Databehandleraftale

mellem

[Kundens navn]
[Adresse]
CVR-nr. [ ]
(den "Dataansvarlige")

og

Clerkr ApS
Nørregade 28D, 1.
1165 København K
CVR-nr. 46311809
(den "Databehandler")

(tilsammen "Parterne")

Version 2.0, 3. november 2026. Denne skabelon erstatter version 1 af 14. oktober 2026. Felterne for den Dataansvarlige udfyldes ved underskrift.
De engelske dokumenter er originalerne. Denne danske udgave er en oversættelse til orientering. Ved uoverensstemmelse gælder den version, der er underskrevet. Den engelske udgave findes på https://clerkr.ai/en/data-processing-agreement.

1. Baggrund og anvendelsesområde

1.1 Parterne har indgået denne databehandleraftale ("Aftalen") for at overholde artikel 28, stk. 3, i forordning (EU) 2016/679 ("GDPR") og for at sikre en forsvarlig beskyttelse af fysiske personers privatliv og grundlæggende rettigheder og frihedsrettigheder.

1.2 Databehandleren udvikler og leverer "Clerkr", en AI-arbejdsplatform til advokatvirksomheder ("Platformen"). Platformen tilgås via en webapplikation og tilføjelser til Microsoft Word og Outlook og kan kobles til Microsoft Teams og til den Dataansvarliges dokument- og sagsstyringssystemer. Platformen holder sagens materiale samlet, forbereder udkast, opsummeringer, opgaver og overblik og besvarer spørgsmål om sagen med henvisning til kildedokumenterne ved hjælp af retrieval-augmented generation: kun de mest relevante fragmenter af den Dataansvarliges egne dokumenter sendes sammen med brugerens forespørgsel til en sprogmodel i ét enkelt kald. Alt output er udkast til gennemgang af den Dataansvarliges medarbejdere. Platformen kan ikke sende kommunikation på den Dataansvarliges vegne.

1.3 I forbindelse med levering, hosting, support, vedligeholdelse og videreudvikling af Platformen behandler Databehandleren personoplysninger på vegne af den Dataansvarlige i overensstemmelse med denne Aftale.

1.4 Denne Aftale har forrang for tilsvarende bestemmelser i andre aftaler mellem Parterne om behandling af personoplysninger.

1.5 Følgende bilag udgør en integreret del af denne Aftale: Bilag A (Oplysninger om behandlingen), Bilag B (Underdatabehandlere), Bilag C (Instruks og tekniske og organisatoriske foranstaltninger) og Bilag D (Andre forhold aftalt mellem Parterne).

1.6 Denne Aftale og dens bilag opbevares skriftligt, herunder elektronisk, af begge Parter. Aftalen fritager ikke Databehandleren for forpligtelser, der påhviler Databehandleren direkte efter GDPR eller anden lovgivning.

2. Den Dataansvarliges rettigheder og forpligtelser

2.1 Den Dataansvarlige er ansvarlig for, at behandlingen af personoplysninger sker i overensstemmelse med GDPR (jf. artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og denne Aftale.

2.2 Den Dataansvarlige har ret og pligt til at træffe beslutning om formålene med og hjælpemidlerne til behandlingen og er ansvarlig for, at der foreligger et retsgrundlag for den behandling, som Databehandleren instrueres i at foretage, herunder, hvor det er relevant, for særlige kategorier af personoplysninger, oplysninger om straffedomme og lovovertrædelser og danske personnumre.

3. Databehandleren handler efter instruks

3.1 Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den Dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Databehandleren er underlagt; i så fald underretter Databehandleren den Dataansvarlige om dette retlige krav inden behandlingen, medmindre loven forbyder en sådan underretning af hensyn til vigtige samfundsinteresser. Instruksen fremgår af Bilag A og C. Efterfølgende instrukser kan gives af den Dataansvarlige under behandlingen, men skal altid dokumenteres og opbevares skriftligt.

3.2 Databehandleren underretter omgående den Dataansvarlige, hvis en instruks efter Databehandlerens mening er i strid med GDPR eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

3.3 Databehandleren må ikke behandle personoplysninger til andre formål end dem, der er angivet i Bilag A. Databehandleren må navnlig aldrig anvende den Dataansvarliges personoplysninger eller indhold til at træne, finjustere, evaluere eller forbedre nogen sprogmodel eller andet AI-system og skal sikre, at ingen underdatabehandler gør det.

