenfor i avsnitt 4.

Behandlingen av personopplysninger reguleres av Lov om behandling av personopplysninger og EUs personvernforordning (EU 2016/679) ("**GDPR**") («**gjeldende personvernlovgivning**»). Begreper i denne Databehandleravtalen skal forstås i samsvar med definisjoner i GDPR art. 4.

2. GARANTI

Leverandøren garanterer å ha implementert egnede tekniske og organisatoriske tiltak som sikrer at behandlingen av personopplysninger i henhold til denne Databehandleravtale oppfyller kravene til gjeldende personvernlovgivning og sikrer vern av de registrertes rettigheter.

Kunden garanterer at den har lovlig grunnlag for å innhente og behandle personopplysningene og har implementert egnede tekniske og organisatoriske tiltak i henhold til GDPR, i sin rolle som behandlingsansvarlig.

Hvis partene ikke overholder sine forpliktelser i henhold til denne Databehandleravtale og GDPR, anses det som brudd på avtalen.

3. BEHANDLINGSSPESIFIKASJON

Leverandøren garanterer å oppfylle kravene i henhold til GDPR art. 28 ved å:

a) Kun behandle personopplysninger som instruert av kunden i databehandleravtalen eller senere skriftlig instruksjon, (art. 28 nr. 3 (a) og ar. 29).
b) Varsle kunden om leverandøren mener at en instruksjon er i strid med gjeldende personvernlovgivning (art. 28 nr. 3 andre ledd).

c) Sørge for at personer som behandler personopplysninger er underlagt taushetsplikt (art. 28 nr. 3 (b)).
d) Iverksette egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå for behandlingen av personopplysninger som er tilpasset risikoen (art. 28 nr. 3 (c), jf. Art. 32).
e) Assistere kunden i sin plikt til å svare på registrertes anmodninger om å utøve sine rettigheter, (art. 28 nr. 3 (e)).
f) Oppfylle kravet om varsel ved personvernbrudd og assistanse (art. 28 nr. 3 (f), jf. Art. 33). Behandlingsnasvarlig skal varsles uten ugrunnet opphold ved personvernbrudd hos databehandler.
g) Bistå kunden med vurdering av personvernkonsekvenser («DPIA») og eventuelt samarbeid med tilsynsmyndigheten (art. 28 nr. 3 (f)).
h) Skriftlig og umiddelbbart informere kunden om eventuelle juridiske forpliktelser som krever at leverandøren utleverer personopplysninger som leverandøren behandler på vegne av kunden, (art. 28 nr. 3 (a)).
i) Demonstrere overholdelse av forpliktelsene i henhold til GDPR art. 28 ved å gjøre tilgjengelig nødvendig informasjon, på kundens forespørsel (art. 28 nr. 3 (h)).
j) Tillate og bidra til eventuelle rimelige revisjoner gjennomført i regi av kunden (art. 28 nr. 3 (h)).
k) Slette eller returnere personopplysninger og kopier etter kundens valg slutten av tjenesten knyttet til behandlingen (art. 28 nr. 3 (g)).

Ettersom det potensielle omfanget av punktene E, F, G og J er usikkert, er disse oppgavene gjenstand for ekstra betaling i henhold til leverandørens gjeldende priser eller etter avtale.

4. INSTRUKSJONER FOR BEHANDLING

4.1 Behandlingsaktiviteter (informasjon ihht. art. 28 nr. 3 første ledd)

4.1.1 Profilinformasjon

Tjenesten mottar og bruker personopplysninger med det formål å autentisere brukeren, fastslå brukerens tilganger i Tjenesten i henhold til medlemskap i «Active Directory»-grupper i kundens tjener, vise hvem som er innlogget i brukergrensesnittet og å personalisere Tjenesten. For samhandlings- og analyseformål lagres det, i kundens database, også OID for brukerne som bruker systemet, og som endrer data forvaltet av tjenesten. Eksempler på hvordan opplysningene brukes er at det vil stå «Hei, [navn]» når appen åpnes og vise hvilke produksjoner og rapporter brukeren har tilgang til (uthentet fra gruppemedlemskap). Personopplysningene som behandles på vegne av behandlingsansvarlig, skal kun behandles for oppgitte formål.

For å gi hver enkelt bruker muligheten til å bruke Tjenesten, må Quine behandle følgende personopplysninger:

- E-postadresse
- Navn og brukernavn
- Unik bruker-ID
- Tilhørighet (arbeidsgiver)
- Gruppemedlemsskap

Brukeren eller dens arbeidsgiver kan selv velge å legge inn følgende ytterligere informasjon i sin profil, som Quine har tilgang til:

- Telefonnummer
- Kontoradresse
- Hjemmeadresse
- Stillingsbeskrivelse
- Avdeling
- Ansatt-ID
- Ansettelsestidspunkt
- Leder
- Alder

De registrerte er alle som registrerer en bruker hos Quine. For HINN omfatter dette:

- Ansatte
- Studenter
- Gjestebrukere

Quine oppbevarer ikke disse personopplysningene. Disse hentes ut fra kundens «Active Directory» ved behov, mens applikasjonen brukes.

4.1.2 Support

Med «Kundedata» menes all data, inkludert data som inneholder personopplysninger, som Kunden har lagt inn i tjenesten. Eksempler er et bilde, en film eller et dokument. Kategorier av registrerte er brukere og andre som Kunden har lagt inn opplysninger om i tjenesten, for eksempel avbildede.

