DATABEHANDLERAFTALE

mellem den dataansvarlige og CVR Intel som databehandler

Denne aftale fastsætter rettigheder og forpligtelser i forbindelse med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige, jf. artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 (databeskyttelsesforordningen).

Parter

Den dataansvarlige	Databehandleren
Navn / Virksomhed	**CVR Intel**
CVR-nr.:	CVR-nr.: 40342079
Adresse:	Adresse: Solhøjparken 14, 8464 Galten
Kontakt:	Kontakt vedrørende databeskyttelse: support@cvrintel.dk
Email:	
Telefon:	

1. Baggrund og formål

1.1 Databehandleren leverer en softwaretjeneste (CVR Intel), der giver den dataansvarlige adgang til søgning, analyse og overvågning af danske virksomheder på grundlag af offentligt tilgængelige data fra Det Centrale Virksomhedsregister (CVR).

1.2 I forbindelse med levering af tjenesten behandler databehandleren et begrænset omfang af personoplysninger på vegne af den dataansvarlige. Behandlingens karakter og omfang fremgår af Bilag A.

1.3 Virksomhedsdata fra CVR-registret behandles af databehandleren som selvstændig dataansvarlig i overensstemmelse med lov om Det Centrale Virksomhedsregister. Denne aftale omfatter ikke denne behandling.

2. Instruks

2.1 Databehandleren må alene behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige. Denne aftale med bilag udgør den dataansvarliges samlede instruks.

2.2 Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens opfattelse er i strid med databeskyttelsesforordningen eller anden databeskyttelseslovgivning.

2.3 Databehandleren overfører ikke personoplysninger til tredjelande eller internationale organisationer uden forudgående skriftlig instruks fra den dataansvarlige. Der finder på nuværende tidspunkt ingen overførsel sted uden for EU/EØS, jf. Bilag B.

3. Fortrolighed

3.1 Databehandleren sikrer, at enhver person med adgang til de personoplysninger, der behandles på vegne af den dataansvarlige, er underlagt tavshedspligt.

3.2 Adgang til produktionsdata er begrænset til det antal personer, der er nødvendigt for tjenestens drift, jf. Bilag C.

4. Behandlingssikkerhed

4.1 Databehandleren gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der svarer til risikoen, jf. databeskyttelsesforordningens artikel 32.

4.2 De gennemførte foranstaltninger er beskrevet i Bilag C. Foranstaltningerne kan opdateres, forudsat at sikkerhedsniveauet ikke forringes.

4.3 Databehandleren fører en fortegnelse over behandlingsaktiviteter udført på vegne af den dataansvarlige, jf. artikel 30, stk. 2.

5. Underdatabehandlere

5.1 Den dataansvarlige giver ved indgåelse af denne aftale generel godkendelse til anvendelse af de underdatabehandlere, der fremgår af Bilag B.

5.2 Databehandleren underretter skriftligt den dataansvarlige mindst 30 dage før ikrafttræden af enhver påtænkt tilføjelse eller udskiftning af underdatabehandlere. Den dataansvarlige kan gøre indsigelse inden for varslingsperioden.

5.3 Databehandleren pålægger enhver underdatabehandler de samme databeskyttelsesforpligtelser som fastsat i denne aftale og hæfter for underdatabehandlerens opfyldelse heraf.

5.4 Databehandleren opretholder en aktuel oversigt over anvendte underdatabehandlere, som stilles til rådighed for den dataansvarlige på anmodning.

6. Bistand til den dataansvarlige

6.1 Databehandleren bistår, under hensyntagen til behandlingens karakter og så vidt muligt, den dataansvarlige med opfyldelse af forpligtelser over for registrerede, herunder anmodninger om indsigt, berigtigelse, sletning, begrænsning og dataportabilitet.

6.2 Databehandleren bistår den dataansvarlige med at sikre overholdelse af forpligtelserne i artikel 32-36, herunder ved konsekvensanalyser og forudgående høring.

6.3 Modtager databehandleren en anmodning direkte fra en registreret, videresendes anmodningen uden unødig forsinkelse til den dataansvarlige. Databehandleren besvarer ikke selv anmodningen, medmindre andet er aftalt.

7. Brud på persondatasikkerheden

7.1 Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på et brud på persondatasikkerheden.

