UDKAST · GDPR ART. 28

Databehandleraftale

Mellem SimpleEntra (databehandler) og den dataansvarlige kunde, indgået i henhold til Persondataforordningen — særligt artikel 28.

STATUS

Udkast

VERSION

1.0

SENEST OPDATERET / UPDATED

2026-06-15

LOVVALG / JURISDICTION

Dansk ret · Københavns Byret

> *Dette dokument er et udkast. Det skal granskes af kundens og databehandlerens juridiske rådgivere før underskrift. Felter markeret [...] udfyldes ved kontraktindgåelse.*

1. Parter

1.1 Databehandler

Navn	SimpleEntra (leveret af [Selskab, CVR-nr.])
Adresse	[Adresse — udfyldes ved underskrift]
Kontakt for databehandling	hello@simpleentra.com
Kontakt for privacy	hello@simpleentra.com
DPO	Ikke obligatorisk, jf. art. 37; ovenstående kontakt anvendes

1.2 Dataansvarlig

Navn	[Kundens juridiske navn] ("Kunden")
CVR-nr.	[CVR/registreringsnr.]
Adresse	[Adresse]
Kontaktperson	[Navn, titel, e-mail]

Databehandler og Dataansvarlig benævnes hver for sig "Part" og samlet "Parterne".

2. Definitioner

I denne aftale anvendes følgende definitioner, der svarer til GDPR art. 4:

- Personoplysninger: Enhver form for information om en identificeret eller identificerbar fysisk person.
- Behandling: Enhver aktivitet eller række af aktiviteter — med eller uden brug af automatisk behandling — som personoplysninger gøres til genstand for.
- Registrerede: De fysiske personer, hvis personoplysninger behandles.
- Dataansvarlig: Den fysiske eller juridiske person, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger.
- Databehandler: En fysisk eller juridisk person, der behandler personoplysninger på den dataansvarliges vegne.
- Underdatabehandler (sub-processor): En anden databehandler, som Databehandler benytter til at udføre specifikke behandlingsaktiviteter på vegne af den dataansvarlige.
- Brud på persondatasikkerheden: Et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger.
- Persondataforordningen / GDPR: Forordning (EU) 2016/679.

3. Genstand og varighed

3.1 Aftalens genstand

Databehandler leverer SimpleEntra, en SaaS-platform der læser konfiguration og brugerdata fra Kundens Microsoft 365-tenant via read-only Microsoft Graph-tilladelser med det formål at vurdere sikkerhedens modenhed, generere risiko-rapporter til Kundens ledelse og tilbyde anbefalinger om bedre konfiguration.

3.2 Varighed

Aftalen er gyldig så længe Kunden har et aktivt abonnement på SimpleEntra. Aftalen ophører automatisk ved abonnementets ophør. Data slettes senest 30 dage efter ophør (se § 14).

4. Formål med behandlingen

Behandlingens formål er begrænset til:

- Sikkerheds-vurdering af Kundens Microsoft 365-tenant — herunder evaluering af Conditional Access policies, MFA-dækning, privilegerede roller, app-registreringer, enhedscompliance og licens-tildelinger mod kendte baselines (CIS, CISA SCuBA og lignende).
- Generering af ledelsesrapporter der oversætter tekniske fund til forretningsrisiko-sprog.
- Anbefalinger om konfigurations-forbedringer på baggrund af de identificerede huller.
- Trend-analyse der viser ændringer i sikkerheds-modenhed over tid.
- AI-assisteret natursprogs-fortolkning af tekniske fund (se § 5.6 og § 9).

Databehandler må ikke behandle personoplysninger til andre formål end dem, der er angivet i dette afsnit, medmindre Dataansvarlig giver skriftlig forudgående instruktion herom.

5. Behandlingens art

5.1 Read-only adgang

Databehandler tildeles udelukkende læseadgang til Kundens Microsoft 365-tenant via Microsoft Graph. Der er ingen skrive- eller slette-rettigheder.

