

Databehandleraftale — Lovbasen.dk

Databehandleraftale

Vedrørende behandling af personoplysninger i forbindelse med Lovbasen.dk

Mellem

Kunden (den dataansvarlige) — herefter benævnt “den Dataansvarlige” —

og

Stougaard Plan ApS CVR-nr.: 45908941 Rabalderstræde 7, 4000 Roskilde Kontaktperson: Lasse Emil Stougaard
E-mail: kontakt@stpl.dk — herefter benævnt “Databehandleren” —

Samlet benævnt “Parterne”.

Ikrafttrædelsesdato: Samtidig med kundens accept af abonnementsvilkår for Lovbasen.dk.

1. Baggrund og formål

1.1. Denne databehandleraftale (“Aftalen”) er indgået i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger (databeskyttelsesforordningen, herefter “GDPR”), artikel 28, stk. 3.

1.2. Aftalen fastsætter de rettigheder og forpligtelser, der gælder, når Databehandleren behandler personoplysninger på vegne af den Dataansvarlige i forbindelse med levering af tjenesten Lovbasen.dk.

1.3. Lovbasen.dk er en søgbar database over offentligt tilgængelige klagenævnsafgørelser fra Nævnenes Hus (Planklagenævnet, Miljø- og Fødevareklagenævnet og Energiklagenævnet). Tjenesten leveres som Software-as-a-Service (SaaS) til kommunale sagsbehandlere og andre fagprofessionelle.

1.4. Lovbasen.dk indekserer afgørelser fra Nævnenes Hus, der er offentligt tilgængelige på naevneneshus.dk. Afgørelserne kan indeholde personoplysninger om fysiske personer (klagere, naboer, ejere mv.) og udgør i juridisk forstand fortsat personoplysninger omfattet af GDPR, jf. art. 4, nr. 1. Den omstændighed, at oplysningerne er offentliggjort af en offentlig myndighed, ændrer ikke deres karakter som personoplysninger, men er en del af det retsgrundlag, hvorpå Databehandleren foretager indeksering og tilgængeliggørelse, jf. GDPR art. 6, stk. 1, litra e (offentlig interesse) og litra f (legitim interesse), sammenholdt med databeskyttelseslovens § 8, stk. 2. Behandlingen af afgørelses-indholdet sker således i en separat dataansvars-kontekst hos Databehandleren (jf. punkt 1.6), mens behandlingen af brugerdata (kontooplysninger, søgehistorik mv.) sker på vegne af den Dataansvarlige under nærværende aftale.

1.5. **Dual dataansvars-struktur.** Der består to adskilte behandlings-relationer: - **(a)** Databehandleren er **selvstændig dataansvarlig** for indekseringen af de offentliggjorte afgørelser fra Nævnenes Hus. Hjemmel: GDPR art. 6, stk. 1, litra e (samfundets interesse i adgang til retskilder) og litra f (legitim interesse, herunder fagprofessionelles informationsadgang), jf. databeskyttelseslovens § 8, stk. 2. Denne behandling reguleres ikke af nærværende aftale. - **(b)** Databehandleren er **databehandler** for den Dataansvarlige for så vidt angår behandling af brugerdata, herunder kontooplysninger, søgehistorik, betalingsoplysninger og IP-adresser. Denne behandling reguleres af nærværende aftale.

1.6. Aftalen er udformet i overensstemmelse med Datatilsynets standardkontraktbestemmelser for databehandlere.

2. Den Dataansvarliges instruks

2.1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den Dataansvarlige, medmindre det kræves i henhold til EU-ret eller national ret, som Databehandleren er underlagt. I så fald underretter Databehandleren den Dataansvarlige om dette retlige krav inden behandlingen, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

2.2. Databehandleren behandler udelukkende personoplysninger i overensstemmelse med denne aftale og til følgende formål:

- a. Administration af brugerkonti (login, autentificering)
- b. Behandling af betalinger via Stripe
- c. Behandling af søgeforespørgsler, herunder videreformidling til AI-tjeneste med henblik på filtrering af søgeresultater
- d. Generering af anonymiseret brugsstatistik

2.3. Databehandleren må ikke behandle personoplysningerne til egne formål eller til formål, der ligger uden for den Dataansvarliges instruks.