7.2 Underretningen indeholder, i det omfang det er muligt:

- en beskrivelse af bruddets karakter,
- de berørte kategorier og det omtrentlige antal berørte registrerede,
- de sandsynlige konsekvenser af bruddet,
- de foranstaltninger, der er truffet eller foreslås truffet for at håndtere bruddet,
- kontaktoplysninger på den person, hos hvem yderligere oplysninger kan indhentes.

7.3 Databehandleren bistår den dataansvarlige med anmeldelse til Datatilsynet og eventuel underretning af registrerede.

8. Sletning og tilbagelevering

8.1 Ved ophør af tjenesten sletter databehandleren efter den dataansvarliges valg alle personoplysninger eller tilbageleverer dem til den dataansvarlige.

8.2 Den dataansvarlige kan til enhver tid slette sin konto via tjenestens brugergrænseflade, hvorefter samtlige personoplysninger slettes.

8.3 Uanset punkt 8.1 og 8.2 opbevarer databehandleren bogføringspligtige transaktionsoplysninger i 5 år fra udgangen af det regnskabsår, materialet vedrører, jf. bogføringsloven. Denne behandling sker på grundlag af artikel 6, stk. 1, litra c (retlig forpligtelse), hvor databehandleren optræder som selvstændig dataansvarlig.

9. Revision og tilsyn

9.1 Databehandleren stiller på anmodning alle oplysninger til rådighed, der er nødvendige for at påvise overholdelse af artikel 28.

9.2 Databehandleren giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en af denne bemyndiget revisor. Revision kan gennemføres én gang årligt med mindst 30 dages skriftligt varsel, og skal gennemføres på en måde, der ikke unødigt forstyrrer databehandlerens drift.

9.3 Den dataansvarlige afholder egne omkostninger ved revision. Databehandlerens dokumenterede rimelige omkostninger ved bistand hertil kan faktureres.

10. Ikrafttræden, varighed og ophør

10.1 Aftalen træder i kraft ved begge parters underskrift og er gældende, så længe databehandleren behandler personoplysninger på vegne af den dataansvarlige.

10.2 Aftalen kan ikke opsiges særskilt, så længe hovedaftalen om levering af tjenesten består.

10.3 Ved uoverensstemmelse mellem denne aftale og hovedaftalen har denne aftale forrang for så vidt angår behandling af personoplysninger.

11. Lovvalg og værneting

11.1 Aftalen er undergivet dansk ret.

11.2 Enhver tvist afgøres ved de danske domstole med den dataansvarliges hjemting som værneting.

Underskrifter

For den dataansvarlige (Navn / Virksomhed):

_____

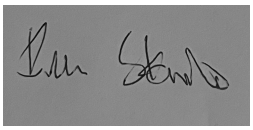
Navn

Titel:

Email:

Dato:

For databehandleren (CVR Intel):



Ivan Staub

CVR Intel

Dato: 24-07-2026

BILAG A — Oplysninger om behandlingen

A.1 Formålet med behandlingen

Levering af softwaretjenesten CVR Intel, herunder virksomhedssøgning, regnskabsanalyse, Lead Finder og overvågning af virksomheder. Behandlingen af personoplysninger sker udelukkende med henblik på at oprette og administrere den dataansvarliges brugerkonti, opbevare brugerskabt indhold og sikre tjenestens drift og sikkerhed.

A.2 Behandlingens karakter

Indsamling, opbevaring, visning, ændring og sletning af kontooplysninger og brugerskabt indhold i tilknytning til tjenestens levering. Der foretages ikke profilering eller automatiske afgørelser med retsvirkning for de registrerede.

A.3 Kategorier af registrerede

Den dataansvarliges medarbejdere og øvrige brugere med adgang til platformen.

A.4 Kategorier af personoplysninger

Der behandles udelukkende almindelige personoplysninger, jf. artikel 6. Der behandles ingen særlige kategorier af personoplysninger, jf. artikel 9, og ingen oplysninger om strafbare forhold, jf. artikel 10.

