

Databehandleraftale

Mellem

Ratios ApS
CVR nr. 43416731
Gydevang 39-41
3450 Allerød

og

Kunden
(Dataansvarlig)

Kunden og Ratios har indgået en aftale om levering af Ratios Applikation. Denne databehandleraftale (herefter benævnt "Databehandleraftale" eller "DPA") er en integreret del af aftalen og fastsætter vilkårene for behandling af personoplysninger. Aftalen indeholder følgende bilag:

- Bilag A: Indeholder oplysninger om behandlingen af personoplysninger, herunder formål og karakter af behandlingen, typen af personoplysninger, kategorierne af registrerede personer samt behandlingens varighed.
- Bilag B: Indeholder den Dataansvarliges betingelser for Databehandlerens brug af Underdatabehandlere samt en liste over de Underdatabehandlere, som den Dataansvarlige har godkendt.
- Bilag C: Indeholder den Dataansvarliges instruks vedrørende behandling af personoplysninger, de minimumssikkerhedsforanstaltninger, som Ratios skal implementere, samt retningslinjer for revision af Ratios og eventuelle Underdatabehandlere.

1. Anvendelse og omfang

1.1 Instruktion. Ratios vil som Databehandler behandle Kundens data, herunder personoplysninger, på vegne af Kunden med det formål at levere Applikationen. Dataen vil kun blive behandlet i overensstemmelse med Kundens instruktion.

1.2 Behandlingsgrundlag. Hver part skal sikre, at den behandling, de udfører, har et retligt grundlag og overholder databeskyttelsesforordningen (herefter benævnt "GDPR") samt relevante nationale databeskyttelsesregler.

1.3 Fortrolighed. Ratios skal behandle Kundens data som fortrolige oplysninger. Ratios skal sikre, at alle medarbejdere er bundet af en fortrolighedsaftale, der er gyldig ud over ansættelsens varighed.

1.4 Sletning. Ratios vil behandle Kundens data, herunder personoplysninger, i aftalens varighed. Ratios vil slette al Kundens data, herunder personoplysninger, tres (60) dage efter kontraktens udløb. Ingen behandling eller konvertering af data foretages af Ratios efter opsigelsen.

2. Sikker behandling

2.1 Sikkerhedsforanstaltninger. Ratios har implementeret sikkerhedsforanstaltninger, der er tilstrækkelige til at beskytte integriteten og fortroligheden af Kundens data. Ratios skal også sikre tilgængeligheden af dataene i Applikationen.

2.2 Sikkerhedshændelse. Ratios skal uden unødigt forsinkelse og, hvor det er muligt, senest seksogtredive (36) timer efter at have fået kendskab til en sikkerhedshændelse underrette Kunden. En sikkerhedshændelse defineres som ethvert sikkerhedsbrud, der fører til utilsigtet eller ulovlig destruktion, tab, ændring, uautoriseret videregivelse af eller adgang til kundens data, som behandles af Ratios og/eller dets Underdatabehandlere.

2.3 Underretning. Ratios skal bistå Kunden med at opfylde Kundens forpligtelse til at underrette den relevante Databeskyttelsesmyndighed inden for tooghalvfjerds (72) timer.

3. Databehandlerens anvendelse af Underdatabehandlere

3.1 Generel godkendelse. Ratios har Kundens generelle og udtrykkelige godkendelse til at anvende Underdatabehandlere. Ratios skal have en skriftlig aftale med hver Underdatabehandler, der sikrer, at Underdatabehandleren overholder bestemmelserne i EU-lovgivningen og de bestemmelser, der er beskrevet i denne Databehandleraftale. Ratios forbliver ansvarlig over for Kunden, hvis en Underdatabehandler ikke opfylder sine databeskyttelsesforpligtelser i forbindelse med behandlingsaktiviteterne under aftalen.

3.2 Underdatabehandlere. Listen over godkendte Underdatabehandlere fremgår af Bilag B. Ratios vil skriftligt underrette Kunden om enhver påtænkt ændring vedrørende tilføjelse eller udskiftning af underdatabehandlere mindst tredive (30) dage i forvejen.

3.3 Indsigelse mod nye Underdatabehandlere. I løbet af den tredive (30) dages varslingsperiode kan Kunden skriftligt gøre indsigelse mod introduktionen af en ny Underdatabehandler. Såfremt Kundens indsigelse er rimelig og begrundet, kan Aftalen ekstraordinært opsiges.

3.4 Tredjelande. Enhver overførsel af personoplysninger til tredjelande må kun foretages af Ratios på baggrund af dokumenterede instruktioner fra Kunden og skal altid ske i overensstemmelse med kapitel V i GDPR.

4. Databehandlerens forpligtelse til at bistå den Dataansvarlige

4.1 Den registreredes rettigheder. Ratios vil, så vidt muligt, bistå Kunden med at opfylde sine forpligtelser til at imødekomme anmodninger vedrørende den registreredes rettigheder.

4.2 Samarbejdsforpligtelser. Efter kundens anmodning vil Ratios yde rimelig bistand til Kunden med at opfylde sine forpligtelser i henhold til GDPR, forudsat at kunden ikke selvstændigt kan opfylde sådanne forpligtelser ved hjælp af den dokumentation, som allerede er stillet til rådighed af Ratios.

