

DATABEHANDLERAVTALE (DPA)

1. Bakgrunn og formål

Databehandleren leverer tjenesten Kvorrum, en digital plattform for organisasjonsstyring, dokumenthåndtering og kommunikasjon, til den Behandlingsansvarlige i henhold til en separat tjenesteavtale («Hovedavtalen»).

I forbindelse med leveransen av tjenesten behandler Databehandleren personopplysninger på vegne av den Behandlingsansvarlige. Denne avtalen regulerer slik behandling i samsvar med Europaparlamentets og Rådets forordning (EU) 2016/679 («GDPR» eller «personvernforordningen»), artikkel 28.

2. Definisjoner

Med «Personopplysninger» menes all informasjon som direkte eller indirekte kan knyttes til en fysisk person, og som behandles av Databehandleren innenfor rammen av tjenesten.

Med «Registrerte» menes de fysiske personene hvis personopplysninger behandles, typisk den Behandlingsansvarliges ansatte, styremedlemmer og øvrige brukere av plattformen.

Med «Underdatabehandler» menes tredjepart som Databehandleren engasjerer for å utføre bestemt behandling på vegne av den Behandlingsansvarlige.

3. Behandlingens gjenstand og formål

Databehandleren behandler personopplysninger utelukkende for å kunne levere Kvorrum-plattformen i henhold til Hovedavtalen. Behandlingen skjer etter instruks fra den Behandlingsansvarlige og på dennes vegne. Databehandleren behandler ikke personopplysningene for egne formål.

I den grad den Behandlingsansvarlige bruker tilleggstjenesten Avtaleinnsikt, behandler Databehandlerens personell også de dokumentene som den Behandlingsansvarlige sender inn for manuell gjennomgang. Slik behandling skjer etter instruks fra den Behandlingsansvarlige og utelukkende for å utføre det bestilte oppdraget.

I den grad den Behandlingsansvarlige bruker funksjonen for automatisk avlesning i modulen Avtalevarsleren, behandles de avtaledokumentene som den Behandlingsansvarlige laster opp der for automatisert avlesning med KI-støtte. Avlesningen utføres av Databehandlerens underdatabehandler Google (Vertex AI / Gemini) innenfor EU/EØS, med det formål å foreslå strukturerte opplysninger fra dokumentet. Behandlingen skjer etter instruks fra den Behandlingsansvarlige og utelukkende for å utføre det bestilte oppdraget. Avlesningen utgjør ikke automatiserte avgjørelser i henhold til GDPR artikkel 22; de foreslåtte opplysningene får virkning først når en bruker hos den Behandlingsansvarlige har gjennomgått og bekreftet dem. Utover den lagringen av dokumentet som allerede skjer i tjenesten, lagrer ikke avlesningsfunksjonen noen ytterligere kopi av dokumentets innhold; kun de foreslåtte strukturerte opplysningene, med tilhørende kildesitater, behandles videre.

I den grad den Behandlingsansvarlige bestiller import av eksisterende avtaler, laster Databehandlerens autoriserte personell opp de dokumentene som den Behandlingsansvarlige leverer, og lar dem avleses på samme måte som ved automatisk avlesning i Avtalevarsleren. Databehandlerens personell gjennomgår de foreslåtte opplysningene før avtalene legges inn i den Behandlingsansvarliges del av tjenesten. Behandlingen skjer etter instruks fra den Behandlingsansvarlige og utelukkende for å utføre det bestilte oppdraget.

Tjenesten sender e-post til brukere gjennom Databehandlerens underdatabehandler for e-postutsendelse (se punkt 5). Utsendelsene gjelder invitasjoner til tjenesten og påminnelser om avtalefrister.

Kategorier av registrerte: Ansatte, styremedlemmer, tillitsvalgte og øvrige brukere hos den Behandlingsansvarlige.

Kategorier av personopplysninger: Navn, e-postadresse, rolle og tittel, tilhørighet til rom, IP-adresse ved innlogging, tidsstempeler for innlogging, navn på betroede enheter (operativsystem og nettleser), opplysninger om hvem som har opprettet eller endret poster i tjenesten og når, innhold i supportsaker, teknisk feilinformasjon ved feil i tjenesten (bruker-ID, organisasjon, tidspunkt, feilmelding, side i tjenesten, appversjon og nettlesertype), samt innhold i de dokumentene og protokollene som den Behandlingsansvarlige lagrer i tjenesten. I gitte tilfeller kan særlige kategorier av personopplysninger i henhold til GDPR artikkel 9 forekomme i innholdet som den Behandlingsansvarlige lagrer eller sender inn. Den Behandlingsansvarlige er ansvarlig for at det foreligger behandlingsgrunnlag for behandling av slike opplysninger.

