Sysevo · Published website snapshot · Captured 21 November 2026
Source: https://www.sysevo.io/legal/dpa
Engagement-specific signed terms remain governed by their agreements.

Last updated: July 2026

Data Processing Agreement (DPA)

This Data Processing Agreement ("**DPA**") forms part of, and is incorporated into, the Terms of Service between you (the "**Customer**", "you") and Sysevo Ltd, a company registered in England and Wales (company number 17329455) with its registered office at Suite Ra01, 195-197 Wood Street, London, United Kingdom, E17 3NU ("**Sysevo**", "we", "us"). It sets out the terms on which we process personal data on your behalf when you use the Sysevo voice AI, CRM, payments, finance, and business platform (the "**Services**"), and reflects the requirements of Article 28 of the UK General Data Protection Regulation (UK GDPR) and the EU GDPR (together, "**GDPR**") and the Data Protection Act 2018.

Where there is a conflict between this DPA and the Terms of Service on the subject of data protection, this DPA prevails. Read it alongside our Privacy Policy and Cookie Policy.

1. Definitions

Terms such as "controller", "processor", "data subject", "personal data", "special category data", "processing", "sub-processor", and "supervisory authority" have the meanings given in the GDPR. "**Customer Personal Data**" means personal data contained in Customer Data that we process on your behalf under the Services. "**Data Protection Law**" means the UK GDPR, EU GDPR, the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 (PECR), and any other applicable data-protection or e-privacy law.

2. Roles of the Parties

The parties acknowledge that, in respect of Customer Personal Data processed through the platform (for example CRM records, caller and contact details, call recordings and transcripts, form submissions, and documents), **you are the controller** (or, where you act on behalf of a third party such as a white-label client, the processor) and **Sysevo is the processor** (or sub-processor). Sysevo processes such data only on your documented instructions.

Separately, Sysevo acts as an independent **controller** for the account, billing, support, and website data of Customers and their users — that processing is governed by our Privacy Policy, not this DPA. Where you connect your own third-party payment account (for example your own Stripe or PayPal), that provider processes payment data under your own agreement with it, and you — not Sysevo — are the merchant of record (see the Terms).

3. Your Instructions and Responsibilities

We will process Customer Personal Data only: (a) to provide, secure, support, and improve the Services in accordance with the Terms; (b) as further documented in your use and configuration of the Services and any written instructions you give; and (c) as required by law (in which case we will inform you unless legally prohibited). If we believe an instruction infringes Data Protection Law, we will notify you.

You are responsible for: the accuracy, quality, and legality of Customer Personal Data and the means by which you acquired it; having a valid lawful basis and giving all required notices and obtaining all required consents (including for call recording, automated/AI interaction, marketing, and any lead sourcing or enrichment); and ensuring your instructions to us comply with Data Protection Law. You must not use the Services to process personal data for which you have no lawful basis.

4. Subject Matter, Duration, Nature, and Purpose of Processing

- **Subject matter:** our processing of Customer Personal Data to provide the Services.
- **Duration:** for the term of the Terms of Service and until deletion or return of Customer Personal Data in accordance with section 11 (subject to any legal retention requirement).
- **Nature and purpose:** hosting, storage, and transmission; running inbound and outbound AI voice agents and telephony; recording, transcribing, summarising, scoring, and analysing calls; caller memory; CRM, pipeline, campaign, booking, forms, document-vault, and finance functionality; facilitating payments through your own payment provider; and related support, security, and analytics — all as further described in Annex 1.

5. Categories of Data Subjects and Personal Data

The categories of data subjects and personal data are set out in Annex 1. They may include special category data (for example health-related data in dental or veterinary use) where you choose to process it; you are responsible for ensuring an applicable condition and appropriate safeguards apply, and you must not upload special category or highly sensitive data unless the Services and your configuration are appropriate for it.

6. Confidentiality

We ensure that personnel authorised to process Customer Personal Data are bound by appropriate confidentiality obligations and are informed of the confidential nature of the data. Access is limited to personnel who need it to provide, support, or secure the Services.

7. Security of Processing

Taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing, as well as the risk to individuals, we implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as described in Annex 2. You are responsible for your own security controls, including safeguarding credentials and configuring access, and for assessing whether the measures meet your requirements.

8. Sub-Processors

You provide general authorisation for us to engage sub-processors to process Customer Personal Data in order to provide the Services. Our current sub-processors are listed in Annex 3. We impose data-protection obligations on each sub-processor that are no less protective than those in this DPA, and we remain responsible to you for a sub-processor's performance of its obligations.

