Databehandleraftale

Version 2026-10-08 · efter strukturen i Datatilsynets standardkontraktsbestemmelser

1. Parterne

Den dataansvarlige: [VIRKSOMHEDENS NAVN], CVR [VIRKSOMHEDENS CVR], [VIRKSOMHEDENS ADRESSE] (herefter "den dataansvarlige" eller "virksomheden").

Databehandleren: AI Optimize ApS, CVR 44389908, Midtager 33, 2605 Brøndby, support@autora.nu (herefter "databehandleren" eller "Autora").

Parterne har indgået denne databehandleraftale (herefter "aftalen") for at opfylde kravene i artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 (databeskyttelsesforordningen, "GDPR").

2. Baggrund og formål

Databehandleren stiller en CRM-platform til rådighed som en onlinetjeneste (software as a service), hvor virksomheden registrerer og behandler oplysninger om sine kunder, kontaktpersoner, emner (leads), opgaver, aftaler, dokumenter, tilbud, underskrifter, tidsregistrering, mails og, når modulet er slået til, oplysninger til kundekendskabsprocedurer efter hvidvaskloven (KYC).

Virksomheden er dataansvarlig for de personoplysninger, den registrerer i platformen og lader sine kunder indsende via kundeportalen. Databehandleren behandler oplysningerne på virksomhedens vegne og efter dennes instruks.

Databehandleren er selvstændigt dataansvarlig for oplysninger om virksomhedens egne brugere (medarbejderkonti: navn, e-mail, adgangskode i hashet form, tofaktor-opsætning, login-tidspunkter og IP-adresser til begrænsning af forsøg), i det omfang behandlingen sker for at drive, sikre og fakturere tjenesten. Den behandling er beskrevet i databehandlerens privatlivspolitik.

3. Instruks

Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves efter EU-ret eller national ret, som databehandleren er underlagt. I så fald underretter databehandleren den dataansvarlige om retskravet før behandlingen, medmindre loven forbyder det af vægtige samfundsmæssige hensyn.

Instruksen er virksomhedens brug af platformens funktioner: oprettelse, redigering, visning, eksport, anonymisering og sletning af poster, afsendelse af mails og dokumenter, automatik, som virksomheden selv har slået til og sat op, kundeportalen, kundekendskabsprocedurer (herunder automatisk screening mod offentlige sanktions- og PEP-lister, når virksomheden har slået den til) og de integrationer (betaling, bogføring, CVR-opslag), som virksomheden selv forbinder. Databehandleren behandler ikke oplysningerne til egne formål.

Databehandleren underretter straks den dataansvarlige, hvis en instruks efter databehandlerens opfattelse strider mod GDPR eller anden databeskyttelsesret.

4. Kategorier af registrerede og personoplysninger (bilag A)

Behandlingen omfatter følgende kategorier af registrerede personer og oplysninger, afhængigt af de moduler, virksomheden har slået til:

- Virksomhedens kunder og deres kontaktpersoner: navn, adresse, e-mail, telefon, CVR-nummer, kundenummer, rolle, status, egne felter, noter, tidslinje og korrespondance (sendte mails).
- Emner (leads) fra webformular, booking og import: navn, firma, e-mail, telefon, besked og status.
- Brugere af kundeportalen: e-mail, adgangskode (kun hash), login-tidspunkter, beskeder, uploads og svar.
- Kundekendskab (KYC, hvidvaskloven), når modulet er slået til: svar på spørgeskema (herunder oplysning om politisk eksponerede personer), reelle ejere (navn og rolle), legitimationsdokumenter (fx pas, kørekort, sygesikringsbevis), CVR-udskrifter, resultater af screening mod offentlige sanktions- og PEP-lister (mulige match, medarbejdernes vurderinger og screeningsrapporter), risikovurdering, godkendelser og interne noter. Oplysninger om straffedomme behandles ikke; oplysninger om politisk eksponering er følsomme i deres kontekst og afskærmes til roller med adgang til KYC.
- Tilbud og underskrifter: modtagerens navn og e-mail, dokumentets indhold, underskriftens tidspunkt, IP-adresse og browseroplysninger som bevis.