5.2 Ingen ændringer i kundens systemer

Databehandler foretager ingen ændringer i Kundens Microsoft 365-konfiguration. Anbefalinger leveres som rapporter — gennemførelse heraf er Kundens eget ansvar.

5.3 Ingen adgang til indhold

Databehandler læser ikke indholdet af e-mails, kalendere, OneDrive-filer, SharePoint-dokumenter, Teams-beskeder eller andet brugergenereret indhold. Tilladelser som Mail.Read, Files.Read.All eller ChatMessage.Read indgår ikke i tilladelsessættet.

5.4 Pseudonymisering og 3-tier data-strategi

Kunden vælger hvilken datakategori der lagres hos Databehandler:

TIER	HVAD GEMMES	ANVENDELSE

Snapshot	Kun konklusioner og tællere — ingen rå rows	Default; minimal databehandling
Pseudonymiseret	Rå rows med tokens i stedet for UPN/e-mail/IP	Drill-down uden direkte identifikation
Fuld	Rå data i klartekst	Detaljeret analyse — kræver eksplicit aftale

Kunden kan til enhver tid skifte tier i portalen. Skift til lavere tier medfører øjeblikkelig sletning af data i højere tiers.

5.5 Audit-spor i kundens egen tenant

Hvert Microsoft Graph-kald som Databehandler foretager, logges automatisk i Kundens egen Entra ID under Sign-In Logs / Audit Logs. Kunden ejer dette audit-spor og kan til enhver tid verificere Databehandlers aktivitet.

5.6 AI-anvendelse

Databehandler anvender Anthropic Claude API til at generere natursprogs-resuméer og "værste tænkelige hændelse"-scenarier. Før data sendes til Anthropic, pseudonymiseres alle identifikatorer (UPN, e-mail, IP, firmanavn, GUID). Anthropic anvender ikke API-input til træning, og data-retention er slukket via API-konfigurationen.

6. Kategorier af personoplysninger og registrerede

6.1 Kategorier af personoplysninger

Databehandler behandler følgende kategorier af personoplysninger:

- Identifikatorer: User Principal Names (UPN), e-mail-adresser, display-navne, Microsoft tenant-id, objekt-id'er
- Login-metadata: IP-adresser, geo-lokation, sign-in-tidspunkter, klient-app, success/failure-status
- Konfigurations-data: Conditional Access policies, MFA-registrering, app-registreringer, role-tildelinger, license-tildelinger, enhedscompliance-status
- Aggregerede tællere og scores

Databehandler behandler ikke særlige kategorier af personoplysninger (art. 9 GDPR) eller oplysninger om straffedomme eller lovovertrædelser (art. 10 GDPR).

6.2 Kategorier af registrerede

- Medarbejdere hos Kunden (Microsoft 365-brugere)
- Eksterne gæstekonti i Kundens Microsoft 365-tenant
- Administratorer med privilegerede roller

7. Databehandlerens forpligtelser (GDPR art. 28 stk. 3)

7.1 Instruksbundethed

Databehandler må kun behandle personoplysninger efter dokumenteret instruktion fra Dataansvarlig — herunder med hensyn til overførsler til tredjelande. Denne aftale (med tilhørende dokumentation af scope, formål og sub-processors) udgør Dataansvarliges dokumenterede instruktion.

7.2 Fortrolighed

Databehandler sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er undergivet en passende lovbestemt tavshedspligt.

7.3 Sikkerhedsforanstaltninger

Databehandler træffer alle nødvendige foranstaltninger som krævet i henhold til GDPR art. 32. Specifikke foranstaltninger er beskrevet i § 9.

7.4 Underdatabehandlere

Databehandler engagerer ikke andre databehandlere uden Dataansvarliges forudgående generelle eller specifikke skriftlige tilladelse. Se § 8.

7.5 Bistand med registreredes rettigheder

Databehandler bistår — i det omfang det er muligt under hensyntagen til behandlingens art — Dataansvarlig med passende tekniske og organisatoriske foranstaltninger med opfyldelse af Dataansvarliges forpligtelser til at besvare anmodninger om udøvelse af de registreredes rettigheder. Se § 11.