3. Kategorier af registrerede og personoplysninger

3.1. Behandlingen omfatter følgende kategorier af registrerede:

- Brugere af Lovbasen.dk (typisk kommunale sagsbehandlere, rådgivere og advokater)

3.2. Behandlingen omfatter følgende typer af personoplysninger:

Kategori	Eksempler	Grundlag
Kontooplysninger	E-mailadresse (bruges som login)	Kontraktopfyldelse
Søgehistorik	Søgetermer og anvendte filtre	Kontraktopfyldelse
Betalingsoplysninger	Betalingsoplysninger håndteret af Stripe (Databehandleren opbevarer ikke fulde kortoplysninger)	Kontraktopfyldelse
Tekniske data	IP-adresse (i serverlogfiler, Simply.com)	Legitim interesse (sikkerhed)

3.3. Der behandles ikke følsomme personoplysninger (særlige kategorier af personoplysninger, jf. GDPR artikel 9) eller oplysninger om strafbare forhold (jf. GDPR artikel 10).

4. Fortrolighed

4.1. Databehandleren sikrer, at de personer, der er autoriseret til at behandle personoplysningerne, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

4.2. Fortrolighedsforpligtelsen gælder også efter ophør af denne aftale.

5. Behandlingssikkerhed

5.1. Databehandleren gennemfører passende tekniske og organisatoriske foranstaltninger i henhold til GDPR artikel 32 for at sikre et sikkerhedsniveau, der passer til risikoen ved behandlingen. Databehandleren tager hensyn til det aktuelle tekniske niveau, implementeringsomkostningerne og behandlingens art, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

5.2. Databehandleren har implementeret følgende sikkerhedsforanstaltninger:

Tekniske foranstaltninger:

- HTTPS/TLS-kryptering på alle forbindelser til lovbasen.dk
- Autentificering via e-mailbaseret login med token opbevaret i localStorage
- Betalingshåndtering outsourcet til Stripe (PCI DSS-certificeret)
- Adgangsbegrænsning til serverinfrastruktur (SSH med Ed25519-nøgle)
- .htaccess-beskyttelse af konfigurationsfiler (.env)
- Gzip-komprimering af datatransmission
- Ingen lagring af fulde betalingskortoplysninger på egne servere
- AI-søgning via Anthropic API med krypteret API-kommunikation (HTTPS)

Organisatoriske foranstaltninger:

- Begrænset adgang: kun Databehandlerens ansvarlige person har adgang til serverinfrastruktur
- Underdatabehandlere er vurderet og godkendt (se Bilag 1)
- Løbende overvågning og vedligeholdelse af tjenesten

Analytics:

- Plausible Analytics anvendes til brugsstatistik. Plausible er cookiefri og behandler ikke personoplysninger i GDPR-forstand. Data aggregeres og kan ikke henføres til enkeltpersoner.

Cookies:

- Tjenesten anvender udelukkende nødvendige cookies/tokens (login-token i localStorage). Der anvendes ingen tracking-cookies eller tredjepartscookies.

5.3. Audit-log over søgninger på navngivne fysiske personer.

5.3.1. Databehandleren logger pr. brugersession følgende metadata: tidsstempel, bruger-ID (intern), anonymiseret IP, søgetekst og anvendte filtre. Loggen opbevares i 12 måneder og slettes derefter automatisk.

5.3.2. På anmodning fra den Dataansvarlige leverer Databehandleren inden for 10 arbejdsdage en udtræk af loggen for den Dataansvarliges egne brugere. Udtrækket leveres i CSV-format og kan filtreres på bruger, periode og fritekst-match.

5.3.3. Audit-logning understøtter den Dataansvarliges fortegnelses-pligt jf. GDPR art. 30 og pligten til at kunne dokumentere lovlig behandling jf. art. 5, stk. 2 (ansvarlighedsprincippet) — særligt ved søgninger der involverer navne på fysiske personer i offentliggjorte afgørelser.