- Betaling og bogføring, når modulerne er slået til: kundens navn og e-mail hos Stripe, beløb, status og datoer; posteringer og manglende bilag fra e-conomic.
- Tidsregistrering: medarbejderens registreringer pr. kunde og opgave.
- Virksomhedens egne medarbejdere som brugere: navn, e-mail, rolle, titel, telefon, tofaktor-status, handlinger i revisionssporet.

5. Databehandlerens forpligtelser

Databehandleren behandler kun oplysningerne til de formål og med de midler, instruksen angiver, og kun så længe aftalen gælder.

Databehandleren sikrer, at adgangen til personoplysninger er begrænset til de personer, der har brug for den for at levere og drive tjenesten (platform-administratorer), og at disse personer er underlagt fortrolighed.

Databehandleren fører en fortegnelse over de kategorier af behandling, der foretages på vegne af den dataansvarlige, jf. GDPR artikel 30, stk. 2.

6. Fortrolighed

Databehandleren sikrer, at de personer, der er autoriseret til at behandle personoplysninger på vegne af den dataansvarlige, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt. Fortrolighed gælder også efter ansættelsens eller samarbejdets ophør.

Databehandleren giver kun adgang til personoplysninger til personer, der har et arbejdsbetinget behov, og kan på anmodning dokumentere, hvem der har adgang til produktionsmiljøet.

7. Behandlingssikkerhed (bilag C)

Databehandleren gennemfører passende tekniske og organisatoriske foranstaltninger efter GDPR artikel 32 under hensyn til det aktuelle tekniske niveau, omkostningerne og behandlingens karakter, omfang, sammenhæng og formål samt risiciene for de registrerede. Foranstaltningerne omfatter mindst:

- Hosting i EU med adskillelse mellem virksomhederne i applikationslaget: alle forespørgsler filtreres på virksomhedens id, og adskillelsen afprøves automatisk i testkørsler.
-

Kryptering under transport (TLS) og kryptering af uploadede filer og gemte hemmeligheder i hvile (AES-256-GCM).

- Adgangskoder gemmes kun i hashet form; tofaktor-login (TOTP) kan slås til og kan kræves af roller med adgang til KYC; begrænsning af login- og loginlink-forsøg.
- Roller og rettigheder pr. virksomhed; KYC-oplysninger kan kun ses af roller med adgang til KYC, også i revisionsspor, beskeder, filer og eksport.
- Revisionsspor over ændringer af data og indstillinger (Indstillinger ’ Log) og eksport af det.
- Database og filer på vedvarende lager i EU med løbende sikkerhedskopiering, så oplysningerne kan genskabes efter et nedbrud, og afprøvning af gendannelsen.
- Overvågning af tjenesten (/api/health), fejlrapportering uden kundedata, og personlige engangslinks i mails, der maskeres i udbakken.
- Sletning og anonymisering pr. kunde, eksport af hele virksomhedens data og sletning af hele virksomheden som funktioner i produktet.

8. Underdatabehandlere (bilag B)

Den dataansvarlige giver en generel godkendelse til, at databehandleren anvender underdatabehandlere. Databehandleren indgår en skriftlig aftale med hver underdatabehandler, der pålægger denne de samme databeskyttelsesforpligtelser som denne aftale, og forbliver fuldt ansvarlig over for den dataansvarlige for underdatabehandlerens opfyldelse af dem.

Databehandleren underretter den dataansvarlige om påtænkte tilføjelser eller udskiftninger af underdatabehandlere mindst 30 dage, før ændringen får virkning (via en opdateret version af denne aftale i systemet og en besked til virksomhedens ejer). Den dataansvarlige kan gøre indsigelse inden ændringen; kan parterne ikke blive enige, kan den dataansvarlige opsige aftalen og eksportere og slette sine data, jf. punkt 12.

