

JURIDISK

Databehandleraftale

Denne databehandleraftale ("Aftalen") indgås mellem den dataansvarlige, som er den kunde, der er angivet i Ordreformularen ("Kunden"), og databehandleren Kompas Indsigt ApS, CVR: 46307739, Glentevej 16, 4600 Køge ("Databehandleren"). Aftalen vedrører Databehandlerens behandling af personoplysninger på vegne af Kunden i forbindelse med levering af Kompas-platformen ("Platformen") i henhold til samarbejdsaftalen mellem parterne, bestående af Ordreformularen og de Generelle Vilkår ("Hovedaftalen").

Aftalen er struktureret efter Datatilsynets standardkontraktbestemmelser for databehandleraftaler (GDPR art. 28, stk. 3) og svarer til standarddatabehandleraftalen i Kompas' compliance-pakke, version 1.0 af 15.08.2026.

1. Baggrund og formål

1.1 Aftalen fastsætter de rettigheder og forpligtelser, der gælder, når Databehandleren behandler personoplysninger på vegne af Kunden.

1.2 Aftalen er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 (databeskyttelsesforordningen, "GDPR") samt databeskyttelsesloven (LBK nr. 289 af 22/02/2024).

1.3 I forbindelse med leveringen af Platformen behandler Databehandleren personoplysninger på vegne af Kunden i overensstemmelse med Aftalen.

1.4 Aftalen har forrang for eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne for så vidt angår behandling af personoplysninger.

1.5 Bilag A-D er en integreret del af Aftalen: Bilag A (oplysninger om behandlingen), Bilag B (underdatabehandlere), Bilag C (instruks om behandlingssikkerhed og opbevaring), Bilag D (bistand og procedurer).

2. Den dataansvarliges rettigheder og forpligtelser

2.1 Kunden er dataansvarlig og har ansvaret for, at behandlingen af personoplysninger sker inden for rammerne af GDPR og databeskyttelsesloven, herunder at der foreligger gyldigt behandlingsgrundlag, og at de registrerede har modtaget oplysning efter artikel 13 og 14.

2.2 Kunden har ret og pligt til at træffe beslutning om, til hvilke formål og med hvilke hjælpemidler der må ske behandling, herunder beslutninger om opbevaringsperioder inden for lovgivningens rammer (jf. Bilag C).

2.3 Kunden er ansvarlig for, at de behandlinger, som Databehandleren instrueres i at foretage, har et retligt grundlag. For sociale tilbud omfatter dette bl.a. serviceloven (herunder dokumentationspligten i SEL § 148) og, for sundhedsfaglige optegnelser, autorisationsloven og journalføringsbekendtgørelsen.

3. Databehandleren handler efter instruks

3.1 Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra Kunden, medmindre behandling kræves i henhold til EU-ret eller national ret, som Databehandleren er underlagt. I så fald underretter Databehandleren Kunden om dette retlige krav inden behandlingen, medmindre den pågældende ret forbyder underretning af hensyn til vigtige samfundsinteresser.

3.2 Kundens instruks fremgår af Aftalen med bilag samt af Kundens konfiguration og brug af Platformen (herunder opsætning af moduler, roller, adgange og opbevaringsperioder). Instruks ud over dette skal være skriftlig.

3.3 Databehandleren underretter omgående Kunden, hvis en instruks efter Databehandlerens mening er i strid med GDPR eller databeskyttelsesretlige bestemmelser i anden EU-ret eller national ret.

4. Fortrolighed

4.1 Databehandleren sikrer, at kun personer, der aktuelt er autoriseret hertil, har adgang til de personoplysninger, der behandles på vegne af Kunden. Adgang begrænses til personer, for hvem adgang er nødvendig for at levere, drive og supportere Platformen.

4.2 Databehandlerens medarbejdere har ikke rutinemæssig adgang til Kundens data og tilgår alene Kundens data efter Kundens instruks, fx i forbindelse med support eller fejlsøgning.

4.3 Databehandleren sikrer, at personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt passende lovbestemt tavshedspligt.

