

DATABEHANDLERAVTALE

i henhold til personvernforordningen (GDPR) artikkel 28

1. Innledning

Denne databehandleravtalen ("DPA") er inngått mellom:

Behandlingsansvarlig (Kunden)	Databehandler
Som angitt i Avtalens forside	Rehub AS Org.nr. 934 100 832

DPA er en del av avtalen om bruk av Rehubs tjenester ("Tjenesteavtalen"), bestående av Forsiden og Standard Vilkår. For å oppfylle Tjenesteavtalen behandler Databehandler personopplysninger på vegne av Behandlingsansvarlig. Ved motstrid har DPA forrang for forhold spesifikt knyttet til behandling av personopplysninger.

2. Definisjoner

"Personvernlovgivning" – GDPR (forordning 2016/679) og gjeldende nasjonal personvernlovgivning.

"Personopplysninger" – enhver opplysning om en identifisert eller identifiserbar fysisk person ("Registrerte").

"Underdatabehandler" – underleverandør Databehandler benytter til å behandle Personopplysninger under DPA.

For øvrige begreper gjelder GDPR artikkel 4.

3. Omfang av behandlingen

Databehandler behandler Personopplysninger kun på vegne av Behandlingsansvarlig og i henhold til Tjenesteavtalen, denne DPA og Behandlingsansvarliges dokumenterte instruks. Databehandler skal omgående underrette Behandlingsansvarlig dersom en instruks anses å være i strid med Personvernlovgivningen.

Nærmere opplysninger om behandlingen følger av seksjonen "Beskrivelse av behandlingen" nedenfor.

4. Behandlingsansvarliges plikter

Behandlingsansvarlig er ansvarlig for at det foreligger gyldig rettslig grunnlag for behandlingen, at de Registrerte har mottatt nødvendig informasjon, og at instruks gitt til Databehandler er i samsvar med Personvernlovgivningen.

5. Taushetsplikt

Databehandler skal sikre at personell og Underdatabehandlere med tilgang til Personopplysninger er underlagt taushetsplikt. Taushetsplikten gjelder også etter DPAs opphør, slik det er standard etter GDPR artikkel 28(3) (b).

6. De registrertes rettigheter

Databehandler skal, i den grad det er mulig, bistå Behandlingsansvarlig med å besvare anmodninger fra Registrerte om innsyn, korrigering, sletting, begrensning og dataportabilitet. Anmodninger som mottas direkte hos Databehandler videresendes uten ugrunnet opphold.

7. Annen bistand

Databehandler skal, hensyntatt behandlingens art og tilgjengelig informasjon, bistå Behandlingsansvarlig med vurderinger av personvernkonsekvenser (DPIA) og forhåndsdrøftelser med tilsynsmyndighet.

8. Sikkerhet

Databehandler iverksetter egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå tilpasset risikoen, jf. GDPR artikkel 32. Sikkerhetstiltakene er nærmere beskrevet i seksjonen "Sikkerhet" nedenfor.

9. Melding om sikkerhetsbrudd

Databehandler skal varsle Behandlingsansvarlig uten ugrunnet opphold og senest innen 72 timer etter å ha fått kjennskap til brudd på personopplysningssikkerheten. Varselet skal minimum beskrive (i) arten av bruddet, kategoriene av og omtrentlig antall Registrerte og Personopplysninger som er berørt, (ii) sannsynlige konsekvenser, og (iii) tiltak som er iverksatt eller foreslås. Behandlingsansvarlig melder bruddet til relevant tilsynsmyndighet.

10. Overføring til tredjeland

Behandlingen omfatter overføring av Personopplysninger til USA (se seksjonen "Underdatabehandlere" nedenfor). Overføringene skjer på grunnlag av EUs standardvilkår (SCC), EU-US Data Privacy Framework der dette gjelder, og/eller andre gyldige overføringsgrunnlag. Endringer i bruk av tredjelandsoverføringer varsles i henhold til punkt 11.

