

Data Processing Agreement

Distronode Corporation — District AI • Version 1.5 • Effective on execution • Published 2026-09-10

To execute this DPA, or to have Distronode countersign your own, contact legal@distronode.com.

Revision note (v1.5, 2026-09-10). Section 6 is restated in shorter sentences with no change in meaning. No obligation or liability term changed between v1.4 and v1.5.

Revision note (v1.4, 2026-09-10). Section 6 is corrected against the platform as it is operated from 2026-09-10, and no obligation or liability term changed between v1.3 and v1.4. Three corrections, none of them in either party's favour. First, the Canadian voice engine is no longer described as optional and off by default: it is the engine a new Canadian workspace starts on, the other engines stay available, and the language model runs in Montreal on all of them but the realtime engine, whose single listen-and-speak model Google does not serve from its Montreal region, so a Canadian workspace that selects that engine is processed in the United States. Second, section 6 now states where a Canadian telephone call is handled, which it did not address at all: such a call is handled in Montreal in both directions where Distronode issued the number through Telnyx, while a call arriving on a number issued through Twilio, whether Canadian or United States, reaches Distronode in the United States. Third, section 6 records that Distronode's statements about a call stop at the handoff to the carrier, as the data residency map does.

Revision note (v1.3, 2026-09-02). Six changes, stated by whom they favour. In Distronode's favour: section 4(1) now allows aggregated, de-identified statistics that identify neither the Customer nor any individual; section 4(5) redirects individuals who contact Distronode directly to the Customer and allows a reasonable charge for assistance beyond the product tools where requests are excessive; section 4(8) bounds audits to once in any twelve-month period, on 30 days' written notice, during business hours, at the Customer's cost, under confidentiality and never touching another customer's data, satisfied first by documentation and third-party reports; and section 5(5) adds the Customer's warranty that its instructions are lawful, with an indemnity for processing carried out on unlawful ones. In the Customer's favour: section 4(7) adds written confirmation of deletion on request, and section 6 states that the Standard Contractual Clauses and the UK Addendum prevail where they conflict with this DPA. Corrections: section 6 now says support correspondence is held in Canada, which is outside the Customer's region unless the workspace is Canadian (the v1.1 wording said outside the region unconditionally, which was wrong for a Canadian Customer), and notes the optional Canadian voice engine; the retention wording in section 4(7) and Annex II now matches the website. No liability cap or exclusion changed.

Revision note (v1.2, 2026-08-29). Annex I now names number registration documents among the types of Personal Information processed: where the Customer registers a telephone number in a country whose regulator requires documents, Distronode stores the documents the Customer provides — which, for registrations in an individual's name, can include government identity documents — in the Customer's workspace region, transmits them to the telephony carrier's regulatory-compliance service in the United States on submission, and deletes them 30 days after the number is released or the registration is withdrawn, and on account deletion. This is an addition describing a new, opt-in processing activity; no obligation or liability term changed between v1.1 and v1.2.

Revision note (v1.1, 2026-08-15). Three technical measures in Annex II were corrected because each was inaccurate as written: databases are reachable on an address restricted to Distronode's own servers rather than having no public endpoint; database storage is encrypted at rest by each hosting provider, while Google Cloud KMS protects stored third-party credentials; and the backup decryption key is held in a managed secret store separate from the storage provider rather than outside the cloud. Section 6 now states that support correspondence is held outside the Customer's region, and section 4(7) states the 365-day retention window for a resolved support request and confirms that an erasure covers support correspondence. No obligation or liability term was weakened between v1.0 and v1.1; the retention window and the erasure scope are additions in the Customer's favour.

1. Parties and Roles

This Data Processing Agreement ("DPA") is entered into between **Distronode Corporation**, a Canadian corporation federally incorporated under the Canada Business Corporations Act, with its head office at RBC WaterPark Place, 20

Bay Street, 11th Floor, Toronto, Ontario, M5J 2N8, Canada ("**Distronode**", the "**Processor**"), and the customer identified in the signature block below (the "**Customer**", the "**Controller**").

The Customer determines the purposes and means of processing the personal information handled through its District AI workspace. Distronode processes that personal information only on the Customer's behalf and documented instructions, as the Customer's processor and service provider and, where Ontario's Personal Health Information Protection Act, 2004 (PHIPA) applies, as the Customer's agent and electronic service provider. This DPA supplements the Distronode Terms of Service; where this DPA and the Terms differ on the handling of personal information, this DPA governs.

2. Definitions

"**Personal Information**" means any information relating to an identified or identifiable individual processed through the Customer's workspace. "**Applicable Privacy Law**" means the privacy and data-protection laws that apply to the processing, which may include PIPEDA, Québec's Act respecting the protection of personal information in the private sector (as amended by Law 25), PHIPA, the EU and UK General Data Protection Regulations ("GDPR"), and US state privacy laws. "**Sub-processor**" means a third party engaged by Distronode to process Personal Information on the Customer's behalf.