We will give at least **30 days' notice** (by email or through the Services) before adding or replacing a sub-processor that processes Customer Personal Data, so that you may object on reasonable data-protection grounds. If you object and we cannot reasonably accommodate the objection, you may terminate the affected part of the Services as your remedy.

9. Data Subject Rights

Taking into account the nature of the processing, we will assist you by appropriate technical and organisational measures, insofar as possible, to respond to requests from data subjects to exercise their rights (access, rectification, erasure, restriction, portability, and objection). The Services also provide self-service tools (for example export and deletion features) that let you respond to many such requests directly. If we receive a request directly from a data subject relating to your Customer Personal Data, we will, unless legally required to act, refer them to you and, where appropriate, inform you.

10. Assistance, Breach Notification, and DPIAs

Taking into account the nature of processing and the information available to us, we will assist you in ensuring compliance with your obligations under Articles 32 to 36 of the GDPR, including security, personal-data-breach notification, and data protection impact assessments and prior consultation.

We maintain procedures to detect and respond to personal-data breaches. We will notify you **without undue delay** after becoming aware of a personal-data breach affecting Customer Personal Data, and will provide the information reasonably available to us to help you meet your own notification obligations (which, where applicable, include notifying your supervisory authority within 72 hours and affected individuals where the risk is high). Our notification is not an acknowledgement of fault or liability.

11. Return and Deletion of Data

On termination or expiry of the Services, and at your choice, we will delete or return Customer Personal Data, and delete existing copies, unless we are required by law to retain it. During your subscription and for a limited period after termination (where you are not in material breach), you can export Customer Data through the Services. Residual copies held in routine backups are deleted or overwritten in the ordinary course of our backup cycle.

12. Audits and Information

We will make available to you information reasonably necessary to demonstrate compliance with this DPA and Article 28, and will allow for and contribute to audits, including inspections, conducted by you or an auditor you mandate. Audits are subject to reasonable prior notice, confidentiality obligations, no more than once per year (unless required by a supervisory authority or following a breach), and conduct that does not disrupt our operations or compromise the security or confidentiality of other customers. Where available, we may satisfy audit requests by providing relevant third-party reports, security documentation, or a completed security questionnaire.

13. International Transfers

Some of our sub-processors are located outside the UK and EEA, including in the United States (see Annex 3). Where Customer Personal Data is transferred internationally, we rely on an adequacy decision or adequacy regulations where one applies, or on appropriate safeguards — the UK International Data Transfer Agreement (IDTA), the UK Addendum to the EU Standard Contractual Clauses (SCCs), or the SCCs — together with supplementary measures where needed. You authorise these transfers for the purpose of providing the Services, and further details of the relevant safeguards are available on request.

14. Liability and Term

Each party's liability under or in connection with this DPA is subject to the limitations and exclusions of liability set out in the Terms of Service. This DPA takes effect when you accept the Terms or first use the Services and continues for as long as we process Customer Personal Data on your behalf.

15. Supervisory Authority and Contact

Sysevo is a UK-based company, and our lead supervisory authority is the UK Information Commissioner's Office (ICO). If you are in the EU/EEA, your local supervisory authority may apply. For data-protection enquiries, to exercise audit rights, or to request a countersigned copy of this DPA, contact privacy@sysevo.io.

Annex 1 — Details of Processing

Categories of data subjects

- Your contacts, leads, and customers ("End Users");
- People who call, or are called by, your voice agents (callers and call recipients);
- People who book appointments, reservations, or bookings, and guests or attendees;
- People who submit forms or whose details appear in documents you upload;
- For industry-specific modules, the relevant individuals (for example patients in dental, animal owners in veterinary, guests in hospitality/rentals, buyers/sellers in real estate);
- Your own personnel and Authorised Users of your account.

Categories of personal data

Category	Examples
Identity & contact	Names, email addresses, telephone numbers, postal and business addresses, job titles
Call & voice data	Call recordings and transcripts, caller and recipient phone numbers, call duration, timestamps, outcomes, sentiment and AI scoring output, caller-memory and conversation history
CRM & pipeline	Contact records, notes, tags, deal/pipeline information, communication history
Booking & scheduling	Appointment, reservation, and booking details, availability, attendance
Forms & documents	Form submissions and uploaded documents/files (contents defined by you)
Payment-related	Transaction, invoice, and billing records and status. Full card details are handled by the relevant payment provider and are not stored by Sysevo.

Category	Examples
Verification (KYC)	Business and identity details and documents used for telephony/carrier registration
Technical & usage	IP address, device/browser data, identifiers, and usage/log data
Special category (if you choose to process it)	For example health-related data in dental or veterinary use. You are responsible for the applicable condition and safeguards.