11. Underdatabehandlere

Behandlingsansvarlig godkjenner Underdatabehandlerne oppført i seksjonen "Underdatabehandlere" nedenfor, og forhåndsgodkjenner at Databehandler kan ta i bruk nye Underdatabehandlere innenfor de kategoriene som er angitt der. Databehandler skal sikre at forpliktelser tilsvarende denne DPA pålegges Underdatabehandler gjennom skriftlig avtale.

Databehandler varsler Behandlingsansvarlig senest 30 dager før en ny Underdatabehandler tas i bruk. Behandlingsansvarlig kan komme med rimelige innvendinger innen 14 dager etter varsel. Dersom innvendingen ikke kan avhjelpes, kan Behandlingsansvarlig si opp Tjenesteavtalen med virkning fra den dagen endringen iverksettes.

12. Revisjoner

Databehandler skal på forespørsel gi Behandlingsansvarlig informasjon som er nødvendig for å dokumentere etterlevelse av DPA. For Tjenestens standardiserte deler oppfylles dette i utgangspunktet ved at Databehandler fremlegger relevante sertifiseringer eller tredjepartsrapporter (f.eks. SOC 2 eller ISO 27001) når slike foreligger, eventuelt tilsvarende rapporter fra Underdatabehandlere.

Behandlingsansvarlig har rett til å gjennomføre fysisk revisjon én gang per år med minst to ukers skriftlig varsel. Behandlingsansvarlig dekker egne og Databehandlers rimelige kostnader knyttet til slik revisjon. Disse begrensningene gjelder ikke ved begrunnet mistanke om brudd på DPA eller Personvernlovgivningen.

13. Varighet og opphør

DPA gjelder så lenge Databehandler behandler Personopplysninger for Behandlingsansvarlig. På skriftlig anmodning fra Behandlingsansvarlig skal Databehandler innen rimelig tid slette eller returnere Personopplysningene, med mindre fortsatt lagring er pålagt ved lov. Aggregerte og anonymiserte data kan beholdes av Databehandler i samsvar med Tjenesteavtalen.

14. Ansvarsbegrensning

Databehandlerens samlede ansvar etter DPA er begrenset til samme beløp som er angitt i Tjenesteavtalens ansvarsbegrensning (vederlag fakturert i de siste 12 månedene). Begrensningen gjelder ikke ved forsett eller grov uaktsomhet.

15. Lovvalg og verneting

DPA er underlagt norsk rett med Oslo tingrett som verneting.

16. Varsler og endringer

Varsler etter DPA sendes til kontaktpunktene angitt nedenfor. Endringer av DPA krever skriftlig avtale mellom partene.

17. Kontaktinformasjon

Hos Behandlingsansvarlig	Hos Databehandler (Rehub AS)
Navn: [•] Stilling: [•] Telefon: [•] E-post: [•]	Navn: Sunniva Baarnes Stilling: Kontaktperson Telefon: [•] E-post: sunniva@rehub.no

* * *

Beskrivelse av behandlingen

Formål og art

- Levere og drifte Rehubs plattform for kartlegging, dokumentasjon, deling og publisering av materialer ("Listings").
- Brukerautentisering, tilgangsstyring, support og videreutvikling av Tjenesten.
- Formidle kontakt mellom brukere på Rehubs markeds plass når Listings publiseres eksternt.

Typer personopplysninger

- Navn, e-post, telefon, stilling og arbeidsplass for brukere.
- Brukerinteraksjon i plattformen (innlogging, søk, publiseringer, henvendelser).
- Eventuelle kontaktpersoner oppført av Kunden i Listings.

Kategorier av Registrerte

- Kundens brukere (ansatte, innleide og autoriserte samarbeidspartnere).
- Kundens kontaktpersoner og fakturareferanser.
- Brukere hos andre organisasjoner som kontakter Kunden via markeds plassen.

