Data Processing Addendum

Version 2026-11-14-draft - published 2026-11-14

This Data Processing Addendum ("DPA") forms part of the Terms of Service between [CLIENTOR LEGAL ENTITY] ("Clientor", "Processor") and the Customer named in the account ("Customer", "Controller"). It applies whenever Clientor processes Customer Personal Data on Customer's behalf. It takes effect when Customer accepts the Terms of Service, with no separate signature needed. Customers that need a countersigned copy can request one at [PRIVACY EMAIL].

1. Definitions

- "Data Protection Laws" means all laws that apply to the processing of Customer Personal Data under the Agreement, including the California Consumer Privacy Act as amended by the California Privacy Rights Act and its regulations ("CCPA"), the other US state comprehensive privacy laws, the EU General Data Protection Regulation 2016/679 ("GDPR"), the UK GDPR and Data Protection Act 2018, the Swiss Federal Act on Data Protection, and Canada's PIPEDA, each as amended.

- "Customer Personal Data" means personal data or personal information (as defined by Data Protection Laws) contained in Customer Data that Clientor processes on Customer's behalf, including data about Contacts, call recordings, transcripts, messages and emails.

- "Security Incident" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data in Clientor's or its subprocessors' control.

- "Subprocessor" means a third party Clientor engages to process Customer Personal Data.

- "SCCs" means the standard contractual clauses approved by European Commission Implementing Decision (EU) 2021/914; "UK Addendum" means the International Data Transfer Addendum issued by the UK Information Commissioner.

- "De-identified Data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual or household, and that is held subject to the commitments in section 4.

Terms such as "controller", "processor", "business", "service provider", "contractor", "data subject", "processing", "sell" and "share" have the meanings given in Data Protection Laws. Other capitalized terms have the meanings given in the Terms of Service.

2. Roles and scope

2.1 Roles. Customer is the controller (or business) and Clientor is the processor (or service provider) of Customer Personal Data. Where Customer is itself a processor for a third party (for example, an agency acting for its clients), Clientor is Customer's subprocessor, and Customer warrants that its instructions are authorized by the relevant controller.

2.2 Clientor as controller. This DPA does not apply to personal data Clientor processes as a controller, such as account, User, billing, website and demo data, which the Privacy Policy

covers.

2.3 Details of processing. Annex 1 describes the subject matter, nature, purpose and duration of the processing, the types of personal data and the categories of data subjects.

3. Clientor's obligations as processor

3.1 Instructions. Clientor processes Customer Personal Data only on Customer's documented instructions, which are the Agreement, Customer's configuration of the Service (including its Agents, flows, connectors, retention settings and modes), and any other written instructions Customer gives that are consistent with the Agreement, unless the law requires otherwise (in which case Clientor will tell Customer before processing, unless the law prohibits it). Clientor will tell Customer promptly if, in its opinion, an instruction infringes Data Protection Laws.

3.2 Confidentiality. Clientor ensures that personnel authorized to process Customer Personal Data are bound by confidentiality obligations and receive appropriate privacy and security training.

3.3 Security. Clientor implements and maintains the technical and organizational measures in Annex 2.

3.4 Assistance. Taking into account the nature of the processing, Clientor assists Customer by appropriate technical and organizational measures, insofar as possible, in responding to data subjects' requests, and provides reasonable information to help Customer carry out data protection impact assessments, risk assessments and prior consultations required by Data Protection Laws.

3.5 Data subject requests. The Service lets Customer search, export, correct and delete Contact records, recordings and transcripts. If Clientor receives a request from a data subject about Customer Personal Data, it will refer the data subject to Customer, notify Customer promptly, and not respond directly except to confirm the referral, unless Customer authorizes it or the law requires it.

4. US state law service-provider terms

4.1 Clientor will not: (a) sell or share Customer Personal Data; (b) retain, use or disclose it for any purpose (including any commercial purpose) other than the business purposes specified in the Agreement and Annex 1, or as otherwise permitted for service providers by the CCPA and its regulations; (c) retain, use or disclose it outside the direct business relationship between Clientor and Customer; or (d) combine it with personal information Clientor receives from or on behalf of another person, or collects from its own interactions with the consumer, except as permitted for service providers by the CCPA regulations (for example, to detect security incidents or prevent fraud).

4.2 Clientor will comply with the CCPA and other applicable US state privacy laws, provide the same level of privacy protection as they require, and notify Customer if it determines it can no longer meet its obligations. Customer may take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data, including by exercising its rights under section 10.

