DRAFT · GDPR ART. 28

Data Processing Agreement

Between SimpleEntra (processor) and the customer (controller), entered into pursuant to the GDPR — in particular Article 28.

STATUS

Draft

VERSION

1.0

SENEST OPDATERET / UPDATED

2026-06-15

LOVVALG / JURISDICTION

Danish law · Copenhagen City Court

> *This document is a draft. It must be reviewed by legal counsel for both parties before signing. Fields marked [...] are filled in at contract execution.*

1. Parties

1.1 Processor

Name	SimpleEntra (operated by [Company, VAT/CVR no.])
Address	[Address — to be completed at signing]
Contact for processing	hello@simpleentra.com
Contact for privacy	hello@simpleentra.com
DPO	Not mandatory under Art. 37; contact above is used

1.2 Controller

Name	[Customer legal name] ("Customer")
Registration no.	[VAT/registration number]
Address	[Address]
Contact person	[Name, title, email]

The Processor and the Controller are individually referred to as a "Party" and jointly as the "Parties".

2. Definitions

The following definitions correspond to GDPR Art. 4:

- Personal data: Any information relating to an identified or identifiable natural person.
- Processing: Any operation or set of operations performed on personal data, whether or not by automated means.
- Data subject: The natural persons whose personal data is processed.
- Controller: The natural or legal person that determines the purposes and means of processing.
- Processor: The natural or legal person that processes personal data on behalf of the Controller.
- Sub-processor: Another processor engaged by the Processor to carry out specific processing activities on behalf of the Controller.
- Personal data breach: A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
- GDPR: Regulation (EU) 2016/679.

3. Subject matter and duration

3.1 Subject matter

The Processor provides SimpleEntra, a SaaS platform that reads configuration and user data from the Customer's Microsoft 365 tenant through read-only Microsoft Graph permissions for the purpose of assessing

the maturity of the Customer's security posture, generating executive risk reports and offering recommendations for improved configuration.

3.2 Duration

The Agreement remains in force for as long as the Customer maintains an active subscription to SimpleEntra. The Agreement terminates automatically upon termination of the subscription. Data is deleted no later than 30 days after termination (see § 14).

4. Purpose of processing

The purpose of processing is limited to:

- Security assessment of the Customer's Microsoft 365 tenant — including evaluation of Conditional Access policies, MFA coverage, privileged roles, app registrations, device compliance and licence assignments against established baselines (CIS, CISA SCuBA and similar).
- Executive report generation that translates technical findings into business-risk language.
- Recommendations for configuration improvements based on the identified gaps.
- Trend analysis showing changes in security maturity over time.
- AI-assisted natural-language interpretation of technical findings (see § 5.6 and § 9).

The Processor may not process personal data for purposes other than those set out in this section without prior written instruction from the Controller.

5. Nature of processing

5.1 Read-only access

The Processor is granted read-only access to the Customer's Microsoft 365 tenant via Microsoft Graph. No write or delete permissions are granted.

5.2 No changes to Customer systems

The Processor does not modify the Customer's Microsoft 365 configuration. Recommendations are delivered as reports; implementation is the Customer's responsibility.

5.3 No access to content

The Processor does not read the contents of emails, calendars, OneDrive files, SharePoint documents, Teams messages or other user-generated content. Permissions such as Mail.Read, Files.Read.All or ChatMessage.Read are not part of the permission set.

5.4 Pseudonymisation and 3-tier data strategy

The Customer chooses which data category is stored with the Processor:

TIER	WHAT IS STORED	USE CASE

Snapshot	Conclusions and counters only — no raw rows	Default; minimal processing
Pseudonymised	Raw rows with tokens replacing UPN/email/IP	Drill-down without direct identification
Full	Raw data in clear text	Detailed analysis — requires explic- it agreement

The Customer can change tier at any time in the portal. Switching to a lower tier triggers immediate deletion of data held in higher tiers.

5.5 Audit trail in the Customer's own tenant

Every Microsoft Graph call made by the Processor is automatically logged in the Customer's own Entra ID under Sign-In Logs / Audit Logs. The Customer owns this audit trail and may at any time verify the Processor's activity.

5.6 Use of AI

The Processor uses the Anthropic Claude API to generate natural-language summaries and "worst-case scenario" narratives. Before data is sent to Anthropic, all identifiers (UPN, email, IP, company name, GUID) are pseudonymised. Anthropic does not use API input for training, and data retention is disabled through the API configuration.

6. Categories of personal data and data subjects

6.1 Categories of personal data

The Processor processes the following categories of personal data:

- Identifiers: User Principal Names (UPN), email addresses, display names, Microsoft tenant ID, object IDs
- Sign-in metadata: IP addresses, geolocation, sign-in timestamps, client app, success/failure status
- Configuration data: Conditional Access policies, MFA registration, app registrations, role assignments, licence assignments, device-compliance status
- Aggregated counters and scores

The Processor does not process special categories of personal data (Art. 9 GDPR) or data relating to criminal convictions or offences (Art. 10 GDPR).