4. Fortrolighed

4.1 Databehandleren sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og at adgangen er begrænset til personer, der har behov for den for at udføre deres opgaver.

4.2 Databehandleren anerkender, at den Dataansvarlige er en advokatvirksomhed, og at de personoplysninger og det indhold, der behandles under denne Aftale, kan være omfattet af advokaters tavshedspligt og lovbestemt fortrolighed. Databehandlerens fortrolighedsforpligtelse for sådanne oplysninger er ikke tidsbegrænset og består efter ophøret af denne Aftale og af enhver anden aftale mellem Parterne.

5. Behandlingssikkerhed

5.1 Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører Databehandleren passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, herunder, alt efter hvad der er relevant, pseudonymisering og kryptering, evnen til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed, evnen til rettidigt at genoprette tilgængeligheden af og adgangen til oplysningerne samt en procedure for regelmæssig afprøvning, vurdering og evaluering af foranstaltningernes effektivitet.

5.2 De foranstaltninger, Databehandleren har gennemført, fremgår af Bilag C og af Databehandlerens Security Overview & Technical and Organisational Measures (version 2.0), som indgår i Bilag C. Databehandleren kan opdatere foranstaltningerne fra tid til anden, forudsat at det samlede sikkerhedsniveau ikke forringes.

5.3 Databehandleren sikrer under alle omstændigheder, at: (a) alle den Dataansvarliges personoplysninger og alt indhold opbevares og behandles, herunder al sprogmodel-inferens og vektorindeksering, på infrastruktur i Den Europæiske Union; (b) personoplysninger og indhold krypteres under transport og i hvile; (c) adgangen er begrænset til den Dataansvarliges organisation og inden for denne følger de adgangsrettigheder, der er sat på hver sag; (d) Databehandlerens eget personale kun kan tilgå den Dataansvarliges miljø, mens den Dataansvarlige har låst den supportadgang op, der er beskrevet i Bilag C; og (e) sprogmodeludbyderen ikke gemmer prompts eller svar efter et inferenskald.

5.4 Databehandleren bistår den Dataansvarlige med at sikre overholdelse af GDPR artikel 32 til 36.

6. Anvendelse af underdatabehandlere

6.1 Den Dataansvarlige giver hermed Databehandleren en generel godkendelse til at anvende de underdatabehandlere, der er anført i Bilag B. Databehandleren vedligeholder listen og stiller den til rådighed for den Dataansvarlige.

6.2 Inden en underdatabehandler anvendes, gennemfører Databehandleren en passende vurdering og indgår en skriftlig aftale med underdatabehandleren, som pålægger denne de samme databeskyttelsesforpligtelser som dem, der fremgår af denne Aftale, herunder navnlig tilstrækkelige garantier for gennemførelse af passende tekniske og organisatoriske foranstaltninger, således at behandlingen opfylder kravene i GDPR. Databehandleren udleverer på anmodning en kopi af den relevante underdatabehandleraftale til den Dataansvarlige; kommercielle vilkår kan overstreges.

6.3 Hvis en underdatabehandler ikke opfylder sine databeskyttelsesforpligtelser, forbliver Databehandleren fuldt ansvarlig over for den Dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser, jf. GDPR artikel 28, stk. 4.

6.4 Databehandleren underretter skriftligt den Dataansvarlige om enhver påtænkt tilføjelse eller udskiftning af en underdatabehandler mindst 30 dage før, underdatabehandleren behandler nogen af den Dataansvarliges personoplysninger. Underretningen skal angive underdatabehandleren, formålet, behandlingsstedet og, hvor det er relevant, overførselsgrundlaget.

6.5 Den Dataansvarlige kan gøre indsigelse mod den påtænkte ændring på rimelige databeskyttelsesretlige grunde ved skriftlig meddelelse inden 14 dage efter modtagelsen af underretningen. Kan Parterne ikke løse indsigelsen inden for en rimelig periode, kan Databehandleren vælge ikke at anvende underdatabehandleren, eller, hvor

underdatabehandleren er nødvendig for levering af tjenesten, kan hver af Parterne opsige de berørte tjenester ved skriftlig meddelelse uden ansvar for opsigelsen, og Databehandleren tilbagebetaler forudbetalte vederlag for perioden efter ophøret.