4.4 Autorisationer gennemgås løbende og inddrages, når de ikke længere er nødvendige.

5. Behandlingssikkerhed

5.1 Databehandleren iværksætter, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene for fysiske personers rettigheder og frihedsrettigheder, passende tekniske og organisatoriske foranstaltninger, jf. GDPR artikel 32. Behandlingen omfatter særlige kategorier af personoplysninger (artikel 9), herunder helbredsoplysninger og oplysninger om sociale forhold, hvilket er afspejlet i sikkerhedsniveauet.

5.2 De implementerede foranstaltninger er beskrevet i Bilag C. Databehandleren kan opdatere foranstaltningerne, forudsat at sikkerhedsniveauet ikke derved forringes.

6. Anvendelse af underdatabehandlere

6.1 Databehandleren må ikke gøre brug af en underdatabehandler til opfyldelse af Aftalen uden forudgående generel skriftlig godkendelse fra Kunden.

6.2 Kunden giver ved Aftalens indgåelse generel godkendelse til brug af de underdatabehandlere, der er anført i Bilag B.

6.3 Databehandleren underretter Kunden skriftligt om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 dages varsel og giver derved Kunden mulighed for at gøre indsigelse, inden ændringen får virkning. Den til enhver tid gældende liste kan rekvireres hos Databehandleren.

6.4 Databehandleren pålægger underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af Aftalen, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller national ret, og forbliver fuldt ansvarlig over for Kunden for underdatabehandlerens opfyldelse af sine forpligtelser.

7. Overførsel til tredjelande

7.1 Personoplysninger, som Databehandleren behandler på vegne af Kunden, lagres som hovedregel i EU (jf. Bilag B: hosting, database og dokumentlager i EU/Frankfurt), og følsomme oplysninger (artikel 9) forlader ikke Databehandlerens EU-infrastruktur i forbindelse med Platformens tale-til-tekst, journal-strukturering og oplæsningsfunktioner, der drives som Databehandlerens egne tjenester i EU uden brug af tredjepart.

7.2 I det omfang en underdatabehandler er etableret i et tredjeland (USA), sker overførsel alene på et gyldigt overførselsgrundlag, jf. GDPR kapitel V: EU-Kommissionens standardkontraktbestemmelser (SCC) med de pågældende leverandører, suppleret af EU-U.S. Data Privacy Framework, hvor leverandøren er certificeret (Clerk, Sentry, GitHub). For Anthropic er SCC (Module 2) inkorporeret i leverandørens Commercial Terms.

7.3 Databehandleren gennemfører og vedligeholder Transfer Impact Assessments for tredjelandsoverførsler og revurderer disse ved ændringer i leverandørforhold eller retsgrundlag.

7.4 Ved overførsel af data til Anthropic (AI-indsigter, der alene aktiveres efter Kundens tilvalg) pseudonymiserer Databehandleren borgernes navne inden overførsel, og der overføres ikke fritekst med følsomme oplysninger.

8. Bistand til den dataansvarlige

8.1 Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt Kunden med passende tekniske og organisatoriske foranstaltninger med opfyldelse af Kundens forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder (GDPR kapitel III).

8.2 De registrerede (borgere, medarbejdere m.fl.) retter henvendelse til Kunden som dataansvarlig. Databehandleren leverer efter anmodning teknisk bistand, herunder eksport af den registreredes oplysninger i et struktureret, almindeligt anvendt og maskinlæsbart format, senest 5 arbejdsdage efter Kundens anmodning. Udlivering sker sikkert (krypteret arkiv med adgangskode fremsendt ad separat kanal). Se Bilag D.

8.3 Databehandleren bistår Kunden med at sikre overholdelse af forpligtelserne i GDPR artikel 32-36, herunder ved at stille dokumentation for de tekniske og organisatoriske foranstaltninger til rådighed, bistå ved konsekvensanalyser (DPIA) med et teknisk grundlag, som Kunden færdiggør, og bistå ved eventuel forudgående høring af Datatilsynet.

9. Underretning om brud på persondatasikkerheden

9.1 Databehandleren underretter Kunden uden unødigt forsinkelse, og så vidt muligt inden for 48 timer, efter at være blevet opmærksom på et brud på persondatasikkerheden, der vedrører Kundens data.

9.2 Underretningen skal så vidt muligt indeholde de oplysninger, Kunden skal bruge for at kunne opfylde sin anmeldelsespligt over for Datatilsynet inden 72 timer (GDPR artikel 33), herunder bruddets karakter, kategorier og omtrentligt antal berørte registrerede og registreringer, sandsynlige konsekvenser samt trufne og foreslåede foranstaltninger.