Kategori	Oplysninger	Beskyttelse
Kontooplysninger	Navn, e-mailadresse	Krypteret på feltniveau (AES-256-GCM)
Adgangskoder	Adgangskode	Hashet (bcrypt) — ikke reversibel
Brugerskabt indhold	Navne på lister, overvågningsporteføljer, notifikationer	Krypteret på feltniveau (AES-256-GCM)
Tekniske logs	IP-adresse, user agent, tidsstempel	Klartekst, automatisk tidsbegrænset sletning
Betalingsreference	Kunde-ID fra Stripe	Klartekst. Ingen kortoplysninger opbevares

Bemærk: E-mailadresse og navn opbevares tillige som pseudonymiserede opslagsværdier (SHA-256) af hensyn til databasesøgning. Disse værdier udgør

fortsat personoplysninger.

A.5 Oplysninger der ikke er omfattet

Virksomhedsoplysninger fra CVR-registret (herunder virksomhedsnavne, adresser, regnskabstal, ejerforhold og ledelsesoplysninger) behandles af databehandleren som selvstændig dataansvarlig på grundlag af offentligt tilgængelige registerdata. Denne behandling er ikke omfattet af nærværende aftale.

A.6 Anvendelse af kunstig intelligens

Tjenesten anvender OpenAI's sprogmodel (GPT) til generering af beskrivende regnskabsanalyser.

Der overføres udelukkende:

- numeriske nøgletal fra offentligt tilgængelige årsrapporter
- en bucketet branche- og størrelseskategori (fx "Handel og distribution", "10–49 medarbejdere")

Der overføres ikke:

- virksomhedsnavne eller CVR-numre
- brugeridentifikatorer, e-mailadresser eller sessionsoplysninger
- brugerskabt indhold, herunder lister og overvågningsporteføljer

Da der ikke overføres personoplysninger til OpenAI, optræder OpenAI ikke som underdatabehandler i denne aftales forstand og fremgår derfor ikke af Bilag B.

Behandlingen sker via OpenAI's API-vilkår, hvor input og output ikke anvendes til træning af OpenAI's modeller. Forespørgsler og svar logges ikke af databehandleren ud over den genererede analyse, som gemmes tilknyttet den pågældende årsrapport.

A.7 Behandlingens varighed

Behandlingen finder sted, så længe den dataansvarliges konto er aktiv. Ved sletning af konto slettes personoplysninger straks, jf. Bilag C, punkt 7.

A.8 Adgang for eksterne AI-klienter (MCP)

Tjenesten kan efter den dataansvarliges eksplicitte samtykke tilkobles eksterne AI-klienter (fx Claude, ChatGPT, Cursor) via Model Context Protocol (MCP). Adgangen aktiveres via et OAuth 2.1-flow på *app.cvrintel.dk/oauth/mcp-grant*, hvor den dataansvarlige eksplicit godkender forbindelsen, og kan tilbagekaldes når som helst.

Hvilke data overføres til AI-klienten via MCP:

- Offentlige registerdata fra CVR (Danmark) og Brønnøysundregistrene (Norge): CVR-nummer / organisasjonsnummer, virksomhedsnavn, adresse, branche, status, selskabsform, regnskabstal og beregnede nøgletal.
- Aggregerede ledelsesoplysninger (antal medlemmer + roller — fx "1 direktør, 2 bestyrelsesmedlemmer"), uden navne eller person-ID'er.
- Metadata-flags til nedstrøms GDPR-vurdering: `contains_personal_data`, `advertising_protection`, `data_updated_at`, evt. `stale_data_warning`.
- Den dataansvarliges egne overvågningsdata (hvilke virksomheder brugeren følger, tilføjelses-tidspunkter, hændelseskategorier).
- Et `web_link` til den fulde virksomhedsprofil i CVR Intel-webappen.

Hvilke data overføres IKKE til AI-klienten via MCP:

- Navne eller person-ID'er på ledelsesmedlemmer og reelle ejere.
- Direkte kontaktoplysninger (telefon, e-mail).
- Gadeadresse for sole-trader-shaped virksomheder (I/S, PMV, enkeltmandsvirksomhed) — kun de generelle registerdata mærkes som personoplysning.
- Selve teksten fra notifikationer om overvågede virksomheder (kun hændelseskategori og tidspunkt).
- Betalingsoplysninger, adgangskoder, session-tokens eller andre kontooplysninger.
- API-nøgler, som kun opbevares hos den dataansvarlige og videresendes krypteret som Bearer-header pr. forespørgsel.