7. Overførsel til tredjelande eller internationale organisationer

7.1 Databehandleren må ikke overføre personoplysninger til et tredjeland eller en international organisation og må ikke tillade nogen underdatabehandler at gøre det, bortset fra som angivet i Bilag B eller med den Dataansvarliges forudgående skriftlige godkendelse. Den Dataansvarlige godkender hermed de forhold, der er anført i Bilag B, afsnit 5, på de dér angivne betingelser.

7.2 Enhver godkendt overførsel skal ske på grundlag af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet fra Europa-Kommissionen eller andre fornødne garantier efter GDPR kapitel V (artikel 44 til 50), herunder de standardkontraktbestemmelser, Kommissionen har vedtaget. Databehandleren vurderer og dokumenterer på anmodning, om supplerende foranstaltninger er nødvendige.

7.3 Den Dataansvarliges indhold (dokumenter, sagsdata, søgeindeks, embeddings, chathistorik og sprogmodel-inferens) må under ingen omstændigheder overføres til eller behandles i et tredjeland.

7.4 Modtager Databehandleren eller en underdatabehandler en retligt bindende anmodning fra en offentlig myndighed, herunder en myndighed i et tredjeland, om udlevering af personoplysninger behandlet under denne Aftale, skal Databehandleren: (a) underrette den Dataansvarlige uden unødig forsinkelse og senest 24 timer efter at være blevet bekendt med anmodningen, medmindre det er forbudt ved lov, og i så fald bruge sine bedste bestræbelser på at opnå dispensation fra forbuddet; (b) anfægte anmodningen, hvor der er rimelig grund til det, og kun udlevere det minimum af oplysninger, der kræves; (c) omgående suspendere og afbryde forbindelsen til enhver underdatabehandler, der er pålagt at udlevere den Dataansvarliges indhold; og (d) kræve, at underdatabehandleren sletter alt den Dataansvarliges indhold, som den opbevarer. Databehandleren bekræfter, at den på datoen for denne Aftale aldrig har modtaget en sådan anmodning.

8. Bistand til den Dataansvarlige

8.1 Under hensyntagen til behandlingens karakter bistår Databehandleren så vidt muligt den Dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med at opfylde den Dataansvarliges forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder efter GDPR kapitel III og med at sikre overholdelse af forpligtelserne efter GDPR artikel 32 til 36, herunder anmeldelse af brud på persondatasikkerheden, konsekvensanalyser vedrørende databeskyttelse og forudgående høring af tilsynsmyndigheden.

8.2 Databehandleren giver den Dataansvarlige de oplysninger, der er nødvendige for at besvare en anmodning fra en registreret, inden 10 arbejdsdage efter den Dataansvarliges anmodning. Databehandleren svarer ikke de registrerede direkte uden instruks fra den Dataansvarlige.

8.3 Databehandleren kan fakturere den Dataansvarlige for bistand efter medgået tid til sine til enhver tid gældende takster, medmindre bistanden er nødvendig som følge af Databehandlerens brud på denne Aftale eller GDPR eller vedrører et brud på persondatasikkerheden; i disse tilfælde er bistanden vederlagsfri.

9. Underretning om brud på persondatasikkerheden

9.1 Databehandleren underretter den Dataansvarlige uden unødig forsinkelse og under alle omstændigheder senest 24 timer efter at være blevet bekendt med et brud på persondatasikkerheden, der vedrører personoplysninger behandlet under denne Aftale.

9.2 Underretningen skal, i det omfang det er kendt, beskrive bruddets karakter, herunder kategorierne og det omtrentlige antal berørte registrerede og registreringer, de sandsynlige konsekvenser af bruddet, de foranstaltninger, der er truffet eller foreslås truffet for at håndtere bruddet og begrænse dets mulige skadevirkninger, samt kontaktpunktet for yderligere oplysninger. Oplysninger, der ikke er tilgængelige ved den første underretning, gives trinvist uden unødig forsinkelse.

