Databehandleraftale

Gældende fra 1. november 2026

1. Parter og baggrund

Aftalen gælder mellem dig som kunde hos Striive («den dataansvarlige») og Striive v/ Mathias Quist Michaelsen, Midgårdsvej 10, 8800 Viborg, Danmark, CVR-nr. 46826159, som driver Striive («databehandleren»).

Aftalen er et bilag til og en del af Striives handelsbetingelser og indgås, når du accepterer dem. Den gælder, så længe databehandleren behandler personoplysninger på vegne af den dataansvarlige, og fortsætter, indtil oplysningerne er slettet efter punkt 11.

Aftalen opfylder databeskyttelsesforordningens artikel 28, stk. 3. Begreber har samme betydning som i forordningen. Ved uoverensstemmelse mellem aftalen og handelsbetingelserne går aftalen forud for så vidt angår behandling af personoplysninger.

2. Behandling efter instruks

Databehandleren behandler kun personoplysninger efter dokumenteret instruks fra den dataansvarlige. Instruksen er givet i denne aftale med bilag 1, i handelsbetingelserne og gennem de valg og handlinger, den dataansvarlige og dennes team foretager i Striive, for eksempel når en formular oprettes, et indhold udgives, eller AI-assistenten bedes udføre en opgave. Yderligere instrukser gives skriftligt.

Behandling, som EU-retten eller dansk ret pålægger databehandleren, må ske uden instruks. Databehandleren underretter da den dataansvarlige om kravet før behandlingen, medmindre loven forbyder det af hensyn til vigtige samfundsinteresser.

Databehandleren underretter straks den dataansvarlige, hvis en instruks efter databehandlerens opfattelse er i strid med databeskyttelsesreglerne.

Databehandleren bruger ikke oplysningerne til egne formål. Det, databehandleren selv behandler som dataansvarlig, for eksempel oplysninger om kundens konto og betaling og referencebiblioteket, er beskrevet i Striives privatlivspolitik og er ikke omfattet af denne aftale.

3. Fortrolighed

Kun personer, der har brug for det for at levere Striive, får adgang til personoplysningerne. De har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt. Adgangen gennemgås og fratages, når behovet ophører.

4. Sikkerhed

Databehandleren træffer de tekniske og organisatoriske foranstaltninger, der kræves efter forordningens artikel 32, under hensyn til det aktuelle tekniske niveau, omkostningerne og behandlingens karakter, omfang, sammenhæng og formål samt risiciene for de registrerede. Foranstaltningerne er beskrevet i bilag 3.

Databehandleren kan ændre foranstaltningerne, så længe sikkerhedsniveauet ikke forringes.

Den dataansvarlige er ansvarlig for de valg, den dataansvarlige selv træffer i Striive, herunder hvem der får adgang til hjemmesiden, om tofaktorlogin bruges, og hvilke oplysninger der indsamles.

5. Underdatabehandlere

Den dataansvarlige giver databehandleren en generel godkendelse til at bruge underdatabehandlere. De underdatabehandlere, der bruges, når aftalen indgås, står i bilag 2 og på striiveai.com/juridisk/underdatabehandlere.

Databehandleren underretter den dataansvarlige på e-mail mindst 30 dage, før en underdatabehandler tilføjes eller udskiftes. Den dataansvarlige kan inden for fristen gøre saglig indsigelse. Kan parterne ikke finde en løsning, kan den dataansvarlige opsige abonnementet, før ændringen træder i kraft, og får den forudbetalte del af perioden tilbage forholdsmæssigt.

Databehandleren pålægger hver underdatabehandler de samme databeskyttelsesforpligtelser som i denne aftale gennem en skriftlig aftale, herunder tilstrækkelige garantier for passende sikkerhed. Databehandleren er over for den dataansvarlige fuldt ansvarlig for underdatabehandlerens opfyldelse af sine forpligtelser.

6. Overførsel til tredjelande

Personoplysningerne opbevares i EU (Google Cloud, Stockholm). Overførsel til lande uden for EU/EØS sker kun til de underdatabehandlere og formål, der står i bilag 2, og kun med et gyldigt overførselsgrundlag efter forordningens kapitel V: en tilstrækkelighedsafgørelse, herunder EU-U.S. Data Privacy Framework for certificerede modtagere, eller EU-Kommissionens standardkontraktbestemmelser.

Med denne aftale instruerer den dataansvarlige databehandleren i at foretage disse overførsler.

7. Bistand med de registreredes rettigheder

Databehandleren bistår den dataansvarlige med at opfylde anmodninger fra registrerede om indsigt, berigtigelse, sletning, begrænsning, dataportabilitet og indsigelse. Den dataansvarlige kan selv se, rette og slette formularsvar og andet indhold i editoren og hente samtykkeregistreringer. Hvad den dataansvarlige ikke selv kan gøre i editoren, udfører databehandleren på skriftlig anmodning uden unødig forsinkelse.