Følgende underdatabehandlere og modtagere anvendes ved aftalens indgåelse:

- Railway Corporation (underdatabehandler): Hosting af applikationen, databasen (Postgres) og de uploadede filer. Placering: Datacenter i EU (Railways region europe-west4, Amsterdam, Nederlandene). Overførsel:

Oplysningerne lagres i EU. Selskabet er amerikansk; eventuel adgang fra USA (fx support) sker på grundlag af EU-Kommissionens standardkontraktsbestemmelser (afgørelse 2021/914) i Railways databehandleraftale.

- Simply.com A/S (CVR 29412006) (underdatabehandler): Afsendelse af mails via platformens mailkonto (SMTP): modtageradresse, navn, emne og indhold. Placering: Danmark (EU). Overførsel: Ingen overførsel til tredjelande. Kun mails, der sendes via platformen. Sender virksomheden via sin egen mailkonto (SMTP), går mails direkte fra virksomhedens egen mailudbyder, som ikke er platformens underdatabehandler.
- Stripe Payments Europe, Ltd. / Stripe, Inc. (underdatabehandler): Betaling og abonnementer (modulet Betaling): kundens navn, e-mail og betalingsoplysninger behandles af Stripe; platformen gemmer kopier af status, beløb og datoer. Placering: Irland (EU); Stripe, Inc. i USA. Overførsel: Stripes egne overførselsgrundlag (EU-U.S. Data Privacy Framework og EU-Kommissionens standardkontraktsbestemmelser). Kun hvis virksomheden forbinder sin egen Stripe-konto. Stripe-kontoen er virksomhedens egen, og virksomhedens egen aftale med Stripe gælder for Stripes behandling; platformen behandler kun kopierne.
- Visma e-conomic A/S (underdatabehandler): Bogføringsdata (modulet Bogføring): posteringer og manglende bilag hentes fra kundens e-conomic-aftale. Placering: Danmark (EU). Overførsel: Ingen overførsel til tredjelande. Kun hvis virksomheden eller dens kunde forbinder en e-conomic-aftale. Aftalen er kundens egen; platformen henter kun det, automatikken bruger.
- Erhvervsstyrelsen (CVR) (modtager af opslag): Opslag af virksomhedsoplysninger ud fra CVR-nummer (KYC og kundeoprettelse). Placering: Danmark (offentlig myndighed). Overførsel: Ingen overførsel til tredjelande. Kun CVR-nummeret (eller et navn) sendes ved opslaget. Erhvervsstyrelsen er en offentlig myndighed og ikke en underdatabehandler; opslaget kræver virksomhedens egen system-til-system-adgang.
- cvrapi.dk (Online Gateway ApS, CVR 36421231) (modtager af opslag): Reserveopslag af offentlige virksomhedsdata (navn, adresse, branche) ud fra CVR-nummer eller navn. Placering: Danmark. Overførsel: Ingen overførsel til tredjelande. Kun CVR-nummeret eller det søgte navn sendes; der sendes aldrig oplysninger om personer.

9. Overførsel til tredjelande

Personoplysninger lagres og behandles som udgangspunkt i EU/EØS. Overførsel til et tredjeland sker kun via de underdatabehandlere, der er nævnt i punkt 8, og kun på et gyldigt overførselsgrundlag efter GDPR kapitel V (EU-U.S. Data Privacy Framework eller EU-Kommissionens standardkontraktsbestemmelser med fornødne supplerende foranstaltninger).

Databehandleren overfører ikke oplysninger til tredjelande på eget initiativ og uden instruks i øvrigt.

10. Bistand til den dataansvarlige

Databehandleren bistår, under hensyn til behandlingens karakter og så vidt muligt gennem funktioner i produktet, den dataansvarlige med at opfylde dennes forpligtelser til at besvare anmodninger om udøvelse af de registreredes rettigheder (indsigt, berigtigelse, sletning, begrænsning, dataportabilitet og indsigelse): eksport pr. kunde, anonymisering og sletning pr. kunde, kundeportalen, hvor registrerede selv ser og retter deres oplysninger, og revisionssporet.