3. Scope and Duration of Processing

The subject matter, duration, nature and purpose of processing, the types of Personal Information, and the categories of individuals are set out in **Annex I**. Processing continues for as long as the Customer's subscription is active, plus the limited period needed to delete or return Personal Information afterward.

4. Distronode's Obligations as Processor

1. **Instructions.** Distronode processes Personal Information only to provide the service and to follow the Customer's documented instructions, including the settings the Customer chooses in its workspace. Distronode does not use the Customer's content for its own purposes, does not sell Personal Information, and does not use it to train public or foundational AI models. If Distronode believes an instruction violates Applicable Privacy Law, it will inform the Customer promptly. Distronode may create and use statistics about use of the service that are aggregated and de-identified so that they identify neither the Customer nor any individual.
2. **Confidentiality.** Persons authorized to process Personal Information are bound by confidentiality obligations, and access to production data is scoped and least-privilege.
3. **Security.** Distronode maintains the technical and organizational measures set out in **Annex II**, and will not materially decrease the overall security of the service during a subscription term.
4. **Sub-processors.** The Customer generally authorizes the Sub-processors listed at distronode.com/compliance/subprocessors (incorporated into this DPA by reference, including each Sub-processor's purpose, data category, and region). Distronode remains responsible for its Sub-processors'

performance, imposes data-protection obligations on them consistent with this DPA, and will give the Customer at least **30 days' notice** (via that page and email) before adding or replacing a Sub-processor, so the Customer can object on reasonable data-protection grounds. If an objection cannot be resolved, the Customer may terminate the affected subscription.

5. **Assistance with individual requests.** Distronode will assist the Customer in responding to requests to access, correct, delete, or port Personal Information, through the export and deletion tools in the product and through direct support at legal@distronode.com where needed. Where an individual contacts Distronode directly about Personal Information the Customer controls, Distronode redirects the individual to the Customer and does not respond on the Customer's behalf unless instructed. Assistance beyond the export and deletion tools in the product may be charged at a reasonable rate where requests are excessive.
6. **Breach notification.** Distronode maintains security incident logs and will notify the Customer without undue delay, and in any case within **48 hours of confirming** a breach of security safeguards affecting the Customer's Personal Information, with the information reasonably available to help the Customer meet its own notification duties. Distronode will not characterize the Customer's legal obligations in its notice.
7. **Deletion and return.** On termination of the subscription, or on the Customer's request, Distronode deletes or returns the Customer's workspace data. Archived call recordings are additionally deleted on a rolling retention schedule (90 days by default; a different default retention window can be arranged as part of an enterprise agreement), and a resolved support request is deleted 365 days after it was opened, from the support desk and from Distronode's own copy of the conversation. Deleted data ages out of encrypted backups within approximately eight weeks. Erasure requests are honored without undue delay and within 30 days, and an erasure covers support correspondence as well as workspace data. On request, Distronode provides written confirmation that deletion has completed.
8. **Records, audits, and cooperation.** Distronode keeps records of its processing activities and will cooperate with the Customer's reasonable audit and information requests (satisfied first through documentation, written responses and any third-party report Distronode holds), and with supervisory authorities where the law requires it. An audit beyond that is limited to once in any twelve-month period, on at least 30 days' written notice, during business hours, at the Customer's cost, under confidentiality obligations and in a scope agreed in advance, and may not access another customer's data.

5. Customer's Obligations as Controller

1. Have a lawful basis for the Personal Information collected through the Customer's receptionist, and give callers the notice and, where required, the consent the Customer's situation calls for — including configuring the receptionist's greeting to identify the assistant as automated, which Distronode recommends and supports.
2. Use call recording, transcription, and outbound calling or messaging in accordance with the laws that apply to the Customer and its callers, including consent-to-record rules and anti-spam laws such as CASL (Canada) and the TCPA (United States).
3. Configure the workspace (recording, retention, enrichment, and team access) to match the Customer's own policies, and keep team accounts secure.

4. Where PHIPA applies, remain the health information custodian and use District AI within the Customer's own PHIPA compliance program.
5. Ensure that its instructions to Distronode are lawful, and indemnify Distronode against claims, penalties and reasonable costs arising from processing carried out on the Customer's unlawful instructions.

6. International Transfers

Workspace data is stored in the data-residency region the Customer selects at signup (United States, Canada, Europe, or Asia-Pacific). Some processing occurs outside that region, as described on the data residency map at distronode.com/compliance/data-residency (incorporated by reference). For example, most AI processing runs in the United States, while the language model powering live calls runs in the EU (europe-west4) for European workspaces.

