

Data Processing Agreement.

VERSION 2.1, LAST UPDATED: 14 OCTOBER 2026

This Data Processing Agreement ("DPA") is between **EchoNova AI L.L.C-FZ**, licensed by Meydan Free Zone, Dubai (trade licence no. 2650442.01), Meydan Grandstand, 6th floor, Meydan Road, Nad Al Sheba, Dubai, UAE ("**EchoNova**"), and the business that holds an EchoNova account (the "**Customer**").

The Customer accepts this DPA online, by accepting the Platform Terms or the Enterprise Terms when opening or upgrading its account. No separate signature is needed. The acceptance date, version and account are recorded by EchoNova.

It forms part of the Platform Terms or the Enterprise Terms, whichever applies to the Customer's account (the "**Agreement**"). If this DPA and the Agreement conflict on data protection, this DPA prevails.

1. Definitions

1.1 "**Data Protection Law**" means all laws on personal data that apply to the processing under this DPA, including:

- the UAE Personal Data Protection Law (Federal Decree-Law No. 45 of 2021) and its implementing regulations ("**UAE PDPL**");
- the Saudi Personal Data Protection Law (Royal Decree No. M/19 of 1443H, as amended) and its implementing and transfer regulations ("**KSA PDPL**"); and
- where the Customer is subject to it, the EU General Data Protection Regulation ("**GDPR**").

1.2 "**Customer Personal Data**" means personal data that EchoNova processes for the Customer under the Agreement, including call audio, voice messages, transcripts, chat and messaging content, phone numbers, and AI-generated summaries or actions.

1.3 "**Personal Data Breach**" means a breach of security that leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data.

1.4 "**Subprocessor**" means a third party that EchoNova engages to process Customer Personal Data.

1.5 "Controller", "processor", "data subject", "processing" and "sensitive personal data" have the meanings given in the Data Protection Law that applies.

2. Roles

2.1 The Customer is the **controller** and EchoNova is the **processor** of Customer Personal Data.

2.2 EchoNova is a separate controller only for the account, billing and usage data it needs to run its business. Its Privacy Policy covers that data.

2.3 The details of the processing are set out in **Annex 1**.

3. EchoNova's obligations

EchoNova will:

- 3.1 process Customer Personal Data only on the Customer's **documented instructions**, which are the Agreement, this DPA, and the Customer's configuration and use of the platform. If EchoNova believes an instruction breaks the Data Protection Law, it will tell the Customer. If the law requires EchoNova to process the data otherwise, it will tell the Customer first, unless the law forbids it;
- 3.2 ensure everyone authorised to process Customer Personal Data is bound by **confidentiality**;
- 3.3 implement the **security measures** in **Annex 2**, and keep them appropriate to the risk;
- 3.4 keep a **record** of the processing it carries out for the Customer;
- 3.5 **assist the Customer**, taking into account the nature of the processing, with data subject requests, security, breach notification, data protection impact assessments, and consultations with regulators;
- 3.6 make available the information needed to show compliance with this DPA (section 9).

4. AI models and training

- 4.1 The Customer instructs and authorises EchoNova to use Customer Personal Data, de-identified where possible, to train, fine-tune and evaluate EchoNova's own models, unless the Customer turns this off in its account settings. Turning it off applies from then on, not to data already used. The Customer is responsible for telling data subjects about this use and for having a lawful basis for it.
- 4.2 EchoNova will contractually prohibit its Subprocessors, including any provider of AI models, from using Customer Personal Data to train or improve their models.
- 4.3 **Voice cloning and biometrics.** EchoNova will not create a voiceprint or synthetic voice from any data subject's voice unless the Customer has enabled that feature in writing and has confirmed it holds the data subject's explicit consent.

5. Customer's obligations

The Customer:

- 5.1 is responsible for having a **lawful basis** for the processing and for giving data subjects the required notices. In particular, it is responsible for informing callers that they are speaking with AI, and for obtaining any consent the law requires before calls are recorded or transcribed (see the Acceptable Use Policy);
- 5.2 will not send EchoNova categories of data restricted by section 2.7 of the Acceptable Use Policy without EchoNova's prior written agreement;
- 5.3 is responsible for its own decisions based on AI output.

6. Subprocessors

- 6.1 The Customer **authorises** the Subprocessors listed in **Annex 3**.
- 6.2 EchoNova will give at least **30 days' notice** before adding or replacing a Subprocessor, by email or through a subscription to its subprocessor page. 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 Services and receive a refund of prepaid fees for the unused period.

6.3 EchoNova will impose data protection terms on each Subprocessor that are at least as protective as this DPA, and remains **responsible** to the Customer for its Subprocessors.

7. International transfers

7.1 EchoNova will store Customer Personal Data in the hosting region(s) stated in Annex 1. It will not move the data to another country without the Customer's prior written agreement, except for the Subprocessor access listed in Annex 3.

7.2 Every transfer out of the UAE must meet the UAE PDPL's conditions for cross-border transfers. Every transfer out of Saudi Arabia must meet the KSA PDPL transfer regulations. Where needed, the parties will sign the transfer clauses required by the relevant regulator or, for GDPR, the European Commission's standard contractual clauses.

7.3 If a public authority asks EchoNova for Customer Personal Data, EchoNova will refer the authority to the Customer and tell the Customer promptly, unless the law forbids this.

8. Personal Data Breaches

8.1 EchoNova will notify the Customer **without undue delay, and in any case within 24 hours** of becoming aware of a Personal Data Breach.

8.2 The notice will include, as far as known: what happened; the categories and approximate number of data subjects and records affected; the likely consequences; and the steps taken or proposed. EchoNova will add information as it becomes available.