Behandlingsart: Lagring, visning, søking, eksport, sikkerhetskopiering, e-postutsendelse, logging av tekniske feil for feilsøking og support, manuell gjennomgang (ved Avtaleinnsikt og import), automatisert avlesning med KI-støtte (ved Avtalevarsleren og import) og sletting av ovennevnte opplysninger via plattformens funksjoner.

4. Databehandlerens forpliktelser

4.1 Instruksbundethet. Databehandleren behandler personopplysninger kun i samsvar med dokumenterte instruks fra den Behandlingsansvarlige, med mindre unionsretten eller svensk lovgivning krever noe annet. I så fall underretter Databehandleren den Behandlingsansvarlige før behandlingen påbegynnes, med mindre loven forbyr slik underretning.

4.2 Konfidensialitet. Databehandleren sikrer at personell som har tilgang til personopplysningene er underlagt taushetsplikt og har fått nødvendig opplæring i personvern.

4.3 Tekniske og organisatoriske sikkerhetstiltak. Databehandleren gjennomfører egnede tekniske og organisatoriske tiltak for å beskytte personopplysningene mot uautorisert tilgang, tap eller ødeleggelse, i samsvar med GDPR artikkel 32. Tiltakene omfatter blant annet:

- Kryptering av data under overføring (TLS) og i hvile (AES-256 via Google Cloud)
- Rollebasert tilgangskontroll i plattformen

- Autentisering via Firebase Authentication med totrinnsverifisering (TOTP)
- Regelmessig sikkerhetskopiering til en kryptert lagringsenhet i Databehandlerens lokaler i Sverige
- Automatisert opprydding av personopplysninger i samsvar med dokumentert lagringspolicy (se Vedlegg 2A)

4.4 Bistand til den Behandlingsansvarlige. Databehandleren bistår den Behandlingsansvarlige, i den grad det er mulig og rimelig, med å oppfylle sine plikter knyttet til:

- De registrertes rettigheter (innsyn, retting, sletting, begrensning, dataportabilitet og protest)
- Brudd på personopplysningssikkerheten i henhold til GDPR artikkel 33–34
- Personvernkonsekvensvurderinger (DPIA) i henhold til GDPR artikkel 35

4.5 Underretning ved brudd på personopplysningssikkerheten. Databehandleren underretter den Behandlingsansvarlige uten ugrunnet opphold, og senest innen 48 timer, etter å ha fått kjennskap til et brudd på personopplysningssikkerheten som gjelder den Behandlingsansvarliges data.

4.6 Sletting ved avtalens opphør. Når Hovedavtalen opphører, beholder den Behandlingsansvarlige tilgang til tjenesten i tretti (30) dager i henhold til Hovedavtalen for å kunne hente ut sine data. Deretter sletter Databehandleren alle kundedata innen tretti (30) dager fra utløpet av tilgangsperioden, med mindre Partene skriftlig har avtalt noe annet eller lovgivning krever fortsatt lagring. Kopier i sikkerhetskopier slettes i takt med at sikkerhetskopiene ryddes i henhold til Vedlegg 2A.

4.7 Revisjon. Databehandleren stiller til rådighet all informasjon som er nødvendig for at den Behandlingsansvarlige skal kunne kontrollere at forpliktelsene i henhold til denne avtalen overholdes. Den Behandlingsansvarlige, eller en revisor utpekt av denne, har rett til å gjennomføre revisjon med rimelig forhåndsvarsel (minst 30 dagers varsel) og på Partenes felles bekostning.

5. Underdatabehandlere

Databehandleren har den Behandlingsansvarliges generelle tillatelse til å engasjere underdatabehandlere. Databehandleren engasjerer for tiden følgende underdatabehandlere:

Underdatabehandler	Tjeneste	Region
Google LLC / Google Cloud Platform	Firebase Firestore (database), Firebase Authentication (innlogging), Firebase Storage (filer), Cloud Functions (serverlogikk), Firebase App Check (beskyttelse mot automatisert misbruk), Vertex AI / Gemini (KI-assistert avlesning av	EU/EØS — Firestore: europe-north2 (Stockholm), Storage: europe-north1 (Finland), Functions/Vertex AI: europe-west1 (Belgia), App Check (reCAPTCHA Enterprise): global tjeneste som kan behandle opplysninger utenfor EU/EØS, bl.a. i USA (SCC)

	opplastede avtaledokumenter)	
Plus Five Five, Inc. (Resend)	E-postutsendelse: invitasjoner til tjenesten og påminnelser om avtalefrister. Behandler mottakerens e-postadresse og meldingens innhold.	Utsendelse fra EU (Irland, eu-west-1). Resend er et amerikansk selskap og kan behandle opplysninger i USA. Overføringen skjer med støtte i EU–USA Data Privacy Framework og EU-kommisjonens standardkontraktsklausuler (SCC)