5.3.4. (usikker — kræver verifikation hos John inden pilot-launch at audit-log faktisk er implementeret i sessions-tabellen og at CSV-eksport er tilgængelig via /api/sessions.php eller separat admin-endpoint).

6. Anvendelse af underdatabehandlere

6.1. Den Dataansvarlige giver ved indgåelse af denne aftale Databehandleren en generel skriftlig godkendelse til at anvende underdatabehandlere.

6.2. De godkendte underdatabehandlere fremgår af Bilag 1 til denne aftale.

6.3. Databehandleren underretter den Dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere og giver dermed den Dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer. Underretning sker via e-mail med mindst 30 dages varsel inden den nye underdatabehandler påbegynder behandling.

6.4. Gør den Dataansvarlige indsigelse mod en ny underdatabehandler, har Databehandleren ret til at opsige aftalen med virkning fra det tidspunkt, hvor den nye underdatabehandler ville have påbegyndt behandlingen, dog med mindst 30 dages varsel.

6.5. Databehandleren sikrer, at underdatabehandlere er underlagt samme forpligtelser som dem, der er fastsat i denne aftale, ved indgåelse af en skriftlig aftale med den pågældende underdatabehandler.

6.6. Databehandleren er fuldt ansvarlig over for den Dataansvarlige for underdatabehandlerens opfyldelse af sine forpligtelser.

7. Overførsel til tredjelande

7.1. Behandling af personoplysninger finder som udgangspunkt sted inden for EU/EØS.

7.2. Hosting af tjenesten sker hos Simply.com med servere i Danmark.

7.3. Stripe kan overføre betalingsoplysninger til USA. Stripe er certificeret under EU-U.S. Data Privacy Framework og overholder dermed GDPR artikel 45 (afgørelse om tilstrækkeligt beskyttelsesniveau).

7.4. Anthropic (Claude AI-tjeneste) behandler søgeforespørgsler i USA. Overførslen sker på grundlag af EU-standardkontraktbestemmelser (Standard Contractual Clauses, SCC) i henhold til GDPR artikel 46, stk. 2, litra c, samt Anthropic's tillægsgarantier. Kun selve søgeteksten overføres — ikke brugerens e-mailadresse eller andre identifikationsoplysninger.

7.5. Databehandleren foretager ikke øvrige overførsler af personoplysninger til tredjelande uden forudgående skriftlig godkendelse fra den Dataansvarlige.

8. Bistand til den Dataansvarlige

8.1. Databehandleren bistår, under hensyntagen til behandlingens karakter, den Dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger, i det omfang det er muligt, med opfyldelse af den Dataansvarliges forpligtelse til at besvare anmodninger fra registrerede om udøvelse af deres rettigheder i henhold til GDPR kapitel III, herunder:

- a. Ret til indsigt (artikel 15)
- b. Ret til berigtigelse (artikel 16)
- c. Ret til sletning (artikel 17)
- d. Ret til begrænsning af behandling (artikel 18)
- e. Ret til dataportabilitet (artikel 20)

- f. Ret til indsigelse (artikel 21)

8.2. Databehandleren bistår den Dataansvarlige med at sikre overholdelse af forpligtelserne i henhold til GDPR artikel 32-36 (behandlingssikkerhed, anmeldelse af brud, konsekvensanalyse og forudgående høring), under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for Databehandleren.

8.3. Modtager Databehandleren en henvendelse fra en registreret vedrørende den registreredes rettigheder, videresender Databehandleren straks henvendelsen til den Dataansvarlige.

9. Underretning om brud på persondatasikkerheden

9.1. Databehandleren underretter uden unødigt forsinkelse den Dataansvarlige efter at være blevet opmærksom på et brud på persondatasikkerheden.