9.3 Databehandleren samarbejder fuldt ud med den Dataansvarlige og eventuelle tilsynsmyndigheder om undersøgelse, begrænsning og udbedring af bruddet og giver de oplysninger, den Dataansvarlige skal bruge til at anmelde bruddet til tilsynsmyndigheden inden 72 timer og, hvor det kræves, til at underrette de registrerede.

10. Sletning og tilbagelevering af personoplysninger

10.1 Den Dataansvarlige kan til enhver tid eksportere sine dokumenter i DOCX- eller PDF-format via Platformen og kan slette dokumenter og chathistorik via Platformen. Sletning af et dokument sletter dets afledte tekstfragmenter og embeddings.

10.2 Ved tjenesternes ophør sletter eller tilbageleverer Databehandleren efter den Dataansvarliges valg alle personoplysninger og sletter eksisterende kopier inden 30 dage, medmindre EU-ret eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne. På anmodning udleverer Databehandleren et SQL-udtræk af den Dataansvarliges organisationsdata inden sletningen.

10.3 Backups, der indeholder den Dataansvarliges personoplysninger, opbevares i højst 30 dage og udløber automatisk. Alle den Dataansvarliges personoplysninger er derfor fjernet fra Databehandlerens systemer, inklusive backups, senest 60 dage efter ophør eller en anmodning om sletning.

10.4 Databehandleren bekræfter sletningen skriftligt på anmodning.

11. Revision, herunder inspektion

11.1 Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelse af GDPR artikel 28 og denne Aftale, til rådighed for den Dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der gennemføres af den Dataansvarlige eller en anden revisor, som er bemyndiget af den Dataansvarlige.

11.2 Databehandleren udleverer på anmodning sin sikkerhedsdokumentation, de certificeringer og revisionsrapporter fra sine underdatabehandlere, som den må dele, og en sammenfatning af eventuelle penetrationstests til den Dataansvarlige.

11.3 Revisioner og inspektioner gennemføres med et rimeligt varsel på mindst 14 dage, højst én gang om året, medmindre et brud eller en tilsynsmyndighed giver anledning til andet, inden for normal arbejdstid og på en måde, der begrænser forstyrrelsen af Databehandlerens drift mest muligt. Den Dataansvarlige bærer sine egne omkostninger og Databehandlerens rimelige, dokumenterede omkostninger ved at understøtte revisionen, medmindre revisionen afdækker et væsentligt brud på denne Aftale fra Databehandlerens side.

12. Andre forhold, ikrafttræden og ophør

12.1 Parterne kan skriftligt aftale yderligere forhold, som ikke er omfattet af denne Aftale; en sådan aftale anføres i Bilag D.

12.2 Denne Aftale træder i kraft på datoen for begge Parters underskrift og gælder, så længe Databehandleren behandler personoplysninger på vegne af den Dataansvarlige. Punkt 4.2 og 10 gælder efter ophør.

12.3 Denne Aftale er underlagt dansk ret. Tvister afgøres af de danske domstole.

13. Kontaktpersoner

Dataansvarlig	Databehandler
Navn: [ ] / E-mail: [ ]	Navn: Niels Høgh Høiberg / E-mail: privacy@clerkr.ai / Clerkr ApS, Nørregade 28D, 1., 1165 København K

14. Underskrifter

Denne Aftale underskrives digitalt.

For den Dataansvarlige	For Databehandleren, Clerkr ApS
Navn: / Titel: / Dato:	Navn: / Titel: / Dato:

Bilag A: Oplysninger om behandlingen

Emne	Beskrivelse
Formål med behandlingen	Levering, hosting, drift, support og vedligeholdelse af Clerkr-platformen for den Dataansvarlige, herunder: opbevaring af dokumenter og sagsmateriale; tekstudtræk og opdeling i fragmenter; vektorindeksering til genfinding; genfinding af relevante fragmenter ved brugerforespørgsler; udarbejdelse af udkast, opsummeringer, opgaver og rettelser; tilkobling til den Dataansvarliges mail, Teams og dokument- eller sagsstyringssystemer; versionering og aktivitetslog; eksport; og kundesupport.
Behandlingens karakter	Automatiseret behandling, herunder indsamling fra tilkoblede systemer, opbevaring, organisering, genfinding, analyse, generering af udkast til tekst og sletning. Sprogmodel-inferens er tilstandsløs: fragmenter og forespørgslen sendes til modellen i ét kald og opbevares ikke af modeludbyderen.
Typer af personoplysninger	Alle personoplysninger i den Dataansvarliges sagsmateriale, herunder navne, kontaktoplysninger, identifikationsnumre (herunder danske personnumre), økonomiske oplysninger, ansættelsesoplysninger, korrespondance og alle andre oplysninger i dokumenter, mails og beskeder; samt brugerkontooplysninger om den Dataansvarliges medarbejdere (navn, arbejdsmail, rolle).
Særlige kategorier og andre følsomme oplysninger	Afhængigt af den Dataansvarliges fagområder kan sagsmaterialet indeholde særlige kategorier af personoplysninger efter GDPR artikel 9 (fx helbredsoplysninger i ansættelses- eller personskadesager), personoplysninger om straffedomme og lovovertrædelser efter GDPR artikel 10 og databeskyttelseslovens § 8 samt personnumre efter databeskyttelseslovens § 11. Databehandleren behandler alene sådanne oplysninger som en del af sagsmaterialet, efter den Dataansvarliges instruks og med foranstaltningerne i Bilag C.
Kategorier af registrerede	Den Dataansvarliges klienter og deres kontaktpersoner, modparter og deres repræsentanter, vidner, den Dataansvarliges medarbejdere (brugere) og andre fysiske personer, der er nævnt i sagsmaterialet.
Behandlingens varighed	I den Dataansvarliges abonnementsperiode, efterfulgt af sletning inden 30 dage og udløb af backups inden yderligere 30 dage, jf. punkt 10.
Behandlingssted	Den Europæiske Union: Railway (EU-region, Holland) og Amazon Web Services eu-central-1 (Frankfurt) med EU-only inferensprofiler. Se Bilag C, afsnit C.3, og Bilag B.

Bilag B: Underdatabehandlere

Den Dataansvarlige har godkendt anvendelsen af følgende underdatabehandlere. Enhedsnavne, datakategorier, overførselsgrundlag og links til sikkerhedsdokumentation fremgår af Clerkrs liste over underdatabehandlere, version 2.0, 3. november 2026, som indgår i dette Bilag.

Underdatabehandler	Formål	Placering	Datakategorier
Amazon Web Services EMEA SARL	S3-objektlagring; Bedrock sprogmodel-inferens (Anthropic Claude-modeller)	EU, eu-central-1 (Frankfurt), EU-only inferensprofiler	Dokumentfiler; forespørgselstekst og genfundne fragmenter på inferenstidspunktet (opbevares ikke)
Railway Corp.	Applikationshosting, PostgreSQL-database, tekstudtræk, vektor-embeddings (Databehandlerens egen model), PDF-rendering, observabilitetsmetadata for sprogmodelkald	EU-region (europe-west4, Holland)	Alle strukturerede kundedata: brugere, dokumenter (metadata og udtrukket tekst), fragmenter, embeddings, chathistorik, opgaver, aktivitetslogs
PostHog Inc. (EU Cloud)	Produktanalyse og fejlsporing	EU (Frankfurt)	Kun hændelsesmetadata; intet dokumentindhold
Resend, Inc. (EU-region)	Systemmails (verificering, nulstilling af adgangskode, notifikationer)	EU (Irland)	Modtagerens mailadresse; emne og tekst i systemmails; aldrig dokumentindhold
Microsoft Corporation (kun hvis den Dataansvarlige kobler Microsoft 365 til)	Login, Outlook, Teams og tilkobling til dokumentsystem via OAuth	Den Dataansvarliges egen Microsoft-tenant	OAuth-tokens (krypteret hos Clerkr); mails og dokumenter hentet fra den Dataansvarliges tenant
Tavily, Inc. (kun hvis den Dataansvarliges administrator slår websøgning til; slået fra som standard)	Websøgning mod offentlige retskilder	EU (Tavilys EU-endpoint)	En søgeforespørgsel formuleret af Platformen ud fra brugerens spørgsmål; aldrig dokumentindhold

Modeludbyder. Anthropic, PBC er leverandør af Claude-modellerne. Modellerne afvikles i AWS Bedrock i Frankfurt, drevet af AWS. Anthropic har ingen adgang til den Dataansvarliges oplysninger og er ikke underdatabehandler. Databehandleren bruger ikke Google Cloud, OpenAI eller Anthropics API direkte.