7.6 Bistand med sikkerhed, brud, DPIA og forudgående høring

Databehandler bistår Dataansvarlig med at overholde forpligtelser i henhold til GDPR art. 32-36, herunder DPIA og forudgående høring af tilsynsmyndigheden.

7.7 Tilbagelevering og sletning

Ved aftalens ophør sletter eller tilbageleverer Databehandler — efter Dataansvarliges valg — alle personoplysninger og sletter eksisterende kopier, medmindre EU-ret eller national ret kræver opbevaring. Se § 14.

7.8 Audit-rettigheder

Databehandler stiller alle oplysninger, der er nødvendige for at påvise overholdelse af forpligtelserne i art. 28, til rådighed for Dataansvarlig og giver mulighed for og bidrager til audits. Se § 13.

7.9 Underretning ved ulovlig instruktion

Databehandler underretter omgående Dataansvarlig, hvis Databehandler vurderer, at en instruktion er i strid med GDPR eller anden EU- eller medlemsstats databeskyttelseslovgivning.

8. Underdatabehandlere (sub-processors)

8.1 Generel tilladelse

Dataansvarlig giver hermed Databehandler generel tilladelse til at anvende underdatabehandlere som angivet i § 8.3. Databehandler er ansvarlig for, at underdatabehandlere overholder forpligtelser tilsvarende dem, der påhviler Databehandler i denne aftale, herunder kravene i GDPR art. 28 stk. 4.

8.2 Procedure ved ændring

Databehandler underretter Dataansvarlig skriftligt mindst 14 dage før materielle ændringer i listen over underdatabehandlere (tilføjelse, udskiftning eller fjernelse). Dataansvarlig kan inden for varsel-perioden gøre indsigelse mod ændringen. Ved indsigelse drøfter Parterne en alternativ løsning; hvis enighed ikke kan opnås, kan Dataansvarlig opsige aftalen med øjeblikkelig virkning og uden vederlag.

8.3 Aktuelle underdatabehandlere

NAVN	FORMÅL	LOKATION	SIKKERHED
Supabase Inc.	Database (PostgreSQL) + Auth	eu-central-1 (Frankfurt, DE)	AES-256 at rest, TLS in transit, RLS
Vercel Inc.	Web-hosting + cron-jobs + edge	Frankfurt (fra1)	TLS, krypterede env-variabler
Anthropic PBC	AI (Claude API) — KUN værste-tænkelige-hændelse-scenarier og resuméer; input pseudonymiseres altid	USA (retention slukket, SCCs)	Zero retention via API, SCC-aftaler
Resend Inc.	E-mail-levering (transaktionel)	USA (SCCs)	TLS; ingen længere lagring end nødvendigt
Cloudflare Inc.	DNS + DDoS-beskyttelse	Globalt CDN	TLS-terminering; ingen application data lagres
Microsoft Corp.	Graph API mod Kundens egen tenant; vi læser herfra og gemmer ikke hos Microsoft	Kundens valg af Microsoft-region	Kundens egen aftale med Microsoft

9. Sikkerhedsforanstaltninger (GDPR art. 32)

Databehandler implementerer passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der svarer til risikoen for de registrerede. Foranstaltningerne er bl.a. inspireret af ISO/IEC 27002 og NIST CSF.

9.1 Kryptering

- At rest: AES-256 via AWS KMS (Supabase Postgres).
- In transit: TLS 1.2+ mellem alle komponenter.

9.2 Adgangskontrol

- Multi-factor authentication (TOTP) er obligatorisk for alle Databehandlers administratorer.
- Super-admins listes i tabellen app_admins og auditeres løbende.
- Kundens tenant-data tilgås udelukkende via service_role_key over server-side actions — ikke direkte fra browseren.
- Adgangstokens til Microsoft Graph hentes frisk ved hvert kald og gemmes ikke permanent.

9.3 Audit-log

Alle administrative handlinger logges i tabellen admin_actions med tidsstempel, bruger-id og handlingsbeskrivelse. Logs opbevares i mindst 12 måneder.