Underdatabehandler-status: Den valgte AI-klient (fx Anthropic, OpenAI, Cursor) er valgt af den dataansvarlige og indgået aftale med af den dataansvarlige selv. AI-leverandøren er derfor *ikke* databehandlerens underdatabehandler i denne aftales forstand, og fremgår ikke af Bilag B. Den dataansvarlige er selvstændigt ansvarlig for sin videre behandling hos den valgte AI-leverandør, herunder for eventuel indgåelse af databehandleraftale med AI-leverandøren, overholdelse af CVR-lovens § 19 (reklamebeskyttelse) og øvrige forpligtelser efter GDPR.

Sikkerhedsforanstaltninger: MCP-serveren authenticerer hver forespørgsel individuelt via Bearer-token krypteret med AES-256-GCM. Fejl-logs indeholder alene kategori-navn (fx "auth", "quota", "upstream") og aldrig fritekst fra forespørgsel eller svar. Der føres ikke persistent lagring af data, der passerer MCP-serveren, ud over den korte OAuth-session (30 dages standard-TTL).

Ansvarsafgrænsning: Data udleveret via MCP-serveren behandles hos den eksterne AI-leverandør efter dennes egne vilkår. Databehandleren kan ikke garantere lagring, sletning eller no-training hos AI-leverandøren, og den dataansvarlige må selv vurdere den valgte leverandørs egnethed.

BILAG B — Godkendte underdatabehandlere

Den dataansvarlige har godkendt anvendelsen af følgende underdatabehandlere:

Underdatabehandler	Formål	Lokation	Grundlag
Hetzner Online GmbH	Hosting, database og backup	Tyskland	Intern EU
Stripe Payments Europe Ltd.	Betalingsafvikling og abonnementsadministration	Irland	Intern EU
Curanet A/S	Afsendelse af transaktionsmails	Danmark	Intern EU
Cloudflare Germany GmbH	CDN, DNS og beskyttelse mod netværksangreb	EU	Se note

Noter

- Hetzner Online GmbH er certificeret efter ISO/IEC 27001. Samtlige servere, databaser og backups er placeret i Tyskland.
- Stripe Payments Europe Ltd. behandler betalinger via Stripe Checkout. Kortoplysninger passerer ikke databehandlerens systemer og opbevares ikke af databehandleren.
- Cloudflare Germany GmbH leverer netværkslag foran tjenesten. Trafik dirigeres via Cloudflares europæiske infrastruktur. Cloudflare, Inc. er koncernmoderselskab og er certificeret under EU-US Data Privacy Framework. I det omfang der måtte ske behandling uden for EU/EØS, sker dette på grundlag af EU-Kommissionens standardkontraktbestemmelser (SCC'er) samt Cloudflares tilslutning til EU-US Data Privacy Framework.
- OpenAI anvendes som ekstern tjeneste til generering af regnskabsanalyser, men modtager ikke personoplysninger og optræder derfor ikke som underdatabehandler i denne aftales forstand. Datasnitfladen er beskrevet i Bilag A, punkt A.6.
- Eksterne AI-klienter (fx Anthropic Claude, OpenAI ChatGPT, Cursor) som den dataansvarlige efter eget valg måtte tilkoble via MCP-integrationen, er ikke databehandlerens underdatabehandlere. Den dataansvarlige er selvstændigt ansvarlig for sit forhold til den valgte AI-leverandør. Datasnitfladen er beskrevet i Bilag A, punkt A.8.

Ændringer i ovenstående oversigt varsles skriftligt over for den dataansvarlige med mindst 30 dages varsel, jf. aftalens punkt 5.2.

BILAG C — Tekniske og organisatoriske sikkerhedsforanstaltninger

Følgende foranstaltninger er gennemført i medfør af databeskyttelsesforordningens artikel 32.

1. Kryptering

- Data under transmission beskyttes med TLS 1.2 eller nyere på samtlige forbindelser.
- Personoplysninger og brugerskabt indhold krypteres på feltniveau i databasen med AES-256-GCM. Der anvendes autentificeret kryptering med unik tilfældig nonce pr. post, hvilket beskytter både fortrolighed og integritet.
- Krypteringsnøglen opbevares uden for applikationskoden i en beskyttet miljøkonfiguration og indgår ikke i versionsstyring.
- Adgangskoder opbevares aldrig i klartekst. Der anvendes bcrypt via PHP's password_hash() med automatisk salt.