Ved behov for support kan Kunden gi ansatte hos Quine tilgang til Kundens tjener. Avhengig av hva slags tilgang Kunden gir, kan Quine da få tilgang til Kundedata, inkludert personopplysninger. Kategoriene av personopplysninger som Quine får tilgang til, avhenger derfor av Kundedataen som Kunden har lastet opp i Tjenesten, og hvilke tilganger Kunden velger å gi.

Kunden gir tilgang for support på samme måte som tilgang gis til gjestebrukere. Kunden har derfor kontroll over hvilke tilganger for support som gis og når de opphører. Når Kunden gir tilgang til personopplysninger for support, anses det som en instruks om at Quine skal behandle personopplysningene som tilgjengeliggjøres. Formålet med behandlingen er å bistå i problemretting og support i løsningen for Kunden, og opplysningene skal kun behandles for dette formålet.

Quine oppbevarer ikke personopplysningene det gis tilgang til ved support.

4.1.3 Bruksdata og Diagnostikkdata

Bruksdataen er pseudonymisert når Quine mottar denne, og det er ikke mulig å identifisere personene uten å bryte Tjenesteavtalen punkt 3.

Diagnostikkdataen skal i utgangspunktet ikke inneholde personopplysninger. Det hender imidlertid at dataene inneholder informasjon om brukernavn på datamaskin, maskinens navn og IP-adresser.

Ettersom Quine selv bestemmer formålet med behandlingene og hvilke midler som benyttes, er Quine selv behandlingsansvarlig for personopplysninger som finnes i Bruksdata og Diagnostikkdata.

Quine innhenter samtykke som behandlingsgrunnlag fra den enkelte bruker for dette formålet.

4.2 Plassering av behandlingsoperasjoner

Dataene kunden legger inn i Tjenesten lagres i henhold til kundens instruksjoner til Microsoft. Quine anbefaler at lagring skjer i Microsoft sitt senter i Vest-Europa, eller Norge.

Quine benytter Microsoft sine datasentre i Vest-Europa, innenfor EØS.

4.3 Underdatabehandlere

Kunden gir leverandøren et generelt mandat til å inngå avtaler med underdatabehandlere forutsatt at avtalen er skriftlig og pålegger de samme personvernforpliktelsene som leverandøren har forpliktet seg til overfor kunden, jf. GDPR art. 28 nr. 2 og nr. 4. Leverandøren vil være ansvarlig for egne underbehandlere.

Leverandøren vil varsle kunden om eventuelle tiltenkte endringer av underbehandlere eller steder for behandling slik at kunden får muligheten til å protestere. Hvis kunden har innvendinger mot leverandørens valg av en underdatabehandler, står leverandøren fritt til å si opp avtalen. Begge parter vil i et slikt tilfelle være fri fra sine forpliktelser.

5. TILTAK FOR SIKKERHETEN TIL PERSONOPPLYSNINGENE (ART. 28 NR. 3 FØRSTE LEDD (C))

Quine skal

a) på egnet måte og med hensyn til risikoen ivareta sikkerheten til personopplysningene som behandles i henhold til kravene i GDPR art. 32, jf. art. 28 nr. 3 (c).
b) sørge for at beskyttelsesnivået som den registrerte garanteres etter gjeldende personvernlover, inkludert GDPR, ikke undergraves.

Som ledd i oppfyllelsen av art. 32, jf. Art. 28 nr. 3 (c), har Quine implementert følgende egnede tekniske og organisatoriske sikkerhetstiltak. Tiltakene er tilpasset risikoen ved behandlingen:

- Personopplysningene (access / refresh tokens) er kryptert i databasen og slettes når brukeren logger ut.
- Med unntak av «systemansvarliges epost» og diagnostikkdata, lagrer Quine kun brukerens OID-er i applikasjonens databaser. Kunden kan når som helst treke applikasjonsgodkjenningen og Quine mister dermed muligheten til å koble OID-ene til AD-profiler (samtidig som kunden mister muligheten til å bruke tjenesten). Eventuelle koblinger (med rapporteringsformål) vil i så fall alltid være lagret i kundens databaser, ikke Quines.
- For utvikling har Quine egne «application registrations» og databaser i sin AD-tenant. Applikasjonene som blir godkjent i andre tenants, og databasene brukt i produksjonen, kan administreres kun av et fåtall fortrolige, navngitte personer hos Quine.
- All data overføring skjer ved bruk av sikre koblinger (f.eks. HTTPS).
- Bruk av Azure IAM og KeyVault som gjør det lett å se hvem som har tilgang til applikasjonene hos Quine, samt eventuelle endringer i tilgangene.

6. ANSVAR

Regulering av ansvar og erstatning følger av Tjenesteavtalen.

7. DATAEKSPORT UT AV EØS

7.1 Grunnlag for overføring

Dersom behandlingen av personopplysninger fastsatt i punkt 4 *utelukkende* foregår innenfor EØS, er det ikke nødvendig med ytterligere grunnlag for dataeksport.

For enhver eksport av personopplysninger til land utenfor EØS-leverandøren (tredjeland) skal leverandøren forholde seg til standard kontraktsklausuler, tilstrekkelighetsbeslutning eller annet overføringsverktøy i GDPR kapittel V som grunnlag for overføring av data utenfor EU/EØS på en samsvarende måte.