

Data Processing Agreement

Template for business customers of RingDeck · Version 1.0 · 23 September 2026 · pursuant to Article 28 of Regulation (EU) 2016/679 (GDPR) and the UK GDPR

Customer (controller): _____ **Address:** _____

Contact for data protection: _____ **RingDeck workspace:** _____

Processor: AVEGANDO AI LABS LLC, a limited liability company under the laws of the State of Wyoming, USA ("RingDeck"). Address as stated in the imprint at ringdeck.io/impressum. Contact for data protection: support@ringdeck.io.

1. Subject matter, purpose and roles

1.1 This agreement governs the processing of personal data that RingDeck carries out on behalf of the Customer when providing the RingDeck service (AI phone and chat agents, call handling, transcripts, customer memory, integrations and related features) under the RingDeck Terms of Service (the "Service").

1.2 The Customer is the controller of the personal data of its callers, website visitors, contacts and other data subjects processed through the Service; RingDeck is its processor. Where the Customer itself acts as a processor for a third party, RingDeck acts as its sub-processor and the Customer warrants that it holds the necessary authorisations.

1.3 For the Customer's own account data (users, billing, support), RingDeck is an independent controller; this is described in the RingDeck Privacy Policy and is not part of this agreement.

1.4 Annex 1 describes the processing (subject matter, duration, nature, purpose, types of personal data and categories of data subjects).

2. Instructions

2.1 RingDeck processes personal data only on documented instructions from the Customer, including with regard to transfers to third countries, unless required to do so by Union or Member State law to which RingDeck is subject; in that case RingDeck informs the Customer before processing, unless the law prohibits this on important grounds of public interest.

2.2 The Customer's instructions are given by using and configuring the Service (agents, prompts, knowledge, integrations, retention settings) and, where needed, in writing to support@ringdeck.io. RingDeck informs the Customer without delay if it considers an instruction to infringe data protection law.

3. Confidentiality

RingDeck ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, and that they process the data only as instructed.

4. Security of processing

4.1 RingDeck implements the technical and organisational measures in Annex 2 and keeps them at a level appropriate to the risk in accordance with Article 32 GDPR. RingDeck may update the measures as long as the overall level of protection does not decrease.

4.2 The Customer is responsible for the security of its own accounts, credentials, connected services and for lawful configuration of its agents (for example not uploading special categories of data without a legal basis).

5. Sub-processors

5.1 The Customer gives general authorisation to RingDeck to engage the sub-processors listed in Annex 3 and, for the current list, in section 4 of the RingDeck Privacy Policy at ringdeck.io/privacy.

5.2 RingDeck informs the Customer of any intended addition or replacement of a sub-processor at least 30 days in advance by e-mail to the workspace owner or by notice in the Service. The Customer may object on reasonable data protection grounds within that period. If the parties cannot resolve the objection, the Customer may terminate the affected part of the Service; RingDeck refunds prepaid fees for the period after termination.

5.3 RingDeck imposes on each sub-processor, by written contract, data protection obligations that are essentially the same as those in this agreement and remains fully liable to the Customer for the performance of the sub-processor's obligations.

6. International transfers

6.1 The Service and its database are hosted in the European Union (Germany). Some sub-processors process data outside the EU, mainly in the United States (Annex 3).

6.2 RingDeck is established in the United States. For transfers from the Customer to RingDeck and onward to sub-processors outside the EU/EEA, the parties rely on the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914 (the "SCCs"), Module Two (controller to processor) or, where the Customer is a processor, Module Three (processor to processor), as set out in Annex 4. For transfers subject to the UK GDPR, the UK International Data Transfer Addendum to the SCCs applies. The SCCs are incorporated by reference and take precedence over this agreement in case of conflict.

6.3 RingDeck applies additional safeguards, in particular encryption in transit, encryption of stored credentials and strict workspace separation, and informs the Customer if it becomes unable to comply with the SCCs.

7. Assistance to the Customer

7.1 Taking into account the nature of the processing, RingDeck assists the Customer with appropriate technical and organisational measures in fulfilling its obligation to respond to requests of data subjects (Articles 12 to 23 GDPR). The Service provides export and deletion functions for this purpose; requests that RingDeck receives directly are forwarded to the Customer without delay.

7.2 RingDeck assists the Customer in ensuring compliance with Articles 32 to 36 GDPR (security, breach notification, data protection impact assessments, prior consultation), taking into account the information available to RingDeck.

8. Personal data breaches

RingDeck notifies the Customer without undue delay, and in any case within 72 hours, after becoming aware of a personal data breach affecting the Customer's personal data. The notification describes, as far as known, the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed, and a contact point. RingDeck documents breaches and cooperates with the Customer in its investigation and notifications.

9. Deletion and return of data

9.1 The Customer can export its workspace data at any time in the Service and can delete agents, knowledge, conversations, contacts and the whole account itself.

9.2 At the end of the Service, RingDeck deletes all personal data processed on behalf of the Customer within 30 days unless Union or Member State law requires storage. The retention periods that the Service enforces during the contract are stated in section 5 of the Privacy Policy. Backups are overwritten within 14 days.

10. Information and audits

RingDeck makes available to the Customer all information necessary to demonstrate compliance with Article 28 GDPR and allows for and contributes to audits, including inspections, conducted by the Customer or an auditor mandated by the Customer. Audits take place at most once per year (more often after a breach or on request of a supervisory authority), with at least 30 days' notice, during business hours, without disrupting the Service, and at the Customer's cost; RingDeck may first answer through written information and existing reports.