Modtager databehandleren en anmodning direkte fra en registreret, videresender databehandleren den til den dataansvarlige og besvarer den ikke selv uden instruks.

8. Brud på persondatasikkerheden

Databehandleren underretter den dataansvarlige uden unødig forsinkelse og senest 48 timer efter at være blevet opmærksom på et brud på persondatasikkerheden, der vedrører den dataansvarliges oplysninger, så den dataansvarlige kan overholde sin frist på 72 timer over for Datatilsynet.

Underretningen beskriver, så vidt muligt: bruddets karakter, herunder kategorier og omtrentligt antal registrerede og registreringer; sandsynlige konsekvenser; de foranstaltninger, der er truffet eller foreslås for at håndtere bruddet og begrænse skadevirkningerne; og en kontaktperson. Oplysninger, der ikke kendes straks, gives løbende.

Databehandleren fører en log over alle brud, også dem, der ikke skal anmeldes.

9. Anden bistand

Databehandleren bistår, under hensyn til behandlingens karakter og de oplysninger, databehandleren har, den dataansvarlige med at overholde forpligtelserne efter forordningens artikel 32-36, herunder ved konsekvensanalyser og forudgående høring af Datatilsynet.

Bistand, der går ud over det, Striive stiller til rådighed i editoren eller i denne aftale, og som ikke skyldes databehandlerens egne forhold, kan faktureres efter medgået tid til en rimelig timepris, som aftales på forhånd.

10. Dokumentation og revision

Databehandleren stiller alle oplysninger til rådighed, der er nødvendige for at påvise, at artikel 28 og denne aftale overholdes. Det sker som udgangspunkt ved, at databehandleren på anmodning, højst én gang om året, besvarer den dataansvarliges skriftlige spørgsmål om behandlingssikkerheden.

Den dataansvarlige eller en uafhængig revisor med tavshedspligt kan desuden foretage en revision, herunder en inspektion, med mindst 30 dages varsel, hvis det er nødvendigt efter et brud, en henvendelse fra en myndighed eller begrundet tvivl om overholdelsen. Den dataansvarlige afholder sine egne omkostninger. Revisionen må ikke give adgang til andre kunders oplysninger eller bringe sikkerheden i fare. Revision hos underdatabehandlere sker gennem deres egne revisionserklæringer og certificeringer.

Datatilsynet og andre myndigheder har altid adgang efter lovgivningen.

11. Sletning og tilbagelevering ved ophør

Når abonnementet ophører, gemmes hjemmesiden i 30 dage, eller i 90 dage, hvis den er låst på grund af manglende betaling, så den dataansvarlige kan genoptage tjenesten. Inden sletningen kan den dataansvarlige hente samtykkeregistreringer i editoren og bede om en kopi af hjemmesidens indhold, medier og formularsvar i et almindeligt, maskinlæsbart format.

Herefter sletter databehandleren alle personoplysninger, der behandles for den dataansvarlige, herunder indhold, medier, formularsvar, samtykkeregistreringer, AI-samtaler og overholdelsesgennemgange. Sikkerhedskopier slettes automatisk senest 30 dage efter. Den dataansvarlige får besked på e-mail 7 dage før sletningen.

Det gælder ikke oplysninger, som EU-retten eller dansk ret kræver opbevaret, for eksempel regnskabsbilag. Dem opbevarer databehandleren kun så længe og til det formål, loven kræver.

12. Ansvar og ikrafttræden

Parternes ansvar efter aftalen følger handelsbetingelsernes punkt 19 og forordningens artikel 82. Begrænsningerne i handelsbetingelserne gælder ikke for den registreredes krav.

Ændringer af aftalen varsles som ændringer af handelsbetingelserne. Ændringer, som er nødvendige på grund af ny lovgivning eller en afgørelse fra en myndighed, kan gennemføres med kortere varsel.

Bilag 1. Beskrivelse af behandlingen

Formål: at levere Striive til den dataansvarlige, så den dataansvarlige kan bygge, redigere, hoste og udgive sin hjemmeside, modtage formularsvar, registrere besøgendes samtykker, bruge AI-assistenten og overholdelsesgennemgangen.

Behandlingens karakter: opbevaring, hosting, visning, transmission, sikkerhedskopiering, behandling med AI efter den dataansvarliges anmodning, sletning.

Varighed: så længe abonnementet løber, og indtil sletningen efter punkt 11.