9.2. Underretningen skal som minimum indeholde:

- a. En beskrivelse af bruddet, herunder de berørte kategorier af registrerede og det omtrentlige antal berørte
- b. Navn og kontaktoplysninger på Databehandlerens kontaktperson
- c. En beskrivelse af de sandsynlige konsekvenser af bruddet
- d. En beskrivelse af de foranstaltninger, der er truffet eller foreslået for at håndtere bruddet

9.3. Underretning sker til den Dataansvarliges kontaktperson via e-mail.

10. Sletning og returnering af personoplysninger

10.1. Ved ophør af behandlingen af personoplysninger sletter Databehandleren alle personoplysninger, der er behandlet på vegne af den Dataansvarlige, medmindre EU-ret eller national ret foreskriver opbevaring.

10.2. Den Dataansvarlige kan inden ophør anmode om at få udleveret personoplysningerne i et struktureret, almindeligt anvendt og maskinlæsbart format.

10.3. Sletning foretages senest 30 dage efter aftalens ophør. Databehandleren bekræfter skriftligt, at sletning er sket.

10.4. Sletningen omfatter:

- a. Brugerens e-mailadresse og kontooplysninger
- b. Søgehistorik knyttet til brugeren
- c. Eventuelle logfiler der indeholder personhenførbare oplysninger

10.5. Betalingshistorik hos Stripe er underlagt Stripes egne dataopbevaringspolitikker og lovkrav. Databehandleren bistår den Dataansvarlige med sletningsanmodninger til Stripe.

11. Revision og audit

11.1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelse af GDPR artikel 28, til rådighed for den Dataansvarlige og tillader og bidrager til revisioner, herunder inspektioner, der foretages af den Dataansvarlige eller en af den Dataansvarlige bemyndiget revisor.

11.2. Databehandleren underretter omgående den Dataansvarlige, hvis en instruks efter Databehandlerens opfattelse er i strid med GDPR eller andre databeskyttelsesbestemmelser i EU eller medlemsstaterne.

11.3. Audit kan gennemføres med rimeligt varsel (mindst 14 dage) og i Databehandlerens normale åbningstid. Den Dataansvarlige afholder selv sine omkostninger i forbindelse med audit.

12. Aftalens varighed og ophør

12.1. Aftalen er gældende, så længe Databehandleren behandler personoplysninger på vegne af den Dataansvarlige. Aftalen følger det underliggende abonnements varighed.

12.2. Ved ophør af abonnementet ophører denne aftale automatisk, og bestemmelserne i punkt 10 om sletning finder anvendelse.

12.3. Fortrolighedsforpligtelsen i punkt 4 og bestemmelserne om ansvar gælder fortsat efter aftalens ophør.

13. Ansvar

13.1. Parternes ansvar følger de til enhver tid gældende regler i GDPR, herunder artikel 82 om erstatning og artikel 83 om administrative bøder.

13.2. Databehandlerens samlede ansvar under denne aftale er begrænset til det beløb, den Dataansvarlige har betalt til Databehandleren i de foregående 12 måneder forud for det ansvarspådragende forhold. Denne begrænsning gælder ikke i tilfælde af forsætlig eller groft uagtsom adfærd.

14. Lovvalg og værneting

14.1. Aftalen er underlagt dansk ret.

14.2. Tvister, der udspringer af denne aftale, afgøres ved de danske domstole med Retten i Roskilde som aftalt værneting i første instans.

15. Underskrift

Denne aftale er udarbejdet i to enslydende eksemplarer, et til hver part.

Den Dataansvarlige:

Dato: _____

Navn: _____

Titel: _____

Underskrift: _____

Databehandleren (Stougaard Plan ApS):

Dato: _____

Navn: Lasse Emil Stougaard

Titel: Indehaver

Underskrift: _____

Bilag 1: Godkendte underdatabehandlere

Nedenstående underdatabehandlere er godkendt af den Dataansvarlige ved indgåelse af databehandleraftalen.