11. Liability, term, precedence, law

11.1 Liability of the parties is governed by the RingDeck Terms of Service; each party remains responsible for its own compliance with data protection law.

11.2 This agreement applies for as long as RingDeck processes personal data on behalf of the Customer and ends with the deletion under section 9.

11.3 In case of conflict, the order of precedence is: the SCCs, this agreement, the Terms of Service.

11.4 This agreement is governed by the laws of Ireland; the courts of Ireland have jurisdiction, without prejudice to the rights of data subjects under the SCCs. Changes to this agreement must be made in writing.

Customer
Place, date, name, signature

AVEGANDO AI LABS LLC (RingDeck)
Place, date, name, signature

Annex 1 – Description of the processing

Subject matter	Provision of AI phone and chat agents that answer calls and messages for the Customer, book appointments, forward calls, record conversations and keep customer profiles.
Duration	For the term of the Service, plus the deletion period in section 9.
Nature and purpose	Real-time processing of voice audio and text to understand and answer callers; storage of transcripts, summaries and call metadata; recognition of returning callers (customer memory); execution of the Customer's configured actions (calendar bookings, SMS, e-mails, CRM entries, transfers); billing by minutes.
Types of personal data	Names, phone numbers, e-mail addresses, voice recordings processed in real time, transcripts and summaries of conversations, call metadata (time, duration, numbers), preferences and requests stated by the caller, appointment details, and any data the Customer places in agent knowledge or connected systems. Special categories of data only where the Customer has a legal basis and has configured the agent accordingly (for example health data in a clinic's appointment requests).
Categories of data subjects	Callers and website or messaging visitors of the Customer, its customers, prospects, tenants, patients or guests, and the Customer's employees who appear in conversations or configurations.

Annex 2 – Technical and organisational measures (Article 32 GDPR)

- **Hosting and location:** application and database on servers in the European Union (Germany); network protection and filtering in front of the servers; firewall rules that admit web traffic only from the protection layer.
- **Encryption:** TLS for all connections (browser, phone signalling, sub-processors); credentials of connected services (OAuth tokens, API keys) stored encrypted (AES-256-GCM); passwords stored only as salted hashes.
- **Access control:** strict separation by workspace; role-based access within a workspace; administrative access limited to named RingDeck staff with individual accounts, protected by strong passwords and, where available, two-factor authentication; SSH access to servers restricted and logged.
- **Availability and resilience:** daily encrypted database backups (kept 14 days), off-site copy, monitoring and automatic restart of services, watchdog checks every five minutes.
- **Data minimisation and retention:** automatic deletion of calls, conversations and customer profiles after 24 months; deletion and export functions for the Customer; agents announce that they are AI.
- **Sub-processor control:** written agreements with all sub-processors; list maintained in the Privacy Policy; 30-day notice of changes.
- **Logging and incident handling:** security-relevant events logged; documented breach process with notification within 72 hours; regular review of security settings and dependencies.
- **Organisation:** confidentiality obligations for all persons with access; least-privilege principle; separation of production, test and backup environments.

Annex 3 – Sub-processors (as of 23 September 2026)

The current list is maintained in section 4 of the Privacy Policy at ringdeck.io/privacy. "Only when connected" means the provider receives data only after the Customer connects that service.

Sub-processor	Purpose	Location
Hetzner Online GmbH	Servers and database	Germany (EU)
Cloudflare	Network and security in front of the servers, outgoing e-mail	USA, EU
Google (Gemini)	Language models that write the agent's answers	USA, EU
OpenAI	Language model and speech, fallback	USA
Anthropic	Language model, second fallback	USA
ElevenLabs	Speech recognition and the agent's voice	USA
LiveKit	Real-time audio connection during calls	USA, EU
Twilio, Telnyx	Telephone numbers and the phone network	USA
Stripe	Subscription payments	USA, Ireland
Meta / WhatsApp Cloud API	Only when connected: WhatsApp conversations	USA, Ireland
Telegram	Only when connected: Telegram conversations	—
Tavus	Only when switched on: video avatar	USA
Google Workspace APIs	Only when connected: calendar, spreadsheets, Gmail of the workspace	USA, EU

Annex 4 – Standard Contractual Clauses

The parties agree to the Standard Contractual Clauses of Commission Implementing Decision (EU) 2021/914 with the following choices: Module Two (controller to processor), or Module Three (processor to processor) where the Customer acts as processor; Clause 7 (docking clause) applies; Clause 9(a) Option 2 (general written authorisation) with a notice period of 30 days; Clause 11(a) optional language does not apply; Clause 13: the competent supervisory authority is the authority of the EU Member State in which the Customer is established or, where the Customer is not established in the EU, the authority determined under Clause 13(a); Clause 17: the Clauses are governed by the laws of Ireland; Clause 18: disputes are resolved before the courts of Ireland. Annex I of the SCCs corresponds to the parties named above and Annex 1 of this agreement; Annex II of the SCCs corresponds to Annex 2; Annex III of the SCCs corresponds to Annex 3. For transfers subject to the UK GDPR the UK International Data Transfer Addendum (version B1.0) is incorporated with the same choices.

This template is provided by RingDeck for its business customers. It is not legal advice; customers should have it reviewed for their own situation.