9.3 Databehandleren dokumenterer alle brud og bistår Kunden med opfølgning, herunder med en efterfølgende redegørelse for årsag og iværksatte foranstaltninger ved alvorlige hændelser.

10. Sletning og tilbagelevering af oplysninger

10.1 Ved ophør af tjenesterne vedrørende behandling af personoplysninger sletter Databehandleren personoplysningerne efter den procedure, der fremgår af Bilag C, medmindre EU-retten eller national ret foreskriver opbevaring. Kunden kan forud for sletning rekvirere en komplet eksport af sine data.

10.2 Sundhedsfaglige optegnelser er underlagt lovbestemt opbevaringspligt (mindst 5 år fra seneste optegnelse, jf. journalføringsbekendtgørelsen og autorisationsloven) og slettes ikke, før opbevaringspligten er udløbet, jf. GDPR artikel 17, stk. 3, litra b. Ansvar for fortsat opbevaring efter ophør aftales konkret ved offboarding.

10.3 Databehandleren bekræfter på Kundens anmodning skriftligt, at sletning er gennemført.

11. Revision og tilsyn

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

11.2 Tilsyn gennemføres som udgangspunkt ved, at Databehandleren årligt og ved væsentlige ændringer stiller opdateret dokumentation til rådighed (sikkerheds- og complianceoverblik, underdatabehandlerliste, beskrivelse af foranstaltninger). Fysisk eller udvidet inspektion varsles med mindst 20 arbejdsdage, gennemføres under rimelig hensyntagen til Databehandlerens driftsforhold og sker for Kundens regning, medmindre revisionen afdækker væsentlig misligholdelse.

11.3 Kunden kan tilsvarende føre tilsyn med behandlingen hos underdatabehandlere gennem Databehandleren.

12. Ikrafttræden, varighed og ophør

12.1 Aftalen træder i kraft ved parternes underskrift af Ordreformularen og gælder, så længe Databehandleren behandler personoplysninger på vegne af Kunden i henhold til Hovedaftalen. Har parterne underskrevet en særskilt databehandleraftale, træder den i stedet for denne version.

12.2 Ved Hovedaftalens ophør gælder Aftalen fortsat, indtil behandlingen er ophørt og oplysningerne slettet eller tilbageleveret i henhold til pkt. 10 og Bilag C.

12.3 Ved modstrid mellem Aftalen og Hovedaftalen har Aftalen forrang for så vidt angår behandling af personoplysninger.

Bilag A: Oplysninger om behandlingen

A.1 Formål: Levering af Kompas-platformen: en samlet driftsplatform for sociale tilbud, der omfatter visitation, faglig dokumentation og journalisering, medicin håndtering, vagtplanlægning, personale- og borgeradministration, økonomi, beskeder og rapportering.

A.2 Behandlingens karakter: Registrering, strukturering, opbevaring, fremvisning, eksport, pseudonymisering og sletning af oplysninger, som Kundens autoriserede brugere registrerer eller lader indlæse i Platformen, herunder automatiseret understøttelse (fx vagtplan-generering, tale-til-tekst med obligatorisk brugergodkendelse, regelbaserede indsigter). Behandlingen omfatter desuden udsendelse af driftsbeskeder pr. e-mail til Kundens brugere og medarbejdere som led i tjenesten (fx onboarding af nyoprettede brugere: velkomst og vejledning i brug af Platformen), når Kunden har aktiveret dette; sådanne beskeder indeholder ikke markedsføring, jf. Kundens instruks (pkt. 3.2), og enhver modtager kan framelde sig i beskeden.

A.3 Kategorier af registrerede:

- Borgere (beboere/deltagere i Kundens tilbud), herunder eventuelt mindreårige
- Kundens medarbejdere, vikarer og ledelse
- Borgeres kontakter (pårørende, værger, sagsbehandlere, sundhedspersoner)
- Personer i visitationsforløb, der ikke bliver indskrevet

A.4 Kategorier af personoplysninger:

- Almindelige oplysninger (art. 6): navn, kontaktoplysninger, ansættelses- og kontraktforhold, arbejdstider og fravær, planlægnings- og driftsdata, økonomiske oplysninger knyttet til borgerforløb (takst, budget, egenbetaling), stempelingstidspunkt med lokation (kun ved stempeling)
- Særlige kategorier (art. 9): helbredsoplysninger (journalnotater, medicin, sundhedsvurderinger, diagnoser), oplysninger om sociale forhold, oplysninger i magtanvendelses- og UTH-indberetninger, funktionsevnevurderinger
- Der behandles ikke CPR-numre i Platformens fritekst- og identifikationsfelter; Platformen afviser og scrubber CPR-mønstre (jf. Bilag C). Aktiveres integration til Det Fælles Medicinkort (FMK) på et senere tidspunkt, opdateres Aftalen forinden, jf. pkt. 6.3.

A.5 Varighed: Så længe Hovedaftalen består, og derefter indtil sletning i henhold til Bilag C.

Bilag B: Godkendte underdatabehandlere

Ved Aftalens indgåelse er følgende underdatabehandlere godkendt:

Underdatabehandler	Ydelse	Lokation for behandling	Overførselsgrundlag
Render Inc.	Hosting af applikation og egne AI-tjenester	EU (Frankfurt, Tyskland)	Behandling i EU
Neon (Databricks Inc.)	Database (PostgreSQL) inkl. backup	EU (eu-central-1, Frankfurt)	Behandling i EU
Cloudflare Inc. (R2)	Objektlager til dokumenter, krypteret at-rest	EU	Behandling i EU
Clerk Inc.	Login og adgangsstyring	USA	EU-U.S. DPF + SCC
Functional Software Inc. (Sentry)	Fejl- og ydelsesovervågning	Datalagring i EU; support-adgang fra USA	EU-U.S. DPF + SCC
GitHub Inc. (Microsoft)	Kildekode og CI/CD (ingen kundedata)	USA	EU-U.S. DPF + SCC
Anthropic PBC	AI-indsigter; alene aktiveret ved Kundens tilvalg; borgernavne pseudonymiseres, ingen følsom fritext overføres	USA	SCC (Module 2, Commercial Terms)
Expo (650 Industries, Inc.)	Push-notifikationer til mobilappen; behandler enheders push-tokens; beskedindhold er generisk og indeholder aldrig borger- eller helbredsdata (levering via Apple/Google som transmissionskanal)	USA	SCC
Linear Orbit Inc.	Håndtering af fejl- og feedbackrapporter fra Platformen (CPR scrubbes, navne pseudonymiseres)	USA	SCC
Resend	Transaktionelle statusmails om feedbackrapporter samt driftsbeskeder til Kundens brugere og medarbejdere (fx onboarding-vejledning), når Kunden har aktiveret dette; behandler navn og e-mailadresse	USA	SCC

Tale-til-tekst (dansk), journal-strukturering og oplæsning drives som Databehandlerens egne tjenester i Render-regionen i EU. Der anvendes ingen tredjepart hertil, og lydoptagelser gemmes ikke.

Ikke underdatabehandlere: Kundens egne systemleverandører, som Platformen integrerer til efter Kundens instruks (fx e-conomic, Business Central, Unicon, DataLøn, Danløn, Wolfpack), samt offentlige datakilder (Tilbudsportalen, DAWA, CVR).

Bilag C: Instruks om behandlingssikkerhed, opbevaring og sletning

C.1 Tekniske og organisatoriske foranstaltninger (art. 32):

- Kryptering i transit (TLS 1.2+, TLS 1.3 prioriteret) på alle forbindelser
- Kryptering at-rest i database og objektlager (AES-256) samt feltniveau-kryptering (AES-256-GCM med nøgleafledning og salt pr. række) af følsomme fritextfelter, herunder journalindhold, magtanvendelses- og UTH-indberetninger, sundhedsoplysninger og visitationsmateriale