Databehandleren bistår desuden den dataansvarlige med at sikre overholdelse af GDPR artikel 32-36 (sikkerhed, underretning om brud, konsekvensanalyser og forudgående høring) med de oplysninger, databehandleren råder over.

Databehandleren underretter uden unødig forsinkelse og senest 48 timer efter at være blevet opmærksom på det den dataansvarlige om brud på persondatasikkerheden, der berører virksomhedens oplysninger, med de oplysninger, der er nødvendige for, at den dataansvarlige kan anmelde bruddet til Datatilsynet (artikel 33) og underrette de registrerede (artikel 34). Underretning sker til virksomhedens ejer og administratorer på deres e-mail og i systemet.

11. Revision og tilsyn

Databehandleren stiller alle oplysninger til rådighed, der er nødvendige for at påvise overholdelse af GDPR artikel 28 og denne aftale, og giver mulighed for og bidrager til revisioner, herunder inspektioner, foretaget af den dataansvarlige eller en revisor bemyndiget af den dataansvarlige.

Revision varsles med mindst 30 dage og gennemføres i almindelig arbejdstid uden unødig forstyrrelse af driften, højst én gang årligt, medmindre der er konkret mistanke om brud. Den dataansvarlige bærer egne omkostninger;

databehandlerens rimelige omkostninger ved revisioner ud over den årlige kan faktureres efter aftale. Som dokumentation stiller databehandleren først sin beskrivelse af sikkerhedsforanstaltninger, underdatabehandleraftaler og eventuelle uafhængige revisionserklæringer til rådighed.

12. Sletning og tilbagelevering ved ophør (bilag D)

Ved aftalens ophør kan den dataansvarlige selv eksportere alle sine data (Indstillinger ’ Data og test ’ eksport af alle data og alle filer) og derefter slette virksomheden i systemet. Sletning af virksomheden fjerner alle rækker og filer med det samme; kopier i sikkerhedskopier slettes, efterhånden som sikkerhedskopierne udløber.

Har den dataansvarlige ikke selv slettet virksomheden senest 30 dage efter ophøret, sletter databehandleren oplysningerne efter skriftligt varsel til virksomhedens ejer, medmindre EU-ret eller national ret kræver fortsat opbevaring.

Den dataansvarliges egne opbevaringspligter (fx hvidvasklovens § 30 om kundekendskabsoplysninger i 5 år efter forretningsforbindelsens ophør og bogføringslovens krav) påhviler den dataansvarlige, som skal eksportere oplysningerne, før virksomheden slettes.

Databehandleren bekræfter sletningen skriftligt på anmodning.

13. Ansvar

Parternes ansvar følger GDPR artikel 82 og dansk rets almindelige regler. Databehandleren er ansvarlig for skade forårsaget af behandling, hvor databehandleren ikke har opfyldt de forpligtelser, der specifikt er rettet mod databehandlere, eller har handlet uden for eller i strid med den dataansvarliges lovlige instruks.

14. Varighed og ophør

Aftalen gælder, så længe databehandleren behandler personoplysninger på vegne af den dataansvarlige, og kan ikke opsiges særskilt fra brugen af tjenesten. Den ophører, når den dataansvarlige har slettet sin virksomhed i systemet, eller når databehandleren har slettet oplysningerne efter punkt 12.

Ændres aftalen, udgives en ny version med ny dato i systemet. Virksomhedens ejer bliver bedt om at acceptere den nye version; den hidtidige version gælder, indtil den nye er accepteret. Accepterer virksomheden ikke en ny version, kan hver part opsige med 30 dages varsel, og punkt 12 finder anvendelse.

15. Accept

Aftalen accepteres elektronisk af en ejer af virksomheden i systemet (ved oprettelsen af virksomheden eller under Indstillinger ’ Virksomhed ’ Databehandleraftale). Systemet registrerer aftalens version, tidspunktet, den accepterende brugers navn og e-mail samt IP-adressen, og skriver accepten i virksomhedens revisionsspor. Registreringen vises for virksomhedens ejer og administratorer og kan hentes som PDF sammen med aftalens tekst.

Spørgsmål om aftalen rettes til support@autora.nu.