6.2 Categories of data subjects

- Employees of the Customer (Microsoft 365 users)
- External guest accounts in the Customer's Microsoft 365 tenant
- Administrators with privileged roles

7. Processor obligations (GDPR Art. 28(3))

7.1 Documented instructions

The Processor processes personal data only on documented instructions from the Controller — including with regard to transfers to third countries. This Agreement (together with documentation of scope, purpose and sub-processors) constitutes the Controller's documented instructions.

7.2 Confidentiality

The Processor ensures that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.3 Security measures

The Processor implements all necessary measures required under GDPR Art. 32. Specific measures are described in § 9.

7.4 Sub-processors

The Processor does not engage other processors without the Controller's prior general or specific written authorisation. See § 8.

7.5 Assistance with data-subject rights

The Processor — taking into account the nature of the processing — assists the Controller by appropriate technical and organisational measures with the fulfilment of the Controller's obligation to respond to requests for exercising the data subjects' rights. See § 11.

7.6 Assistance with security, breaches, DPIA and prior consultation

The Processor assists the Controller in ensuring compliance with the obligations under GDPR Art. 32-36, including DPIA and prior consultation with the supervisory authority.

7.7 Return and deletion

Upon termination of the Agreement, the Processor — at the Controller's choice — deletes or returns all personal data and deletes existing copies, unless EU or Member State law requires storage. See § 14.

7.8 Audit rights

The Processor makes available to the Controller all information necessary to demonstrate compliance with the obligations under Art. 28 and allows for and contributes to audits. See § 13.

7.9 Notification of unlawful instructions

The Processor immediately informs the Controller if the Processor considers that an instruction infringes the GDPR or other EU or Member State data protection provisions.

8. Sub-processors

8.1 General authorisation

The Controller hereby grants the Processor a general authorisation to use sub-processors as listed in § 8.3. The Processor is responsible for ensuring that sub-processors comply with obligations equivalent to those imposed on the Processor under this Agreement, including the requirements of GDPR Art. 28(4).

8.2 Change procedure

The Processor notifies the Controller in writing at least 14 days before any material change to the list of sub-processors (addition, replacement or removal). The Controller may object to the change within the notice period. If an objection is raised, the Parties discuss an alternative solution; if agreement cannot be reached, the Controller may terminate the Agreement with immediate effect and without compensation.

8.3 Current sub-processors

NAME	PURPOSE	LOCATION	SECURITY
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, encrypted env variables
Anthropic PBC	AI (Claude API) — ONLY for worst-case scenarios and summaries; input always pseudonymised	US (retention disabled, SCCs)	Zero retention via API, SCC agreements
Resend Inc.	Email delivery (transactional)	US (SCCs)	TLS; no longer retention than necessary
Cloudflare Inc.	DNS + DDoS protection	Global CDN	TLS termination; no application data stored
Microsoft Corp.	Graph API against the Customer's own tenant; we read from it and do not store with Microsoft	Customer's choice of Microsoft region	Customer's own agreement with Microsoft

9. Security measures (GDPR Art. 32)

The Processor implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk to data subjects. The measures are inspired by, among others, ISO/IEC 27002 and NIST CSF.

9.1 Encryption

- At rest: AES-256 via AWS KMS (Supabase Postgres).
- In transit: TLS 1.2+ between all components.

9.2 Access control

- Multi-factor authentication (TOTP) is mandatory for all Processor administrators.
- Super-admins are listed in the app_admins table and continuously audited.
- Customer tenant data is accessed only via service_role_key through server-side actions — never directly from the browser.
- Microsoft Graph access tokens are fetched fresh on every call and are not stored persistently.

9.3 Audit log

All administrative actions are logged in the admin_actions table with timestamp, user ID and a description of the action. Logs are retained for at least 12 months.

9.4 Read-only Graph permissions

The Processor uses only read-only Microsoft Graph permissions (see § 5.1). The permission set is documented in a separate technical appendix and published at simpleentra.com/sadan-virker-det.

9.5 3-tier data strategy

The Customer chooses the storage tier (Snapshot / Pseudonymised / Full) as described in § 5.4 and can lower the tier at any time.

9.6 Automatic deletion

Data is automatically deleted no later than 30 days after termination or upon the Customer's written request (see § 14).

9.7 Secure software development

- Version control (Git) with branch-based deploys
- Dependency scans
- Pre-launch banner and preview environments separated from production
- Enforced TOTP-MFA for all developer accounts

9.8 Backup and recovery

Supabase performs continuous point-in-time backups with 7-day retention as part of the standard platform. Backups are encrypted with the same key as primary data and stored in the same region.

10. Personal data breaches (GDPR Art. 33-34)

10.1 Notification to the Controller

The Processor notifies the Controller without undue delay and no later than 72 hours after becoming aware of a personal data breach. Notification is sent to the Customer's contact email (contact_email) and as an in-portal notification.