8.3 EchoNova will help the Customer meet its own duties to notify regulators and data subjects within the time limits of the Data Protection Law: under the UAE PDPL, the UAE Data Office, within the period set by the implementing regulations; under the KSA PDPL, SDAIA, within the regulations' time limit of 72 hours; and the GDPR regulator within 72 hours where the GDPR applies.

8.4 Notifying a breach is not an admission of fault.

9. Audits

9.1 On request, no more than once a year (or after a Personal Data Breach, or when a regulator requires it), EchoNova will answer a reasonable security questionnaire and provide its security policies and any available audit reports or certificates.

9.2 If that is not enough to show compliance, the Customer may carry out an audit itself or through an independent auditor bound by confidentiality, on **30 days' notice**, during business hours, and in a way that does not disrupt the Services or expose other customers' data. The Customer bears its own audit costs, unless the audit reveals a material breach by EchoNova.

10. Return and deletion

10.1 During the Agreement, the Customer can export or delete conversation data through the platform, or by request to EchoNova.

10.2 When the Agreement ends, EchoNova will, at the Customer's choice made within **30 days**, return the Customer Personal Data in a common machine-readable format, and then **delete** it, including copies held by Subprocessors, within **60 days** of the end date. Backups will be overwritten within **90 days**.

10.3 EchoNova may keep data only where the law requires it, and then only for that purpose and under this DPA. On request it will confirm deletion in writing.

11. Liability

Each party's liability under this DPA is subject to the limitations in the Agreement. Each party is responsible for regulatory fines imposed on it for its own breach.

12. Term, law and disputes

12.1 This DPA lasts as long as EchoNova processes Customer Personal Data for the Customer.

12.2 The governing law and dispute resolution clauses of the Agreement apply, unless the Data Protection Law requires otherwise.

Accepted online with the Platform Terms or the Enterprise Terms.

Annex 1: Details of the processing

ITEM	DETAILS
Data subjects	the Customer's own customers and other people who contact or are contacted through the platform; the Customer's staff who use it
Personal data	call audio; voice messages; transcripts; chat, SMS, email and WhatsApp content; phone numbers and messaging IDs; names and other details people provide; AI summaries, classifications and actions; technical logs
Sensitive data	not intended. People may volunteer sensitive information (for example health details) during a conversation. The Customer must tell EchoNova in advance if its use case involves sensitive data on purpose.
Nature and purpose	speech-to-text, text-to-speech, conversational AI responses and actions in the Customer's workflows, storage, analytics for the Customer, and support
Duration	the term of the Agreement plus the deletion period in section 10
Customer retention setting	as set by the Customer in its account settings
Hosting region(s)	Microsoft Azure, UAE North (platform, database, files); Amazon Web Services, Europe (Stockholm, eu-north-1) for speech processing
Customer contact for data protection	the account owner's email, unless the Customer adds another contact in its account settings

ITEM	DETAILS
EchoNova contact for data protection	privacy@echonova.ai

Annex 2: Security measures

AREA	MEASURE
Access control	individual named accounts for every person with production access; least privilege; access removed when someone leaves
Authentication	multi-factor authentication for cloud consoles and administrative access
Encryption	data encrypted in transit (TLS 1.2 or higher) and at rest in production storage
Logging and monitoring	audit logging of production access (for example Azure Activity Log and AWS CloudTrail) with alerts for suspicious activity
Backups	automated, encrypted backups of production data, with a tested restore
Incident response	documented incident response plan with named roles
Vendor access	outsourced providers have restricted, logged and revocable access
Network	DDoS protection and firewalls on production services
Separation	data from customers who have turned training off is kept out of the model-training environment
People	confidentiality agreements for all staff and contractors; security awareness training
Development	code review and change management for production changes
Programme	information security management system being built towards ISO/IEC 27001 and ISO/IEC 42001 (not yet certified)

Annex 3: Authorised subprocessors

SUBPROCESSOR	SERVICE	DATA	LOCATION
Microsoft	cloud hosting (production): platform, database (through MongoDB Atlas), file storage, cache and secrets; language models (Azure AI Foundry); sign-in with Microsoft, when a user chooses it	all Customer Personal Data	UAE North. Language model requests and sign-in with Microsoft may be processed in other Microsoft regions.

SUBPROCESSOR	SERVICE	DATA	LOCATION
MongoDB Inc.	database (MongoDB Atlas)	all Customer Personal Data held in the database	UAE North, on Microsoft Azure
Amazon Web Services	speech processing and speech storage; email delivery (Amazon SES); website delivery (Amazon CloudFront)	text and audio sent for speech processing; name and email address; website requests	Europe (Stockholm, eu-north-1) for speech; US East (N. Virginia, us-east-1) for email; global for website delivery
Cloudflare	DNS, content delivery, bot checks (Turnstile) and cookieless website statistics	website requests, including IP address	global
Twilio	phone calls, SIP and SMS	call audio, phone numbers, SMS messages	United States
Meta Platforms	WhatsApp, Messenger and Instagram channels, where the Customer connects them	messages, phone numbers, account identifiers	Meta's own regions
Stripe	payment processing	billing data	Stripe's own regions
PayPal	payment processing	billing data	PayPal's own regions
Paymob	payment processing	billing data	Paymob's own regions
Google	sign-in with Google; Google Calendar, where the Customer connects it	name and email address; calendar events	Google's own regions
Slack	Slack integration, where the Customer connects it	messages	Slack's own regions
Zendesk	helpdesk integration, where the Customer connects it	support tickets and messages	Zendesk's own regions
Zoho	helpdesk integration, where the Customer connects it	support tickets and messages	Zoho's own regions
Intercom	helpdesk integration, where the Customer connects it	support conversations	Intercom's own regions
Genesys	contact-centre integration, where the Customer connects it	messages and call audio	Genesys's own regions