Kategorier af registrerede	Kategorier af personoplysninger
Personer, der sender formularer på hjemmesiden	De felter, den dataansvarlige har valgt, typisk navn, e-mail, telefon og besked. Striive gemmer ikke afsenderens IP-adresse.
Besøgende, der svarer på cookiebanneret	Et tilfældigt samtykke-id, tidspunkt, de valgte kategorier, de tilbudte kategorier, sidens adresse og bannertekstens version. Ingen IP-adresse eller browseroplysninger. Slettes 3 år efter svaret.
Medlemmer af den dataansvarliges team	Navn, e-mail og rolle som de fremgår af hjemmesidens indhold og indstillinger (deres konti behandles af Striive som dataansvarlig).
Personer, der omtales eller vises på hjemmesiden	Navne, billeder, kontaktoplysninger og andet, den dataansvarlige selv lægger på hjemmesiden.
Personer, der optræder i AI-samtaler	Det, den dataansvarlige og teamet skriver til AI-assistenten, og det indhold, assistenten arbejder med.
Personer, der optræder i overholdelsesgennemgangen	Den dataansvarliges svar om sin virksomhed og resultaterne af gennemgangen. Gennemgangen læser de udgivne sider som en anonym besøgende og læser ikke besøgendes oplysninger.

Følsomme oplysninger efter artikel 9 og oplysninger om strafbare forhold behandles kun, hvis den dataansvarlige selv indsamler dem. Det må den dataansvarlige kun, hvis der er et lovligt grundlag, og den dataansvarlige skal da selv vurdere, om Striives foranstaltninger er tilstrækkelige.

Bilag 2. Underdatabehandlere

Ved aftalens indgåelse bruger databehandleren disse underdatabehandlere til den dataansvarliges oplysninger:

Underdatabehandler	Opgave	Placering og overførselsgrundlag
Google Cloud EMEA Ltd. (Google Cloud)	Servere, database, lagring af medier, sikkerhedskopier og driftslogs	EU, region europe-north2 (Stockholm)
Resend, Inc.	Afsendelse af e-mails, herunder besked om nye formularsvar (uden formularens indhold)	Afsendelse i EU; kontodata, metadata og logs i USA. Standardkontraktbestemmelser
OpenRouter, Inc.	Videreformidling af AI-forespørgsler til AI-leverandøren	USA. Standardkontraktbestemmelser
Anthropic, Google og OpenAI	AI-modeller, der behandler forespørgsler fra AI-assistenten	USA. EU-U.S. Data Privacy Framework eller standardkontraktbestemmelser
Unsplash Inc.	Levering af stockbilleder, som den dataansvarlige har valgt til hjemmesiden; den besøgendes browser henter billedet direkte fra Unsplash	Besøgendes IP-adresse og browseroplysninger. Ingen cookies. USA. Standardkontraktbestemmelser

Den aktuelle liste, også over leverandører, Striive bruger som dataansvarlig, står på striiveai.com/juridisk/underdatabehandlere.

Bilag 3. Tekniske og organisatoriske foranstaltninger

- Placering: alle data opbevares hos Google Cloud i EU (Stockholm). Data er krypteret i hvile med Googles standardkryptering.
- Kryptering under transport: al trafik til editoren og de udgivne hjemmesider sker over HTTPS med HSTS. Certifikater udstedes automatisk.
- Adskillelse af kunder: hver hjemmesides data er adskilt på databaseniveau med row-level security, som altid håndhæves. Serveren nægter at starte, hvis adskillelsen ikke er aktiv.
- Login: brugere logger ind med en engangskode sendt til deres e-mailadresse (gemt kun som hash, gyldig i 10 minutter, højst 5 forsøg) eller med en adgangsnøgle (passkey), hvor kun den offentlige nøgle gemmes. Tofaktorlogin (TOTP) med gendannelseskoder, der gemmes som hash. Kontoen låses midlertidigt efter gentagne fejlede forsøg. Følsomme handlinger kræver, at brugeren bekræfter sig igen. Sessionscookies er HttpOnly, Secure og bundet til domænet.
- Roller: hver hjemmeside har roller, så kun de rette personer kan redigere, udgive og administrere betaling.
- Webbeskyttelse: Content Security Policy, beskyttelse mod indlejring i andre sider og begrænsning af antal forespørgsler på login og offentlige formularer.
- Hemmeligheder: nøgler og adgangskoder til systemer opbevares i Google Secret Manager. Følsomme værdier i databasen krypteres med AES-256-GCM.
- Driftsadgang: serverne kan kun nås via Googles Identity-Aware Proxy med personligt login. Kun port 80 og 443 er åbne for internettet. Operativsystemet installerer sikkerhedsopdateringer automatisk.
- Sikkerhedskopier: databasen sikkerhedskopieres hver 6. time og medier dagligt til en adskilt, privat lagerplads i EU. Kopier slettes automatisk efter 30 dage. Gendannelse er afprøvet.
- Adskilte miljøer: test sker i et adskilt Google Cloud-projekt, aldrig på kundernes data.
- Logning: vigtige handlinger registreres i en revisionslog med hvem, hvad og hvornår. Loginforsøg registreres.
- Dataminimering: formularsvar og samtykkeregistreringer gemmes uden IP-adresse. Midlertidige rå sidekopier slettes inden for 1 time.
- Brud og hændelser: en skriftlig procedure for håndtering og underretning ved brud og en log over hændelser.
- Fortrolighed: kun personer med et arbejdsmæssigt behov har adgang, og de er underlagt tavshedspligt.