Afsnit 5. Tredjelandsoverførsler og garantier. Der sker ingen overførsel af den Dataansvarliges personoplysninger til et tredjeland: alle underdatabehandlere behandler oplysningerne i EU-regioner. Railway Corp., Resend, Inc. og Tavily, Inc. har hovedsæde i USA. Deres databehandleraftaler med Databehandleren indeholder EU's standardkontraktbestemmelser som garanti for eventuel fjernsupport uden for EU, og den Dataansvarlige godkender sådan adgang på dette grundlag. Ingen anden overførsel er godkendt.

Bilag C: Instruks og tekniske og organisatoriske foranstaltninger

C.1 Instruks for behandlingen

Databehandleren må kun behandle personoplysninger i overensstemmelse med instruksen i dette Bilag og eventuelle efterfølgende skriftlige instrukser fra den Dataansvarlige. Databehandleren skal navnlig: (a) opbevare, hoste og administrere den Dataansvarliges dokumenter og sagsmateriale; (b) indsamle mails, beskeder og dokumenter fra de systemer, den Dataansvarlige kobler til, og for mails kun gemme på sagen de beskeder, der matcher en sag på et entydigt signal, og for ikke-matchede beskeder kun gemme emne, afsender, dato og bilagsflag i brugerens kø; (c) udtrække og opdele dokumenter i søgbare tekstfragmenter og oprette vektor-embeddings til genfinding; (d) genfinde relevante fragmenter ved brugerforespørgsler; (e) udarbejde udkast, opsummeringer, opgaver og rettelser efter brugernes instruks eller igangsat af Platformen for tilkoblede sager, altid som udkast til menneskelig godkendelse; (f) føre versioner og en aktivitetslog; (g) yde kundesupport; (h) IKKE sende nogen kommunikation på den Dataansvarliges vegne; (i) IKKE bruge den Dataansvarliges oplysninger til træning, finjustering eller evaluering af nogen model; (j) IKKE bruge den Dataansvarliges oplysninger til analyse eller søgning på tværs af kunder; og (k) IKKE videregive den Dataansvarliges oplysninger til tredjeparter, bortset fra som godkendt i Bilag B.

C.2 Den Dataansvarliges adgang og kontrol

Den Dataansvarlige har fuld adgang til alle dokumenter og oplysninger inden for sin organisation, kan til enhver tid eksportere dokumenter i DOCX og PDF, kan til enhver tid slette dokumenter og chathistorik og kan anmode om sletning af nogle eller alle oplysninger, hvilket Databehandleren gennemfører inden 30 dage. Alle databaseforespørgsler afgrænses til organisationen.

C.3 Dataplacering og AWS Bedrock-setup'et

Alle systemer, der behandler eller opbevarer den Dataansvarliges indhold, er placeret i Den Europæiske Union: webapplikation, baggrundsprocesser, database, tekstudtræk og PDF-rendering hos Railway (EU-region, Holland); dokumentfiler i AWS S3 (eu-central-1, Frankfurt); sprogmodel-inferens i AWS Bedrock (eu-central-1-endpoint, EU-only inferensprofiler); vektor-embeddings med Databehandlerens egen model inde i dets Railway-projekt (EU); observabilitetsmetadata for sprogmodelkald på en selvhostet Langfuse-instans i samme projekt; produktanalyse hos PostHog EU Cloud (Frankfurt). Inferens forlader aldrig AWS' EU-regioner. Efter AWS' servicevilkår for Amazon Bedrock deles input og output ikke med modeludbyderne og bruges ikke til at træne modeller. Amazon Bedrock gemmer ikke prompts eller svar, og Databehandleren har ikke aktiveret model invocation logging. Intet af den Dataansvarliges indhold overføres til USA eller noget andet tredjeland.