1. Simply.com (Hosting)

Felt	Oplysning
Virksomhedsnavn	Simply.com (Gratisdns ApS)
CVR-nr.	20712529
Adresse	Borgergade 14, 1., 1300 København K, Danmark
Behandlingsformål	Hosting af Lovbasen.dk, herunder serverlogfiler, databaseopbevaring og e-mailfunktionalitet
Personoplysninger	E-mailadresser, søgehistorik, IP-adresser (serverlogfiler)
Geografisk placering	Danmark (servere i Danmark)
Overførselsgrundlag	Ikke relevant — behandling sker inden for EU/EØS

2. Stripe, Inc. (Betaling)

Felt	Oplysning
Virksomhedsnavn	Stripe, Inc. / Stripe Payments Europe, Ltd.
Adresse	354 Oyster Point Blvd, South San Francisco, CA 94080, USA / 1 Grand Canal Street Lower, Dublin 2, Irland
Behandlingsformål	Behandling af betalinger for abonnementer på Lovbasen.dk
Personoplysninger	E-mailadresse, betalingsoplysninger (kortnummer håndteres udelukkende af Stripe)
Geografisk placering	EU (Irland) og USA
Overførselsgrundlag	EU-U.S. Data Privacy Framework (tilstrækkelighedsafgørelse)
Certificeringer	PCI DSS Level 1, SOC 2 Type II

3. Anthropic (AI-søgning)

Felt	Oplysning
Virksomhedsnavn	Anthropic, PBC
Adresse	548 Market St, PMB 90375, San Francisco, CA 94104, USA
Behandlingsformål	Behandling af søgeforespørgsler med henblik på generering af søgefiltre via Claude AI-model
Personoplysninger	Søgetekst (fritekst indtastet af brugeren). Der overføres ikke e-mail, navn eller andre identifikationsoplysninger til Anthropic.

Felt	Oplysning
Geografisk placering	USA
Overførselsgrundlag	EU-standardkontraktbestemmelser (SCC) samt Anthropic Data Processing Addendum
Bemærkninger	Anthropic anvender ikke API-data til modeltræning (jf. Anthropic API Terms of Service). Søgeteksten indeholder typisk faglige termer (lovparagraffer, kommunenavne, emner) og ikke personoplysninger i sig selv.

4. Voyage AI (Embeddings)

Felt	Oplysning
Virksomhedsnavn	Voyage AI Innovations, Inc.
Adresse	Palo Alto, CA, USA
Behandlingsformål	Generering af tekstembeddings til semantisk søgning ("vis lignende sager"). Anvendes både ved indeksering af afgørelser (selvstændig dataansvars-relation, jf. § 1.5(a)) og ved konvertering af brugernes søgetekst til embedding (databehandler-relation under nærværende aftale).
Personoplysninger	Søgetekst (fritekst indtastet af brugeren). Der overføres ikke e-mail, navn eller IP til Voyage.
Geografisk placering	USA
Overførselsgrundlag	EU-standardkontraktbestemmelser (SCC) jf. GDPR art. 46, stk. 2, litra c.
Bemærkninger	Voyage anvender ikke API-data til modeltræning (jf. Voyage API Terms). Modellen voyage-3-lite, 512-dim embeddings.

5. Transaktionsmail — håndteres af Simply.com (jf. underdatabehandler 1)

Afsendelse af login-links, ugentlige alerts om nye afgørelser i gemte søgninger og øvrig transaktionsmail sker via PHPMailer over Simply.com SMTP (websmtp.simply.com:587, STARTTLS). Simply.com er allerede listet som underdatabehandler under pkt. 1 (Hosting), og mail-trafikken er omfattet af samme aftale og samme geografiske placering (Danmark). Der overføres ingen e-maildata til tredjelande i forbindelse med transaktionsmail.

Note (opdateret 30/4-2026): Resend var listet som selvstændig underdatabehandler i tidligere udkast af denne aftale. Det er verificeret 30/4-2026 (J3 — Johns audit-rapport `_fix_runde3_john_pseudonymisering_2026-04-30.md`, pkt. 3) ved kode-søgning på serveren samt gennemgang af `.env`, at Resend ikke faktisk anvendes — Lovbasen.dk sender al mail via PHPMailer + Simply.com SMTP. Hvis Lovbasen senere migrerer til Resend (eller anden ekstern transaktionsmail-leverandør i tredjeland), opdateres denne aftale som tillæg efter proceduren i § 6.3 (30 dages varsel) inden migration.