4.3 Per-customer improvement is a business purpose. Using Customer Personal Data and the event logs of Customer's Agents to maintain contact memory, propose knowledge-base fixes, propose and test prompt and flow changes, and optimize contact timing for Customer's own Agents within Customer's workspace is processing to provide the Service to Customer and is a permitted business purpose. Clientor does not use it to build or improve services for any other customer, except as section 4.4 permits.

4.4 De-identified and aggregated data. Where an Owner of Customer has turned on the platform-learning setting ("Help improve C2R.ai"), Customer instructs and permits Clientor to create De-identified Data and aggregated statistics from the event logs of Customer's Agents and to use them to improve library Agents, evaluation test sets and model routing for the Service. Independently of that setting, Clientor may create aggregated service metrics (such as uptime, volumes and latency) that contain no personal information. For all De-identified Data, Clientor will: (a) take reasonable measures to ensure the data cannot be associated with an individual or household, including by excluding the content of recordings, transcripts, messages and emails, removing direct identifiers, aggregating across organizations and applying minimum-count thresholds; (b) publicly commit to maintain and use the data only in de-identified form and not to attempt to re-identify it, except to test its de-identification processes; (c) contractually obligate any recipient to comply with these requirements; and (d) where the GDPR or UK GDPR applies, create only data that is anonymous within the meaning of Recital 26 GDPR, treating the act of anonymization as processing on Customer's instructions. De-identified Data and aggregated statistics are not Customer Personal Data. Clientor does not use Customer Personal Data or De-identified Data to train foundation or general-purpose AI models.

4.5 Clientor certifies that it understands and will comply with the restrictions in this section 4.

5. Subprocessors

5.1 Authorization. Customer gives Clientor general authorization to engage Subprocessors. The current list, with each Subprocessor's function and location, is in Annex 3 and at clientor.ai/legal/subprocessors.

5.2 Obligations. Clientor imposes on each Subprocessor written data protection terms that are no less protective than this DPA, to the extent appropriate to the service provided, and remains responsible for each Subprocessor's performance.

5.3 Changes and objection. Clientor will give at least 30 days' notice before a new Subprocessor processes Customer Personal Data, by updating the subprocessor page and emailing Customers who subscribe to updates there (and every Owner, for Subprocessors that process call recordings, transcripts or messages). Customer may object on reasonable data protection grounds within that period by writing to [PRIVACY EMAIL]. The parties will discuss the objection in good faith; if Clientor cannot offer a reasonable alternative, Customer may terminate the affected part of the Service and receive a refund of prepaid fees and the purchase price of unused purchased Credits for it. Clientor may replace a Subprocessor with shorter notice if needed urgently for security or continuity, and will give notice as soon as practicable.

6. Security Incidents

6.1 Clientor will notify Customer without undue delay, and in any event within 72 hours, after becoming aware of a Security Incident affecting Customer Personal Data.

6.2 The notice will describe, to the extent then known: the nature of the incident, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed to address it and mitigate its effects, and a contact point. Clientor will provide further information as it becomes available.

6.3 Clientor will take reasonable steps to contain, investigate and mitigate the incident, and reasonably cooperate with Customer in meeting its notification obligations. Unless the law requires otherwise, Customer is responsible for notifying data subjects and authorities about Customer Personal Data; Clientor will not do so on Customer's behalf without Customer's consent, except as required by law.

6.4 Clientor's notification of a Security Incident is not an acknowledgement of fault or liability. Unsuccessful attempts that do not compromise the security of Customer Personal Data (such as pings, port scans or blocked login attempts) are not Security Incidents.

7. Call recordings, transcripts and messages

7.1 Instructions. Clientor records, transcribes, summarizes and stores calls only where Customer has turned recording on for the Agent or number concerned. Recording is on by default for new voice Agents; the dashboard shows the setting.

7.2 Disclosures. The Service plays an AI disclosure and, where recording is on, a recording disclosure at the start of every call by default. Customer remains responsible for obtaining any consent required by Data Protection Laws and by wiretapping, eavesdropping and call-recording laws (including all-party-consent laws) and must not disable the disclosures.

7.3 Purpose limitation. Clientor uses recordings, transcripts and message content only to provide the Service to Customer as described in section 4.3, and to investigate abuse, security incidents and legal complaints about Customer's communications. Clientor does not use them for its own purposes, does not use them to train AI models, and does not include their content in De-identified Data.

7.4 Retention. Customer chooses the retention period for recordings and transcripts in the dashboard. The default is 12 months from the call, after which they are deleted automatically. Customer can delete individual recordings at any time.

7.5 Access. Clientor personnel access recordings, transcripts and messages only to provide support Customer requests, to investigate abuse or a security incident, or when the law requires, and each access is logged.