Databehandleren underretter den Behandlingsansvarlige skriftlig minst 30 dager i forveien ved tillegg eller bytte av Databehandlerens underdatabehandlere. Tillegg eller bytte av underdatabehandlernes egne underdatabehandlere meddeles den Behandlingsansvarlige uten ugrunnet opphold etter at Databehandleren har fått kjennskap til dem. Den Behandlingsansvarlige har rett til å motsette seg slikt bytte. Databehandleren er ansvarlig for underdatabehandlerens oppfyllelse av personvernforpliktelser i samme utstrekning som for sine egne.

6. Overføring til tredjeland

Databehandleren tilstreber at personopplysninger behandles innenfor EU/EØS. Lagring av den Behandlingsansvarliges data og all KI-assistert avlesning skjer innenfor EU/EØS. E-postutsendelse skjer via underdatabehandleren Resend fra dennes EU-region (Irland). Ettersom Resend er et amerikansk selskap, kan mottakerens e-postadresse og meldingens innhold også bli behandlet i USA. Slik overføring skjer med støtte i EU-kommisjonens beslutning om tilstrekkelig beskyttelsesnivå for EU–USA Data Privacy Framework samt EU-kommisjonens standardkontraktsklausuler (SCC), som inngår i Databehandlerens databehandleravtale med Resend. Firebase App Check (Google reCAPTCHA Enterprise), som beskytter tjenesten mot automatisert misbruk, er en global tjeneste uten forpliktelse om lagringssted. Tekniske opplysninger om brukerens nettleser og enhet kan derfor bli behandlet av Google utenfor EU/EØS, blant annet i USA. Slik overføring skjer med støtte i EU-kommisjonens standardkontraktsklausuler (SCC) etter Google Clouds Data Processing Addendum. I den grad andre underdatabehandlere håndterer data i land utenfor EU/EØS, skjer dette med støtte i standardkontraktsklausuler eller annet gyldig overføringsgrunnlag i henhold til GDPR kapittel V.

7. Ansvar og begrensning

Hver Part er ansvarlig for skader som oppstår som følge av at vedkommende bryter GDPR eller denne avtalen. Databehandlerens samlede ansvar overfor den Behandlingsansvarlige under denne avtalen er begrenset til et beløp tilsvarende tolv (12) måneders avgifter under Hovedavtalen, med mindre det foreligger grov uaktsomhet eller forsett.

8. Avtaleperiode

Denne avtalen gjelder for samme periode som Hovedavtalen og opphører automatisk når Hovedavtalen opphører, med mindre annet følger av ufravikelig lovgivning.

9. Gjeldende rett og tvister

Denne avtalen reguleres av svensk rett. Tvister som oppstår i forbindelse med avtalen skal først søkes løst gjennom forhandlinger. Dersom forhandlinger ikke fører til en løsning innen 60 dager, skal tvisten avgjøres av alminnelig domstol med Helsingborg tingrett som første instans.

OPPBEVARINGSTIDER

Personopplysninger som behandles i tjenesten slettes som følger:

Kategori	Lagringstid	Tiltak
Aktive medlemmer	I avtaleperioden samt 30 dagers tilgangperiode deretter	Slettes innen 30 dager etter utløpet av tilgangsperioden
Arkiverte medlemmer	1 år fra arkiveringsdato	Opplysningene slettes automatisk
IP-adresse ved innlogging og betrodd enheter for arkiverte medlemmer	Umiddelbart ved arkivering	Feltene nullstilles automatisk
IP-adresse ved innlogging for aktive medlemmer	90 dager etter siste innlogging	Feltet nullstilles automatisk
Utløpte og brukte invitasjoner	90 dager etter at invitasjonen ble opprettet, når den er brukt, arkivert eller utløpt	Opplysningene slettes automatisk
Poster i papirkurven (dokumenter, avtaler, lisenser, møter, avstemninger)	30 dager etter at posten ble flyttet til papirkurven	Posten og tilhørende filer slettes automatisk
Lukkede supportsaker	2 år etter siste endring	Saken slettes automatisk
Systemlogg (revisjonslogg)	2 år	Loggposten slettes automatisk
Feillogger (tekniske feil i tjenesten)	90 dager fra feilen oppstod	Loggposten slettes automatisk
Sikkerhetskopier	Alle kopier fra de siste 30 dagene; deretter én kopi per måned i 12 måneder	Eldre kopier slettes automatisk

Opprydding skjer via automatiserte, planlagte funksjoner som kjøres daglig. Hver kjøring logges for sporbarhet.