C.4 Autentificering og adgangskontrol

Login med e-mail og adgangskode med bcrypt-hashede adgangskoder (cost factor 10); adgangskoder i klartekst logges eller gemmes aldrig; e-mailverificering før aktivering; sessioner håndteret af Better-Auth med HttpOnly- og Secure-cookies, 30 dages gyldighed og fornyelse for hver 24 timers aktivitet; engangslinks med tidsbegrænsning (24 timer) til nulstilling af adgangskode og verificering; én organisation og én rolle pr. bruger; adgang inden for organisationen følger rettighederne på hver sag; adgang på tværs af organisationer er strukturelt umulig. Multifaktorgodkendelse (en engangskode sendt pr. mail ved login, som den Dataansvarliges administrator kan kræve for alle brugere) lanceres i november 2026; single sign-on via Microsoft Entra ID er på roadmappen for 2027.

C.5 Lås på supportadgang

Den Dataansvarliges organisation har en lås på supportadgang i sine indstillinger, som er låst som standard. Mens den er låst, kan intet af Databehandlerens personale tilgå den Dataansvarliges indhold (dokumenter, chat, mails og sagsmateriale), og supportsessioner kan ikke startes. Den Dataansvarliges administrator kan låse op for at tillade support og låse igen bagefter. Op- og nedlåsning og hver supportsession registreres i den Dataansvarliges aktivitetslog, låsens tilstand er synlig for dens administratorer, og Databehandlerens personales adgang til produktionsdatabasen logges.

C.6 AI-agentens grænser

Platformen har ingen mulighed for at sende mails eller beskeder; al udgående kommunikation, den forbereder, lægges som kladde. Handlinger med virkning uden for Platformen (oprettelse af en klient, flytning af en fil, skrivning tilbage til den Dataansvarliges dokumentsystem) kræver udtrykkelig godkendelse af en bruger. Hver ændring, Platformen laver i et dokument, opretter en ny version, og den tidligere version bevares. Deling af et dokument eller afsendelse til underskrift er altid en handling, en bruger foretager. Hver agentkørsel logges med sag, instruks, læste oplysninger og produceret output. Agenten bruger et lukket værktøjsregister uden værktøjer til shell, kodeudførelse, mail eller beskeder. Indhold hentet fra dokumenter og mails behandles som data, ikke som instruktioner. Platformen træffer ingen automatiske afgørelser med retsvirkning for fysiske personer.

C.7 Dataisolation og fortrolighed

Hver databasetabel med kundedata har en organisationsidentifikator, der indsættes i hver forespørgsel; genfindingsfunktionen har et obligatorisk organisationsfilter, og alle øvrige forespørgsler afgrænses til organisationen i applikationen; S3-nøgler har præfiks med organisation og sag. Produktanalyse registrerer kun hændelsesmetadata, med sessionsoptagelse og autocapture slået fra. Dokumenter crawles ikke, indekseres ikke eksternt og bruges ikke til markedsføringsanalyse.

C.8 Kryptering

TLS 1.2 eller nyere under transport på alle kunde- og leverandørvendte forbindelser, HSTS håndhævet; AES-256 serverside-kryptering af dokumentfiler i S3, med kundestyrede nøgler tilgængelige på enterprise-kontrakter; diskkryptering af databasen; AES-256-GCM applikationskryptering af integrationstokens og hemmeligheder med nøglen opbevaret alene som produktionsmiljøvariabel; backups arver den respektive platforms kryptering.

C.9 Logning og revision

Pipeline-logs pr. behandlingskørsel; chathistorik, værktøjskald, model og promptversion pr. organisation; genfindingslogs med bruger, organisation og antal resultater (ikke indhold); logs for agentkørsler; dokumentversionshistorik med ophavsperson og tidspunkt; revisionslog over Databehandlerens personales adgang til produktionsdatabasen. Observabilitet for sprogmodelkald på en selvhostet Langfuse-instans i EU registrerer kun tidsforbrug, model og tokenantal, aldrig prompts, svar eller indhold. Ingen tredjeparts fejlsporingstjeneste eller ekstern LLM-observabilitetstjeneste anvendes.