5. Sletning

5.1 I løbet af abonnementsperioden. I løbet af abonnementsperioden har Kunden adgang til at rette, indlæse, oprette og/eller slette data via de funktioner, der er tilgængelige i Applikationen.

5.2 Ved udløb af aftalen. Ratios vil slette al Kundens data, som Ratios opbevarer i rollen som Databehandler, herunder personoplysninger, tres (60) dage efter aftalens udløb.

6. Revision

6.1 Revision. Ratios stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af GDPR og denne Databehandleraftale, til rådighed for Kunden. Ratios giver desuden mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af Kunden.

6.2 Procedure for revision. Procedurer for revisioner, herunder inspektioner, er nærmere angivet i Bilag C.

Bilag A Oplysninger om behandlingen

A.1. Formålet med Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige

Ratios behandler personoplysninger på vegne af Kunden med det formål at levere de ydelser, der er aftalt mellem parterne.

A.2 Kategorier af Datasubjekter

- Kundens brugere i Applikationen
- Kundens klienter i Applikationen

A.3 Kategorier af data som behandles

- Personoplysninger (ikke-følsomme personoplysninger)
- Applikationen kræver ikke behandling af følsomme personoplysninger, men Kunden kan vælge at behandle sådanne oplysninger.

A.4 Type af data som behandles

- For Kundens brugere: Navn, jobtitel, e-mailadresse, telefonnummer, brugerprofilbillede
- For Kundens klienter: Navn, jobtitel, e-mailadresse, telefonnummer og andre oplysninger, som Kunden vælger at notere og behandle.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ratios har Kundens generelle godkendelse til at gøre brug af Underdatabehandlere. Ratios har ved Databehandleraftalens ikrafttræden specifikt godkendt anvendelsen af disse underdatabehandlere.

Underdatabehandlere	Land	Ydelse	Datalokation
Supabase Inc.	USA	Databasehosting - Ratios 2.0	EU

Nye Underdatabehandlere kan tilføjes i overensstemmelse med Databehandleraftalens pkt. 3.

Bilag C Instruks vedrørende behandling af personoplysninger

Ratios opererer et ISMS (informationssikkerhedssystem) for at sikre fortroligheden og integriteten af de behandlede data samt for at garantere tilgængeligheden og robustheden af Applikationen. Ratios fastlægger de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger for at opnå det nødvendige niveau af informationssikkerhed. Under alle omstændigheder, og som minimum, sikrer Ratios, at følgende sikkerhedsforanstaltninger er implementeret:

C.1 Governance og risikostyring

Ratios' informationssikkerhedspolitik er godkendt af ledelsen og bliver gennemgået mindst én gang om året. Ratios har også etableret en risikostyringsprocedure til at identificere, vurdere og håndtere relevante risici. Både interne og eksterne trusler og sårbarheder overvejes i forhold til de data, der behandles og opbevares i Applikationen. Ratios har interne kommunikations- og rapporteringskanaler, der sikrer, at direktionen og bestyrelsen kan træffe informerede beslutninger.

C.2 Adgangsrettigheder og fortrolighed

Ratios har implementeret en formel adgangsstyringspolitik, der sikrer, at adgangsrettigheder til Applikationen såvel som interne systemer følger principperne om "least privilege" og "need to know". Ratios har integreret adgangsstyring i virksomhedens onboarding- og offboardingprocesser og anvender tofaktorgodkendelse samt single sign-on for yderligere at beskytte adgangen til organisationens systemer.

Adgangen til Ratios produktionsmiljøer er yderligere begrænset gennem tekniske foranstaltninger såsom tofaktorgodkendelse, rollebaseret adgang og unikke brugerkonti. Adgangsrettigheder gennemgås mindst én gang årligt. Ratios bærbare computere er beskyttet med adgangskoder, skærmlås-politik og aktiveret harddiskkryptering.

C.3. Awareness-træning

Alle nye medarbejdere hos Ratios skal gennemføre et træningsforløb om compliance-bevidsthed, der dækker informationssikkerhed og privacy. Derudover skal alle medarbejdere årligt gennemføre et opdateret træningsforløb om disse emner.

C.4 Forretningskontinuitet og nødgendannelse

Ratios tager daglige sikkerhedskopier af lagring og databaser som en del af sin plan for forretningskontinuitet.

C.5 Kryptografi

Kundens data, der behandles i Applikationen, krypteres under overførsel ved hjælp af TLS 1.2 eller højere samt ved lagring. Ratios sikrer, at medarbejderes bærbare computere har aktiveret harddiskkryptering.

C.6.Leverandørstyring

Ratios har en leverandørstyringspolitik, der sikrer, at kun pålidelige leverandører anvendes til at støtte Ratios organisation og Applikation. Ratios udfører en informationssikkerheds- og privacygennemgang af alle leverandører. Mindst én gang årligt anmoder Ratios om og gennemgår relevant compliance-dokumentation fra Underdatabehandlerne.

C.7 Sårbarhedsstyring

Ratios overvåger sårbarheder på teknisk, juridisk og compliance-niveau. Ratios juridiske og compliance-team vurderer løbende landskabet for databeskyttelse og informationssikkerhed for at sikre løbende organisatorisk compliance, herunder overholdelse af regler som GDPR. Ratios produkt- og ingeniørteam overvåger tekniske sårbarheder for at sikre, at relevante sårbarheder håndteres rettidigt og passende.