8. Deletion and return

8.1 During the term, Customer can export and delete Customer Personal Data using the Service.

8.2 After the Agreement ends, Customer has 30 days to export its data. Clientor will then delete Customer Personal Data from production systems within 60 days, and from backups as they

expire (within 35 days), unless the law requires Clientor to keep it, in which case Clientor will keep it confidential and process it only for that legal purpose.

8.3 On request, Clientor will confirm deletion in writing.

9. International transfers

9.1 Clientor may transfer and process Customer Personal Data in the United States and in other countries where Clientor or its Subprocessors operate, as Annex 3 shows.

9.2 EEA transfers. To the extent Customer Personal Data subject to the GDPR is transferred to Clientor in a country without an adequacy decision, the SCCs are incorporated into this DPA as follows: Module 2 (controller to processor) applies where Customer is a controller, and Module 3 (processor to processor) applies where Customer is a processor; Clause 7 (docking clause) applies; under Clause 9, option 2 (general written authorization) applies with the notice period in section 5.3; the optional language in Clause 11 does not apply; under Clause 17, option 1 applies and the governing law is the law of Ireland; under Clause 18, the courts of Ireland have jurisdiction; Annex I of the SCCs is completed by Annex 1 of this DPA, Annex II by Annex 2, and Annex III by Annex 3.

9.3 UK transfers. For transfers subject to the UK GDPR, the UK Addendum applies, completed with the information in this DPA and its Annexes, and either party may end it as permitted by its Section 19.

9.4 Swiss transfers. For transfers subject to the Swiss FADP, the SCCs apply with the Swiss Federal Data Protection and Information Commissioner as the competent supervisory authority and references to member states read to include Switzerland.

9.5 Onward transfers. Clientor ensures that transfers to Subprocessors are covered by an appropriate transfer mechanism.

9.6 Conflict. If the SCCs or UK Addendum conflict with this DPA, the SCCs or UK Addendum prevail.

10. Audits

10.1 Clientor will make available to Customer the information reasonably necessary to demonstrate compliance with this DPA, including its Security Overview, its responses to a standard security questionnaire once per year, and summaries of independent assessments or certifications as Clientor obtains them.

10.2 If that information is not sufficient to show compliance, or a regulator requires it, or after a Security Incident affecting Customer, Customer may audit Clientor's compliance, no more than once a year (except after a Security Incident or as a regulator requires), on at least 30 days' written notice, during business hours, without unreasonably disrupting operations, using an independent auditor bound by confidentiality, and at Customer's expense. Audits do not extend to other customers' data or to Subprocessors' facilities, for which Clientor will provide the Subprocessor's own audit reports where available.

11. Customer's obligations

Customer: (a) is responsible for the lawfulness of the processing it instructs, including having a legal basis and providing notices and obtaining consents (including for call recording, AI interaction and Contact outreach); (b) will not instruct Clientor to process special categories of personal data, protected health information, payment card data or data of children under 13 unless a separate written addendum permits it; (c) will configure retention, roles and access appropriately; and (d) will promptly tell Clientor of any data subject request or complaint that requires Clientor's action.

12. Liability and order of precedence

12.1 Each party's liability under this DPA is subject to the limitations of liability in the Terms of Service, except to the extent Data Protection Laws or the SCCs do not allow it.

12.2 If this DPA conflicts with the Terms of Service about the processing of Customer Personal Data, this DPA prevails.

12.3 This DPA ends when Clientor no longer processes Customer Personal Data.

Annex 1: Details of processing

- Parties: Data exporter: Customer (controller, or processor for its clients). Data importer: [CLIENTOR LEGAL ENTITY], [ADDRESS], contact [DPO/CONTACT] (processor).

- Subject matter: provision of the Clientor AI agent platform under the Agreement.

- Nature of processing: collection, recording, transcription, translation, storage, retrieval, analysis by AI models, generation of replies and summaries, transmission by voice, text, messaging, chat and email, organization, structuring, de-identification and aggregation (section 4.4), deletion.

- Purpose: to provide the Service to Customer: answering and placing calls, sending and answering messages and emails, booking appointments, updating Customer's connected systems, maintaining contact memory, improving Customer's own Agents, analytics, support, security and abuse prevention.

- Categories of data subjects: Customer's Contacts (customers, prospects, leads, callers, patients or clients, and recipients of communications); Customer's employees and Users named in configurations; individuals mentioned in Customer's knowledge sources and connected systems.

- Categories of personal data: names; phone numbers; email addresses; postal addresses; voice recordings; call transcripts and summaries; message and email content; appointment and booking details; CRM and order records; consent and opt-out records; caller ID and call metadata; IP addresses and device data from chat widgets; and any other personal data Contacts disclose in a conversation.