9.4 Read-only Graph-permissions

Databehandler anvender udelukkende read-only Microsoft Graph-tilladelser (jf. § 5.1). Tilladelses-sættet dokumenteres i særskilt teknisk bilag og offentliggøres på simpleentra.com/sadan-virker-det.

9.5 3-tier data-strategi

Kunden vælger lagrings-tier (Snapshot / Pseudonymiseret / Fuld) jf. § 5.4 og kan til enhver tid sænke tier'en.

9.6 Automatisk sletning

Data slettes automatisk senest 30 dage efter opsigelse eller efter Kundens skriftlige anmodning (se § 14).

9.7 Sikker softwareudvikling

- Versions-kontrol (Git) med branch-baseret deploy
- Dependency-scans
- Pre-launch-banner og preview-miljøer adskilt fra produktion
- TOTP-MFA tvunget for alle udvikler-konti

9.8 Backup og retablering

Supabase tager løbende point-in-time-backups med 7 dages retention som del af standard-platformen. Backups er krypterede med samme nøgle som primær-data og opbevares i samme region.

10. Brud på persondatasikkerhed (GDPR art. 33-34)

10.1 Underretning til Dataansvarlig

Databehandler underretter Dataansvarlig uden unødig forsinkelse og senest 72 timer efter Databehandler er blevet bekendt med et brud på persondatasikkerheden. Underretningen sendes til Kundens kontakt-e-mailadresse (contact_email) og som notifikation i portalen.

10.2 Indhold af underretningen

Underretningen indeholder så vidt muligt:

- En beskrivelse af karakteren af bruddet, herunder kategorier og omtrentligt antal berørte registrerede og personoplysninger
- Kontaktoplysninger til Databehandlers kontaktpunkt for spørgsmål
- En beskrivelse af de sandsynlige konsekvenser af bruddet
- En beskrivelse af de foranstaltninger, der er truffet eller foreslås truffet for at håndtere bruddet og afbøde dets eventuelle skadelige virkninger

10.3 Bistand til tilsynsmyndighed

Databehandler bistår Dataansvarlig med dokumentation og oplysninger i forbindelse med eventuel anmeldelse til Datatilsynet eller anden tilsynsmyndighed.

11. Bistand med registreredes rettigheder (GDPR art. 12-23)

Databehandler bistår Dataansvarlig med passende tekniske og organisatoriske foranstaltninger ved håndtering af følgende rettigheder:

RETTIGHED	HVORDAN SIMPLEENTRA UNDERSTØTTER DET
Indsigt (art. 15)	Eksporter alle data via portalen eller via hello@simpleentra.com
Berigtigelse (art. 16)	Data hentes friskt fra Microsoft Graph ved hver scan — fejl rettes ved kilden
Sletning (art. 17)	Skriftlig anmodning via hello@simpleentra.com; typisk inden 24 timer
Begrænsning (art. 18)	Skift af data-tier til Snapshot reducerer behandlingen til konklusioner
Dataportabilitet (art. 20)	JSON-eksport på anmodning
Indsigelse (art. 21)	Tilbagekald Microsoft consent; Databehandler opdager det automatisk

Anmodninger fra registrerede, der modtages direkte af Databehandler, videresendes uden unødig forsinkelse til Dataansvarlig.

12. Internationale overførsler (GDPR kapitel V)

12.1 Primær lagring i EU

Primær lagring af persondata sker i Den Europæiske Union (Frankfurt, Tyskland) hos Supabase Inc. (eu-central-1) og Vercel Inc. (fra1).

12.2 Overførsler til tredjelande

Følgende underdatabehandlere er etableret uden for EU/EØS:

- Anthropic PBC (USA) — pseudonymiserede prompts
- Resend Inc. (USA) — transaktionelle e-mails
- Cloudflare Inc. (globalt CDN, USA-base) — DNS og DDoS-beskyttelse

Disse overførsler sker under EU Standard Contractual Clauses (SCCs) jf. EU-Kommissionens beslutning 2021/914 (Module 3 — processor til processor). Databehandler har gennemført en supplerende risikovurdering (Transfer Impact Assessment) og indført nødvendige supplerende foranstaltninger (pseudonymisering, kryptering, kontraktlige garantier).