Nature, purpose, and duration

As set out in section 4: processing to host, run, secure, support, and improve the Services (voice agents and telephony, recording/transcription/analysis, caller memory, CRM, campaigns, bookings, forms, vault, finance, and payment facilitation), for the term of the Terms and until deletion or return under section 11.

Annex 2 — Technical and Organisational Security Measures

We implement measures including, as applicable:

- **Encryption:** encryption of data in transit (TLS) and encryption of data at rest in our database and storage.
- **Tenant isolation & access control:** logical separation of customer data enforced by row-level security at the database; role-based, least-privilege access; scoped, environment-held credentials, with elevated keys never exposed to the browser.
- **Authentication:** managed authentication with securely handled session tokens; passwords are not stored by us in plain text.
- **Secrets management:** sensitive credentials (including any payment-provider keys you connect) held in a dedicated secrets vault rather than plain database columns.
- **Payment data minimisation:** card processing is performed by the payment provider; we do not store full card numbers, keeping our own PCI DSS scope minimal.
- **Resilience & backups:** vendor-managed, patched cloud infrastructure with automated backups and recovery capability.
- **Logging & monitoring:** application and access logging and monitoring, and error reporting, to detect and investigate issues.
- **Organisational measures:** confidentiality obligations on personnel, access limited to those who need it, and change-management and secure-development practices.
- **Incident response:** procedures to detect, investigate, and respond to security incidents and personal-data breaches.

We continue to develop our security programme; our current posture, including the status of formal certifications, is described honestly on our security page.

Annex 3 — Sub-Processors

We engage the sub-processors below to process Customer Personal Data in order to provide the Services. Most operate internationally; where they process data outside the UK/EEA (typically in the United States), transfers are covered by the mechanisms in section 13 (UK IDTA / UK Addendum to the SCCs / SCCs), and several providers are also certified under the EU–US and UK–US Data Privacy Framework. The legal entity that contracts with you for a given provider, and the exact processing region, can depend on your location and configuration (for example your selected data region and which optional features you enable).

Sub-processor (legal entity)	**Purpose**	**Processing region & transfer basis**
Supabase, Inc.	Application & database hosting, authentication, file storage, and serverless functions (core infrastructure)	Customer data hosted on AWS in the EU (Frankfurt / Ireland); provider is US-incorporated, so any support-related US access is covered by SCCs / UK Addendum
Twilio Inc. (and Twilio Ireland Limited)	Telephony, phone-number provisioning, and carrier / A2P (10DLC) identity registration	United States; Binding Corporate Rules / SCCs
Deepgram, Inc.	Speech-to-text (call transcription)	United States (EU option available); SCCs
ElevenLabs, Inc.	Text-to-speech (voice synthesis) and transcription	United States (EU residency on higher tiers); SCCs / Data Privacy Framework
OpenAI, LLC (OpenAI Ireland Ltd for EEA)	Large language model inference for agents and AI features	United States; SCCs / UK Addendum
Anthropic, PBC	Large language model inference for agents and AI features	United States; SCCs
Google Ireland Limited / Google Cloud EMEA Limited (and Google LLC)	AI model (Gemini) inference; calendar and meeting integration; fonts	EU / United States; SCCs
X.AI LLC	Large language model inference (where selected)	United States; SCCs
Stripe Payments Europe, Limited (and Stripe, Inc.)	Payment processing for Sysevo billing, and facilitation of payments through your connected Stripe account	EU (Ireland) / United States; UK IDTA / SCCs
PayPal (Europe) S.à r.l. et Cie, S.C.A. (and PayPal UK Ltd)	Alternative payment processing for certain invoices	EU (Luxembourg) / UK

Sub-processor (legal entity)	Purpose	Processing region & transfer basis
Squareup International Limited / Squareup Europe Ltd (Block, Inc.)	Read-only financial ledger synchronisation for finance features (where connected)	EU (Ireland) / UK / United States; SCCs
Resend (Plus Five Five, Inc.)	Transactional and notification email delivery	United States; Data Privacy Framework (UK extension)
Vercel Inc.	Website hosting and privacy-preserving analytics	United States; Data Privacy Framework

Additional speech, model, or integration providers may be used where you enable a specific feature or connect a third-party service; where you connect your own account with a provider (for example your own payment provider), that provider acts under your agreement with it. A definitive, current sub-processor list — including the specific contracting entity and processing region applicable to your account — is available on request at privacy@sysevo.io.

Contact

Sysevo Ltd, Suite Ra01, 195-197 Wood Street, London, United Kingdom, E17 3NU. Data-protection enquiries and DPA requests: privacy@sysevo.io.