- Sensitive data: none intended. Customer must not instruct the Service to collect special categories of data, health information, financial account numbers, government ID numbers or precise geolocation unless a separate written addendum permits it. Where Contacts volunteer

such data, it is protected by the measures in Annex 2, including redaction in system logs.

- Frequency: continuous for the term.

- Duration and retention: the term of the Agreement plus the deletion periods in section 8, and the retention settings Customer configures (recordings and transcripts default to 12 months).

- Subprocessor transfers: as described in Annex 3, for the same purposes and duration.

Annex 2: Technical and organizational security measures

Clientor maintains at least the following measures. Items marked "in rollout" are being deployed and will be in place before Customer Personal Data is processed by the feature concerned.

- Encryption: TLS 1.2 or higher for data in transit over public networks; for customers in HIPAA Mode, encryption of sensitive fields (including conversations, call transcripts, messages and contact details) with AES-256 and per-organization keys protected by a cloud key management service; connector credentials stored encrypted; tokens for apps connected through our integration hub encrypted with per-organization keys protected by a cloud key management service; object storage and backups encrypted by the storage provider. Encryption of all database storage and internal network traffic is being rolled out.

- Tenant isolation: every customer record carries an organization identifier, and PostgreSQL row-level security enforces that each request can read and write only its own organization's rows.

- Access control: role-based access for customers (Owner, Admin, Member, Viewer); multi-factor authentication available to all Users and required for Clientor staff with production access; least-privilege staff access, reviewed quarterly; access to customer content only for support, security or legal reasons, logged.

- Authentication: passwords and single sign-on handled by a dedicated identity provider; no plain-text passwords stored by Clientor.

- Network security: production databases are not exposed to the public internet; web traffic passes through a content-delivery and web-application-firewall layer; rate limiting on public endpoints; server-side request protections on website research (blocking private and metadata addresses).

- Application security: code review on every change; automated tests, dependency audits and secret scanning in continuous integration; no secrets in source code; separate staging and production environments; manual approval for production deployments.

- AI safety: Agents act only through allowlisted tools; prompt-injection screening; per-organization and per-Agent budget limits; personal data redacted from system logs; outbound consent checks.

- Logging and monitoring: structured logs without personal data or tokens; audit log of User

and staff actions in the dashboard; error monitoring; alerts on anomalous activity.

- Backups and resilience: automated nightly backups, encrypted by the storage provider, with retention of at least 7 days and no more than 35 days; restore procedures tested at least twice a year (in rollout).

- Incident response: a documented incident response plan with on-call escalation, customer notification within 72 hours under section 6, and post-incident review.

- Vendor management: due diligence and data protection terms with every Subprocessor; AI model providers contractually barred from training on Customer Data.

- Personnel: confidentiality agreements; background checks where lawful for staff with production access; security and privacy training at onboarding and annually.

- Data minimization and deletion: retention settings for recordings and transcripts; automatic deletion after the account ends as in section 8.

- Independent assessment: a SOC 2 Type II assessment is planned; until it is available, Clientor answers security questionnaires under section 10.

Annex 3: Subprocessors

The current list of Subprocessors, with function, data processed and location, is published at clientor.ai/legal/subprocessors and forms part of this Annex. As of the version date, it is:

- Anthropic, PBC (United States): AI model processing of conversation text, transcripts and research.

- OVHcloud ([OVH REGION]): application hosting and databases.

- Amazon Web Services, Inc. (United States): object storage for recordings and files, backups and key management.

- Clerk, Inc. (United States): User authentication and organization management (User data only).

- Cloudflare, Inc. (global): content delivery, DNS and web application firewall.

- Postmark (ActiveCampaign, LLC) (United States): transactional and Agent email delivery.

- Stripe, Inc. (United States): payments (billing data only, not Customer Personal Data).

- Google LLC (United States): Google Places API for Business Brain research and, where Customer connects Google Workspace, calendar and email access.

- Functional Software, Inc. d/b/a Sentry (United States): error monitoring with personal data scrubbed.

- [VOICE PROVIDER] (United States): telephone numbers, call handling, recording and speech

processing.

- [SMS PROVIDER] (United States): text-message delivery and carrier registration (added before text messaging launches).

- [EMBEDDINGS PROVIDER] (United States): conversion of knowledge-base text into search vectors (added before knowledge search launches).

- Meta Platforms, Inc. (United States / Ireland): WhatsApp Business Platform messaging where Customer enables WhatsApp (added before WhatsApp launches).

- n8n (self-hosted by Clientor on its own infrastructure; not a separate Subprocessor).