Underdatabehandlere der IKKE anvendes

For at undgå tvivl bekræftes, at følgende ofte forekommende leverandører **ikke** behandler personoplysninger på vegne af Lovbasen.dk:

- 02.05.2026, 23.03
- Databehandleraftale — Lovbasen.dk
- **Cloudflare** (ingen WAF/CDN konfigureret pr. 29/4-2026 — verificeret af John).
 - **Google Fonts CDN** (Inter font er self-hosted via Simply.com — ingen tredjepartskald).
 - **Plausible Analytics** behandler ikke personoplysninger i GDPR-forstand (cookieløs, fuldt aggregeret) og er derfor ikke optaget på listen — jf. § 5.2.
 - **Resend, Inc.** (transaktionsmail) — verificeret 30/4-2026 (J3) at Resend ikke anvendes; al transaktionsmail sendes via Simply.com SMTP, jf. § 5 ovenfor.

Hvis Databehandleren senere implementerer Cloudflare WAF, anden CDN, Resend eller andre underdatabehandlere, sker det efter proceduren i § 6.3 (30 dages varsel).

Bilag 2: Instruks fra den Dataansvarlige

Den Dataansvarliges instruks til Databehandleren er beskrevet i denne aftales punkt 2 og konkretiseres som følger:

Behandlingens genstand

Levering af SaaS-tjenesten Lovbasen.dk, herunder brugerkontoadministration, søgefunktionalitet (herunder AI-assisteret søgning), betalingshåndtering og brugsstatistik.

Behandlingens varighed

Fra brugerens oprettelse af konto til 30 dage efter ophør af abonnement eller sletning af konto.

Behandlingens art og formål

Aktivitet	Formål	Datatype
Brugeroprettelse og login	Autentificering og adgangsstyring	E-mailadresse
Søgning i database	Levering af kerneydelsen	Søgetermer, filtre
AI-assisteret søgning	Generering af relevante filtre baseret på fritekst	Søgetekst (videresendes til Anthropic)
Betalingshåndtering	Opkrævning af abonnement	E-mail, betalingsoplysninger (via Stripe)
Serverlogging	Driftsovervågning og sikkerhed	IP-adresse, tidsstempel
Analytics (Plausible)	Anonymiseret brugsstatistik	Ingen personoplysninger

Kategorier af registrerede

Brugere af Lovbasen.dk — primært kommunale sagsbehandlere inden for teknik og miljø, planlæggere, advokater og rådgivere.

Kategorier af personoplysninger

Almindelige personoplysninger: e-mailadresse, søgehistorik, IP-adresse, betalingsoplysninger (håndteret af Stripe).

Der behandles ikke følsomme personoplysninger.

Denne databehandleraftale er senest opdateret den 2. maj 2026 (Helge, IT-sikkerheds- og compliance-konsulent).

Versionshistorik: — 29/4-2026 (v1.0): Dual dataansvar (§ 1.4–1.6), audit-log (§ 5.3), Bilag 1 udvidet med Voyage AI og Resend. — 30/4-2026 (v1.1): Resend fjernet fra Bilag 1 efter Johns verifikation (J3) — al transaktionsmail sendes via Simply.com SMTP. Bilag 1 § 5 omformuleret til note om transaktionsmail under Simply.com, og Resend tilføjet til “Underdatabehandlere der IKKE anvendes”. Versionsfodnote i Bilag 2 ajourført. — 2/5-2026 (v1.2): Bekræftet at Voyage AI er aktiv underdatabehandler i Bilag 1 § 4 (AI-paragrafsøgning på /lov2/, voyage-3-lite embeddings, USA via SCC). Implementeret CPR/email/telefon-redaction af søgetekst FØR audit-storage (§ 5.3) i /api/paragraf-search.php, så persondata ikke gemmes i 12-mdr audit-log selv hvis bruger ved et uheld indtaster det. IP-hash bekræftet HMAC-SHA256 med pepper fra .env (TOKEN_PEPPER).