- Tvungen tenant-isolation via Row Level Security i databasen; applikationen kører uden privilegeret databaserolle
- Rollebaseret adgangsstyring med scopes (organisation, afdeling, team, egen bruger) og mulighed for afgrænsning til enkeltborger-niveau; frontline-medarbejdere ser alene borgere, de er vagtsat på
- To-faktor-autentifikation: obligatorisk authenticator-app for ledere og administratorer; alle øvrige brugere verificeres med anden faktor (engangskode pr. e-mail) ved login fra nye enheder, og Kunden kan skærpe kravet til authenticator-app for alle brugere via organisationens sikkerhedspolitik; administrationsmiljø på adskilt identitetsinstans med obligatorisk to-faktor
- Uforanderlige (append-only) revisionsspor for ændringer i følsomme felter og for sletninger; opslagslog over adgang til borgerjournaler
- Automatisk afvisning og scrubning af CPR-numre i identifikations- og fritekstfelter
- Mobilapp med blokering af skærmoptagelse på følsomme skærme og biometrisk lås
- Kontinuert backup (point-in-time recovery) i EU med 7 dages gendannelsesvindue; beskyttet produktionsgren; årlig gendannelsestest
- Databasen forhindrer hard-delete af kernerdata fra applikationen (REVOKE DELETE); sundhedsdata er relationelt værnet mod sletning før opbevaringspligtens udløb
- Sikker udviklingsproces: kodegennemgang, automatiske tests, hemmelighedsscanning, afhængighedsovervågning, patch-SLA (kritisk 7 dage, høj 30 dage)

C.2 Opbevaring og sletning (Kundens instruks, konfigurerbar hvor angivet):

- Borgere: Ved sletning pseudonymiseres personhenførbare oplysninger straks; fuld sletning sker efter 90 dages karenperiode og alene efter Kundens bekræftelse
- Sundhedsfaglige optegnelser: opbevares mindst 5 år fra seneste optegnelse (journalføringsbekendtgørelsen § 35, autorisationsloven § 22) og slettes ikke med borgeren
- Medarbejdere: personoplysninger opbevares som udgangspunkt 5 år efter fratræden (konfigurerbart af Kunden); følsom fritekst (fx sygdomsårsager) scrubbes 90 dage efter fratræden, mens fraværsstrukturen bevares til time- og lønregnskab
- Visitationsoplysninger om personer, der ikke indskrives: slettes 180 dage efter sagens afslutning (konfigurerbart); inaktive henvendelser henlægges automatisk

- Regnskabsmateriale: 5 år fra regnskabsårets udløb (bogføringsloven § 12)
- Tekniske driftsdata: rå integrationssvar 7 dage; webhook-payloads 30 dage; fejløverbågningshændelser 90 dage
- Ved Aftalens ophør: Kundens organisation soft-slettes ved opsigelse og hard-slettes efter 90 dage efter dokumenteret procedure; forinden kan Kunden rekvirere komplet dataeksport. Lovpligtig opbevaring (C.2, 2. og 5. punkt) håndteres konkret ved offboarding

C.3 Sikkerhed hos underdatabehandlere: Databehandleren indgår databehandleraftaler med underdatabehandlere, gennemgår leverandørernes sikkerhedsdokumentation og fører liste med lokation og overførselsgrundlag.

Fejløverbågning er konfigureret, så følsomme oplysninger fjernes før indsendelse.

Bilag D: Bistand og procedurer

D.1 Registreredes rettigheder: Henvendelser fra registrerede rettes til Kunden, der verificerer identitet og besvarer

inden for GDPR's frister (30 dage, med mulighed for forlængelse). Databehandleren leverer på anmodning:

dataeksport (maskinlæsbar JSON samt læsbar udgave) inden 5 arbejdsdage, gennemførelse af godkendt sletning

(pseudonymisering straks, jf. Bilag C), samt teknisk bistand ved berigtigelse. Udløvelse af eksport sker som krypteret arkiv, hvor adgangskoden fremsendes ad en separat kanal. Hver anmodning logges af Databehandleren af hensyn til påvisningspligten.

D.2 Sletning kræver forudgående vurdering hos Kunden af lovbestemte opbevaringspligter (bogføringsloven, ansættelsesretlige regler, SEL § 148, forældelsesloven, journalføringsregler). Databehandleren eksekverer først efter Kundens dokumenterede godkendelse.

D.3 Brud på persondatasikkerheden: Underretning af Kunden uden unødigt forsinkelse med de oplysninger, der er nævnt i pkt. 9.2, samt bistand til anmeldelse og efterfølgende redegørelse.

D.4 Kontaktpunkter: Kunden: den kontaktperson, der er angivet i Ordreformular. Databehandleren:

kontakt@kompas-indsigt.dk

Senest opdateret: September 2026 · Den gældende version findes altid på <https://kompas-indsigt.dk/dpa>