12.3 Adgang for tredjelandes myndigheder

Hvis en myndighed i et tredjeland anmoder om adgang til personoplysninger behandlet under denne aftale, vil Databehandler — i det omfang loven tillader — underrette Dataansvarlig før udlevering og udfordre anmodningen retsligt.

13. Audit og inspections

13.1 Kundens ret til audit

Dataansvarlig kan med mindst 30 dages varsel anmode om en sikkerheds-audit af Databehandlers overholdelse af denne aftale. Auditeren kan være Dataansvarlig selv eller en uafhængig tredjepart, som Dataansvarlig udpeger og som er bundet af fortrolighed.

13.2 Tredjepartsrapporter

Databehandler stiller årligt — eller på anmodning — relevante tredjeparts sikkerheds-rapporter til rådighed for Dataansvarlig. Databehandler benytter Vercels og Supabases eksisterende SOC 2 Type II rapporter som basis for infrastruktur-niveauet og udfører selv en årlig intern security review for applikations-niveauet.

13.3 Omkostninger

Audits udført af Dataansvarlig eller af en uafhængig tredjepart afholdes som udgangspunkt af Dataansvarlig. Hvis auditen afslører væsentlig overtrædelse af Databehandlers forpligtelser, afholdes omkostningerne af Databehandler.

14. Ophør og sletning af data

14.1 Opsigelse

Hver Part kan opsige aftalen med 30 dages skriftligt varsel.

14.2 Sletning efter ophør

Senest 30 dage efter aftalens ophør (eller efter Kundens skriftlige anmodning) sletter Databehandler:

- Alle tenant-rows og relaterede tabeller i Supabase-databasen

- Alle scan-resultater og rapport-data
- Eventuelle backup-kopier (gennem normal backup-rotation inden for 7 dage)
- Alle pseudonymiseringskortlægninger og AI-cacher

Sletningen attesteres skriftligt over for Dataansvarlig på anmodning.

14.3 Undtagelse

Databehandler kan opbevare anonymiserede eller fuldt aggregerede data til statistiske og produkt-forbedrings-formål, hvor disse data ikke kan henføres til en registreret. Audit-logs over administrative handlinger opbevares i mindst 12 måneder af sikkerhedshensyn.

15. Ansvar og forsikring

[Ansvars-cap og forsikringsvilkår udfyldes ved underskrift]

Som udgangspunkt henvises til hovedaftalens (Master Services Agreement / abonnementsaftalens) ansvarsregulering. Hvis hovedaftalen ikke regulerer ansvar, gælder dansk rets almindelige regler om erstatning, herunder begrænsninger for indirekte tab.

Databehandler tegner og opretholder en passende ansvarsforsikring [detaljer udfyldes ved underskrift].

16. Lovvalg og værneting

Denne aftale er underlagt dansk ret. Tvister, der måtte opstå i forbindelse med aftalen, og som ikke kan løses ved forhandling, skal afgøres ved Københavns Byret som første instans.

Denne værnetingsbestemmelse begrænser ikke de registreredes ret til at indgive klage til en tilsynsmyndighed eller anlægge retssag i medfør af GDPR art. 77-79.

17. Diverse

17.1 Aftalens forrang

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

17.2 Ændringer

Materielle ændringer i denne aftale kræver skriftlig tilslutning fra begge Parter. Mindre opdateringer (fx ajour-føring af listen over underdatabehandlere i § 8.3) håndteres efter proceduren i § 8.2.

17.3 Eksemplarer

Aftalen udfærdiges i to enslydende eksemplarer — ét til hver Part.

18. Underskrifter

FOR DATABEHANDLER

Navn: _____

Titel: _____

Dato: _____

Underskrift: _____

FOR DATAANSVARLIG

Navn: _____

Titel: _____

Dato: _____

Underskrift: _____