C.10 Databehandlerens personales adgang

Produktionshemmeligheder opbevares alene i produktionsmiljøet; en kort liste over navngivne udviklere med produktionsadgang, som tilbagekaldes ved fratræden; MFA på alle cloudkonti og SSO på Railway; en dedikeret IAM-bruger afgrænset til Clerkrs S3-buckets og Bedrock-kald; ingen databaseadgang uden for det private netværk; udvikleradgang til produktionsdata kun via en udtrykkelig, tidsbegrænset session, underlagt låsen på supportadgang og logget; ingen administrativ grænseflade, der eksponerer rå personoplysninger.

C.11 Forsyningskæde, ændringsstyring og sårbarhedshåndtering

Afhængigheder låst via lockfile; builds alene fra lockfilen; pull request og CI (lint, typekontrol, skemavalidering) før produktion; adskilte udviklings-, staging- og produktionsmiljøer; ingen kundeproduktionsdata i udvikling eller test; sikkerhedsadvarsler gennemgås og rettes i den almindelige udgivelsescyklus, kritiske sårbarheder uden for cyklus; ekstern penetrationstest planlagt inden udgangen af 1. kvartal 2027 og derefter mindst årligt, med en sammenfatning tilgængelig for den Dataansvarlige på anmodning.

C.12 Backup og katastrofegenopretning

Daglige databasebackups og S3-objektversionering; backup-opbevaring 30 dage; backupsystemer med de samme sikkerhedsforanstaltninger som produktion; Recovery Point Objective 24 timer og Recovery Time Objective 8 arbejdstimer.

C.13 Underretning om brud og samarbejde

Platforms- og pipelinefejl logges og gennemgås af Databehandlerens udviklere, og automatisk alarmering er under indførelse; underretning af den Dataansvarlige uden unødig forsinkelse og senest 24 timer efter kendskab til et brud på persondatasikkerheden med oplysningerne i punkt 9; fuldt samarbejde om undersøgelse og udbedring; bistand til den Dataansvarliges anmeldelse til tilsynsmyndigheden og underretning af de registrerede.

C.14 De registreredes rettigheder

Bistand til indsigt, berigtigelse, sletning, begrænsning og dataportabilitet; oplysninger leveres inden 10 arbejdsdage efter den Dataansvarliges anmodning; intet direkte svar til registrerede uden instruks. Berigtigelse foretages i kildedokumentet, hvorefter fragmenter og embeddings genereres igen. Sletning af et dokument sletter dets fragmenter og embeddings.

C.15 Opbevaring

Kundeindhold: abonnementsperioden, sletning inden 30 dage efter ophør eller anmodning. Backups: 30 dage. Brugerkontodata: slettes inden 90 dage efter ophør. Sikkerheds- og driftslogs samt analysehændelser: 12 måneder. Observabilitetsmetadata for sprogmodelkald: slettes sammen med organisationen. Ingen opbevaring hos AWS Bedrock.

C.16 Tredjelandsoverførsler og myndighedsanmodninger

Ingen af den Dataansvarliges personoplysninger overføres til et tredjeland; alle underdatabehandlere behandler i EU-regioner, herunder systemmails (Resend, EU-region) og, hvis slået til, websøgning (Tavilys EU-endpoint). Leverandører med hovedsæde uden for EU har EU's standardkontraktbestemmelser i deres databehandleraftaler som garanti for fjernsupport, jf. Bilag B, afsnit 5. AWS har forpligtet sig til at underrette kunder om myndighedsanmodninger om kundedata, hvor det er lovligt, og til at anfægte uberettigede anmodninger. Databehandleren anvender proceduren i punkt 7.4, herunder omgående afbrydelse af forbindelsen til enhver underdatabehandler, der pålægges at udlevere den Dataansvarliges indhold.

C.17 Organisation og personale

Skriftlige politikker for informationssikkerhed og databeskyttelse med definerede roller; tavshedspligt og årlig oplæring for alt personale med adgang til kundedata; vurdering af underdatabehandlere før anvendelse og videreførelse af tilsvarende databeskyttelsesforpligtelser; navngivet sikkerheds- og databeskyttelseskontakt (punkt 13).

Bilag D: Andre forhold aftalt mellem Parterne

Ingen.