For a Canadian workspace that model runs in Montreal (northamerica-northeast1) on every voice engine but the realtime one. Google does not serve that engine's single listen-and-speak model from Montreal, so a Canadian workspace that selects it is processed in the United States (us-east4) and the engine picker labels it accordingly. A new Canadian workspace starts on an all-Canadian voice engine that runs speech recognition and speech synthesis in Montreal as well, and a Canadian workspace on one of the other engines has those two speech legs processed in the United States.

A telephone call for a Canadian workspace is handled in Montreal in both directions where Distronode issued the number through Telnyx. A call arriving on a number issued through Twilio, whether Canadian or United States, reaches Distronode in the United States, and the data residency map records where Distronode's statements stop at the handoff to the carrier.

Support correspondence is a further exception and is called out because it is easy to overlook. Requests the Customer sends to Distronode support are received by a single support desk hosted in Canada and serving all four regions, so they are held in Canada, which is outside the Customer's region unless the Customer's workspace is Canadian.

Where Personal Information originating in the EEA or the UK is transferred to a country without an adequacy decision, the parties incorporate by reference the European Commission's Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914), **Module Two (controller to processor)**, with the Customer as data exporter and Distronode as data importer, completed by Annex I and Annex II of this DPA; and, for UK transfers, the UK International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner's Office. For transfers from Canada, Distronode relies on PIPEDA's accountability model, maintaining comparable protection through this DPA and its Sub-processor agreements. Where the Standard Contractual Clauses or the UK Addendum conflict with this DPA, the Clauses or the Addendum prevail.

7. Liability, Term, and Governing Law

The liability of each party under this DPA is subject to the limitations and exclusions set out in the Terms of Service. This DPA takes effect on execution, continues for as long as Distronode processes Personal Information for the Customer, and terminates automatically when deletion or return under section 4(7) completes. This DPA is governed by

the laws of the Province of Ontario and the federal laws of Canada, without prejudice to mandatory data-protection law that applies to a transfer under section 6.

Annex I — Details of Processing

Subject matter	Providing the District AI voice receptionist and related messaging, CRM, and scheduling features.
Duration	The subscription term, plus the limited period needed to delete or return data afterward.
Nature and purpose	Answering, routing, recording, transcribing, and summarizing calls; sending and receiving messages; enriching contacts where the Customer enables it; scheduling; and billing.
Types of Personal Information	Caller phone numbers, call audio and transcripts, contact and CRM records, message content, appointment details, and account and billing information. Where the Customer is a health-care provider, call content may include personal health information. Where the Customer registers a telephone number in a country whose regulator requires documents, also the registration documents the Customer provides: business registry extracts, proofs of address and, for registrations in an individual's name, government identity documents such as a passport or national identity card. Registration documents are stored in a bucket in the Customer's workspace region, are transmitted to the telephony carrier's regulatory-compliance service in the United States when the Customer submits the registration, and are deleted 30 days after the number is released or the registration is withdrawn, and on account deletion.
Categories of individuals	The Customer's callers and customers, its contacts, and its own team members who use the workspace.
Frequency	Continuous, for the duration of the subscription.

Annex II — Technical and Organizational Measures

- Encryption in transit: TLS 1.2 or higher enforced on every public endpoint.
- Encryption at rest: database storage volumes are encrypted by the provider hosting each region, under keys that provider manages and Distrinode does not hold. Stored third-party credentials (for example a telephony account the Customer connects) are additionally encrypted at the application layer with Google Cloud KMS before they are written.
- Tenant isolation: PostgreSQL row-level security enforced at the database, so one tenant cannot read another's data.
- Access control: production access is scoped and least-privilege; credentials and API keys live in a managed secret store and are never committed to source control.
- Network: each region's database accepts connections only from an explicit allow-list of Distrinode's own origin servers, over TLS with certificate verification, and its plaintext listeners are firewalled off. Database ports are not open to the public internet.

- Application hardening: rate limiting and managed firewall rules in front of authentication endpoints; bot and abuse protection on public forms.
- Patching: container base images are rebuilt and redeployed on a monthly cadence.
- Backups: nightly database backups, encrypted inside the region before upload, with the decryption key held in a managed secret store separate from the provider that stores the backups. Retained 14 daily and 8 weekly copies.
- Retention: archived call recordings deleted on a rolling schedule (90 days by default; a different default retention window can be arranged as part of an enterprise agreement).
- Monitoring: security incident logging, error tracking, and operational alerting.

Execution

Signed by the parties' authorized representatives:

Distronode Corporation

Customer

Name: Sean Dean

Title: Founder & CEO

Date:

Legal entity name:

Name / Title:

Date:

Distronode Corporation • RBC WaterPark Place, 20 Bay Street, 11th Floor, Toronto, Ontario, M5J 2N8, Canada • legal@distronode.com

Plain-language summary: distronode.com/compliance/dpa • Sub-processors: distronode.com/compliance/subprocessors • Data residency: distronode.com/compliance/data-residency