Varighet

Behandlingen pågår så lenge Tjenesteavtalen løper. Etterfølgende håndtering av Kundedata reguleres av punkt 13 i denne DPA.

Sikkerhet

Tjenesten er bygget på følgende sertifiserte plattformer som leverer underliggende tekniske sikkerhetstiltak (kryptering i transitt og i hvile, tilgangskontroll, autentisering inkludert 2FA og SSO, sikkerhetslogging, sikkerhetskopier mv.):

- Softr – frontend, brukerautentisering og tilgangsstyring. SOC 2 Type II-sertifisert.
- Airtable – database og lagring. SOC 2 Type II, ISO 27001 og ISO 27701-sertifisert.

Rehub støtter seg på disse sertifiseringene som dokumentasjon på sikkerhetsnivået i underliggende infrastruktur. Oppdatert dokumentasjon: softr.io/security og airtable.com/company/trust-and-security.

Rehubs konfigurasjon og driftspraksis

- 2FA aktivert for administrative tilganger og tilbudt for brukere av Tjenesten.
- Rollebasert tilgangskontroll og prinsippet om minste privilegium.
- Kryptert overføring av Personopplysninger (TLS).
- Skriftlige avtaler med alle Underdatabehandlere og løpende oppfølging av disse.
- Taushetsplikt for ansatte og innleide samarbeidspartnere.
- Opplæring av relevant personell i informasjonssikkerhet og personvern.

Underdatabehandlere

Tjenesten er bygget på følgende godkjente Underdatabehandlere. Oppdatert oversikt utleveres på forespørsel.

1. Softr Inc. – Applikasjonsplattform

Foretak	Softr Inc.
Land	USA
Behandling	Drift av frontend-applikasjon, brukerautentisering og tilgangsstyring.
Sertifiseringer	SOC 2 Type II, GDPR-kompatibel.
Overføringsgrunnlag	EUs standardvilkår (SCC) i henhold til Softrs Data Processing Agreement (softr.io/dpa-v1).

2. Airtable, Inc. – Database og lagring

Foretak	Airtable, Inc.
Land	USA (AWS US-East-1)
Behandling	Lagring og prosessering av Kundedata, herunder Listings, brukerdata og metadata.
Sertifiseringer	SOC 2 Type II, ISO 27001, ISO 27701.
Overføringsgrunnlag	EUs standardvilkår (SCC) i henhold til Airtables DPA (airtable.com/company/dpa). Oppdatert oversikt over Airtables underdatabehandlere: airtable.com/company/subprocessors.

Avgrensning mot markedsføringsverktøy

Markedsføringsverktøy, annonsering og webanalyse som benyttes på rehub.no eller andre eksterne flater (f.eks. Google Analytics, Google Ads, Microsoft Ads, Meta Ads, LinkedIn Ads og tilsvarende), og som ikke behandler personopplysninger om Kundens brukere innenfor pålogget Tjeneste, er ikke å anse som Underdatabehandlere under denne DPA. Slike verktøy reguleres av Rehubs personvernerklæring tilgjengelig på rehub.no/personvern.

Forhåndsgodkjente kategorier

Behandlingsansvarlig forhåndsgodkjenner at Databehandler kan ta i bruk nye Underdatabehandlere innenfor følgende kategorier, forutsatt at konkrete tjenester varsles i henhold til DPA punkt 11:

- Produktanalyse og brukerinnsikt (f.eks. Plausible, PostHog, Mixpanel).
- E-post, varsling og kundekommunikasjon (f.eks. SendGrid, Postmark, Mailgun).
- Kundesupport og dialog (f.eks. Intercom, HubSpot, Crisp).
- Drifts- og integrasjonsverktøy som behandler Kundedata (f.eks. Zapier, Make, n8n).

Databehandler kan ikke benytte Underdatabehandlerne til annen behandling enn beskrevet ovenfor. Endringer varsles etter DPA punkt 11.

* * *

Denne DPA er en del av Tjenesteavtalen og signeres sammen med denne.