10.2 Content of the notification

The notification contains, to the extent possible:

- A description of the nature of the breach, including the categories and approximate number of data subjects and personal data records affected
- Contact information for the Processor's point of contact for queries
- A description of the likely consequences of the breach
- A description of the measures taken or proposed to address the breach and mitigate its potential adverse effects

10.3 Assistance with supervisory authority

The Processor assists the Controller with documentation and information in connection with any notification to the Danish Data Protection Agency (Datatilsynet) or other supervisory authority.

11. Assistance with data-subject rights (GDPR Art. 12-23)

The Processor assists the Controller by appropriate technical and organisational measures in handling the following rights:

RIGHT	HOW SIMPLEENTRA SUPPORTS IT
Access (Art. 15)	Export all data via the portal or via hello@simpleentra.com
Rectification (Art. 16)	Data fetched fresh from Microsoft Graph on every scan — errors corrected at the source
Erasure (Art. 17)	Written request via hello@simpleentra.com; typically within 24 hours
Restriction (Art. 18)	Switching the data tier to Snapshot reduces processing to conclusions
Data portability (Art. 20)	JSON export on request
Objection (Art. 21)	Revoke Microsoft consent; the Processor detects this automatically

Requests from data subjects received directly by the Processor are forwarded without undue delay to the Controller.

12. International transfers (GDPR Chapter V)

12.1 Primary storage in the EU

Primary storage of personal data takes place within the European Union (Frankfurt, Germany) at Supabase Inc. (eu-central-1) and Vercel Inc. (fra1).

12.2 Third-country transfers

The following sub-processors are established outside the EU/EEA:

- Anthropic PBC (US) — pseudonymised prompts
- Resend Inc. (US) — transactional emails
- Cloudflare Inc. (global CDN, US-based) — DNS and DDoS protection

These transfers take place under EU Standard Contractual Clauses (SCCs) pursuant to Commission Decision 2021/914 (Module 3 — processor to processor). The Processor has carried out a supplementary risk assessment (Transfer Impact Assessment) and implemented necessary supplementary measures (pseudonymisation, encryption, contractual safeguards).

12.3 Third-country government access

If an authority in a third country requests access to personal data processed under this Agreement, the Processor will — to the extent permitted by law — notify the Controller before disclosure and challenge the request legally.

13. Audit and inspections

13.1 Customer's right of audit

The Controller may, with at least 30 days' notice, request a security audit of the Processor's compliance with this Agreement. The auditor may be the Controller itself or an independent third party appointed by the Controller and bound by confidentiality.

13.2 Third-party reports

The Processor makes relevant third-party security reports available to the Controller annually — or upon request. The Processor uses the existing SOC 2 Type II reports of Vercel and Supabase as the basis at the infrastructure level and conducts an annual internal security review at the application level.

13.3 Costs

Audits performed by the Controller or an independent third party are in principle borne by the Controller. If the audit reveals a material breach of the Processor's obligations, the costs are borne by the Processor.

14. Termination and deletion of data

14.1 Termination

Either Party may terminate the Agreement with 30 days' written notice.

14.2 Deletion after termination

No later than 30 days after termination of the Agreement (or upon written request from the Customer), the Processor deletes:

- All tenant rows and related tables in the Supabase database
- All scan results and report data
- Any backup copies (through normal backup rotation within 7 days)
- All pseudonymisation mappings and AI caches

Deletion is certified in writing to the Controller on request.

14.3 Exception

The Processor may retain anonymised or fully aggregated data for statistical and product improvement purposes where such data cannot be attributed to a data subject. Audit logs of administrative actions are retained for at least 12 months for security reasons.

15. Liability and insurance

[Liability cap and insurance terms to be completed at signing]

By default, reference is made to the liability provisions of the main agreement (Master Services Agreement / subscription agreement). If the main agreement does not address liability, the general rules of Danish law apply, including limitations for indirect losses.

The Processor maintains appropriate liability insurance [details to be completed at signing].

16. Governing law and jurisdiction

This Agreement is governed by Danish law. Any disputes arising in connection with the Agreement which cannot be resolved by negotiation shall be settled by the Copenhagen City Court (Københavns Byret) as the court of first instance.

This jurisdiction clause does not limit data subjects' right to lodge a complaint with a supervisory authority or to bring legal proceedings under GDPR Art. 77-79.

17. Miscellaneous

17.1 Order of precedence

In case of inconsistency between this Agreement and the main agreement on SimpleEntra, this Agreement prevails with regard to matters relating to the processing of personal data.

17.2 Amendments

Material amendments to this Agreement require written agreement of both Parties. Minor updates (e.g. updating the list of sub-processors in § 8.3) are handled under the procedure in § 8.2.

17.3 Counterparts

The Agreement is executed in two identical copies — one for each Party.

18. Signatures

FOR THE PROCESSOR

Name: _____

Title: _____

Date: _____

Signature: _____

FOR THE CONTROLLER

Name: _____

Title: _____

Date: _____

Signature: _____