2. Adgangskontrol og autentifikation

- Ratebegrænsning på loginforsøg med registrering og blokering ved gentagne mislykkede forsøg.
- Sessionsstyring med automatisk udløb af inaktive sessioner.
- Administrativ adgang til produktionsmiljø og database er begrænset til én navngiven person hos databehandleren.
- To-faktor-autentificering er ikke implementeret på nuværende tidspunkt. TOTP-baseret to-faktor-autentificering er planlagt implementeret i 4. kvartal 2026.

3. Logisk adskillelse

Den dataansvarliges data adskilles fra øvrige kunders data på applikationsniveau. Samtlige databaseforespørgsler er bundet til en autentificeret brugeridentifikator.

4. Infrastruktur og fysisk sikkerhed

- Hosting sker hos Hetzner Online GmbH i datacenter beliggende i Tyskland.

- Hetzner Online GmbH er certificeret efter ISO/IEC 27001, og fysisk adgangskontrol, brandsikring og redundant strømforsyning varetages af leverandøren.
- Der finder ingen behandling sted uden for EU/EØS, jf. Bilag B.

5. Netværkssikkerhed

- Der anvendes Cloudflare som netværkslag foran tjenesten med beskyttelse mod distribuerede overbelastningsangreb (DDoS).
- Applikationen er ikke direkte eksponeret mod internettet uden dette lag.

6. Backup

- Der foretages daglig backup af databasen.
- Backups opbevares hos Hetzner Online GmbH inden for EU.

7. Logning og sletning

Tekniske logs slettes automatisk ved planlagte opgaver efter følgende frister:

Datatype	Opbevaringsperiode	Grundlag
Sessionsdata (IP, user agent)	30 dage	Legitim interesse — drift
Sikkerhedshændelser	90 dage	Legitim interesse — sikkerhed
Loginforsøg	30 dage	Legitim interesse — sikkerhed
To-faktor koder (metadata: IP, user agent)	30 dage	Legitim interesse — sikkerhed
Notifikationer (læste)	30 dage	Legitim interesse — dataminimering
Notifikationer (ulæste)	90 dage	Legitim interesse — dataminimering
Kontooplysninger og brugerskabt indhold	Slettes ved kontosletning	Aftale
Bogføringspligtige oplysninger	5 år	Retlig forpligtelse (bogføringsloven)

8. Betalingsdata

- Betalinger håndteres via Stripe Checkout. Kortoplysninger indtastes direkte hos Stripe og passerer ikke databehandlerens systemer.
- Databehandleren opbevarer alene et kundereference-ID udstedt af Stripe.

- Databehandleren er som følge heraf omfattet af den laveste PCI-DSS-kategori (SAQ A).

9. Sletning ved ophør

- Den dataansvarlige kan til enhver tid slette sin konto via tjenestens brugergrænseflade.
- Ved kontosletning slettes samtlige personoplysninger og brugerskabt indhold umiddelbart og uigenkaldeligt.
- Opsigelse af abonnement medfører alene nedgradering til gratis adgangsniveau. Kontoen og tilhørende data bevares, indtil den dataansvarlige aktivt sletter kontoen.
- Konti uden aktivitet i 24 måneder slettes efter forudgående varsel pr. e-mail.
- Bogføringspligtige transaktionsoplysninger opbevares i 5 år, jf. aftalens punkt 8.3.

10. Håndtering af sikkerhedsbrud

- Ved konstatering af brud på persondatasikkerheden underrettes den dataansvarlige uden unødig forsinkelse.
- Underretningen indeholder de oplysninger, der fremgår af aftalens punkt 7.2.
- Databehandleren bistår den dataansvarlige med anmeldelse til Datatilsynet og eventuel underretning af registrerede.

11. Organisatoriske foranstaltninger

- Databehandleren drives af én person, som er underlagt tavshedspligt.
- Der føres fortegnelse over behandlingsaktiviteter, jf. artikel 30, stk. 2.
- Ved anvendelse af eventuelle fremtidige medarbejdere eller underleverandører indgås skriftlig fortrolighedsaftale forud for adgang til produktionsdata.

Version 1.1 · Bilag C opdateres i takt med ændringer i tjenestens tekniske opsætning. Sikkerhedsniveauet forringes ikke som følge af sådanne opdateringer.