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

Last updated: 31 October 2026

Privacy Policy

This Privacy Policy explains, in full, how Sysevo Ltd, a company registered in England and Wales (company number 17329455) with its registered office in Suite Ra01, 195-197 Wood Street, London, United Kingdom, E17 3NU ("**Sysevo**", "we", "us", or "our"), collects, uses, shares, retains, and protects personal data when you use our website at sysevo.io and our voice AI, CRM, payments, and business platform at app.sysevo.io (together, the "**Services**"), and when you interact with us in other ways.

We are the "data controller" for the personal data described in this policy where we decide how and why it is processed. We process personal data in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 (PECR), and — where it applies to you — the EU GDPR. Read this policy alongside our Cookie Policy, Data Processing Agreement, and Terms of Service.

This policy is designed to be complete: it tells you what we collect, where it comes from, why we use it, the legal basis for every use, who we share it with, where it goes, how long we keep it, how we protect it, and the rights you have. If anything is unclear, contact privacy@sysevo.io.

1. Quick Summary

- We act as a **controller** for account, billing, website, and marketing data, and as a **processor** for the caller and CRM data you handle on the platform.
- We use data to provide and secure the Services, take payments, meet legal and verification (KYC) duties, support and improve the Services, and — with your consent or where permitted — for marketing and sales follow-up.
- We **do not sell** your personal data, and we **do not use your Customer Data to train general AI models** without your opt-in.
- You have rights to access, correct, delete, restrict, port, and object, and to complain to the ICO.

2. Our Two Roles: Controller and Processor

- **As a controller** — for the personal data of our account holders, Authorised Users, website visitors, prospects, and contacts (for example your account details, billing information, communications, and marketing data). This policy governs that processing.

- **As a processor** — when you, as a platform customer, use Sysevo to process personal data about your own contacts, callers, and clients ("End Users"), you are the controller and we process that data on your documented instructions under our Data Processing Agreement. If you are an End User of one of our customers, that customer's privacy notice governs their use of your data, and you should contact them to exercise your rights.

3. Personal Data We Collect

3.1 Information you provide to us

- **Account & identity:** first and last name, email address, phone number, password (stored only in hashed form by our authentication provider), and profile details such as timezone, language, and avatar.
- **Business & verification (KYC):** company name and business address, and, where telephony or carrier registration requires it, know-your-customer information and verification documents (for example for 10DLC or Ofcom-related number registration).
- **Payment & financial:** billing details and, for relevant features, payout and bank details you provide (such as account holder name, IBAN/BIC, sort code, and payment-method type). Card payments are handled by our payment processor — we do not store full card numbers.
- **Communications:** messages and information you send via contact and demo forms, email, chat, or support, and records of those interactions.
- **SMS marketing consent:** the U.S. phone number you submit, whether you selected the optional SMS consent checkbox, the exact consent wording and version shown, the submission time, and the source form URL. We use this record to document and administer your SMS subscription and consent choices.
- **Content you upload:** agent scripts, prompts, knowledge bases, documents, contacts, and other content you add to configure and run the Services.
- **Event & preference data:** demo bookings, event registrations, survey responses, and marketing preferences.

3.2 Information we collect automatically

- **Log & technical data:** IP address, browser and device type, operating system, device identifiers, referring URLs, and access timestamps.
- **Usage data:** features used, pages and screens viewed, actions taken, call volumes, and agent configurations.
- **Cookies & similar technologies:** see our Cookie Policy. Non-essential analytics load only with your consent.

3.3 Voice and call data (platform customers)

When you use the platform to run Voice Agents and the CRM, the Services process — on your behalf as processor — data such as call recordings and transcripts, caller phone numbers and metadata, call duration and outcomes, caller memory, sentiment and scoring output, and the CRM and pipeline records you create. You are responsible for having a lawful basis and for giving any required notices (for example telling callers a call is recorded and that they are speaking with an AI system).

3.4 Information from other sources

We may receive information from: our payment processor (for example payment and verification status); integrations and connectors you enable; providers that help us verify accounts or prevent fraud; and publicly available sources for business contact and marketing purposes where permitted.

3.5 Special category and children's data

We do not intentionally collect special-category data (such as health, biometric, or similar data) about our own account holders as a controller. Where platform customers process such data about their End Users, they do so as controller and are responsible for the additional conditions and safeguards the law requires. The Services are for business use and are not directed at children; we do not knowingly collect data from anyone under 18.

4. Why We Use Personal Data and Our Legal Bases

As a controller, we use personal data for the purposes below. The legal basis under UK GDPR is shown for each. Where more than one basis applies, we rely on whichever is appropriate for the specific processing.

Purpose	Why	Legal basis
Register and administer your Account; deliver the Services	To let you use what you signed up for	Performance of a contract
Process payments, billing, subscriptions, and wallets	To take payment and keep financial records	Contract; legal obligation (tax/accounting)
Verify identity and meet telephony/KYC and anti-fraud requirements	To register numbers and prevent misuse	Legal obligation; legitimate interests
Provide support and respond to your enquiries	To help you and resolve issues	Contract; legitimate interests
Secure, monitor, and troubleshoot the Services; prevent abuse and fraud	To keep the Services safe and reliable	Legitimate interests; legal obligation

Purpose	Why	Legal basis
Improve, develop, and analyse usage of the Services	To make the product better	Legitimate interests; consent (non-essential analytics)
Send service and transactional messages (confirmations, invoices, security and account notices)	To operate your account	Contract; legitimate interests
Send marketing and sales follow-up about our products, offers, and events	To tell you about relevant products	Consent, or legitimate interests / PECR "soft opt-in" where permitted (opt out any time)
Manage business relationships, partners, and resellers	To run partnerships and referrals	Contract; legitimate interests
Establish, exercise, or defend legal claims; enforce our Terms	To protect our rights	Legitimate interests; legal obligation
Comply with legal, regulatory, and tax obligations	Because the law requires it	Legal obligation
Corporate transactions (merger, acquisition, financing)	To run or transfer the business	Legitimate interests

Where we rely on **legitimate interests**, we have carried out a balancing assessment to ensure our interests do not override your rights, and we will provide a summary on request. Where we rely on **consent**, you may withdraw it at any time without affecting processing carried out before withdrawal.

5. Marketing and Sales Communications

If you sign up, book a demo, contact us, or become a customer, we may contact you about your account and — where you have consented or we are otherwise permitted (including the PECR "soft opt-in" for existing customers and similar products) — about sales, onboarding, relevant products, offers, and events. Marketing text messages are sent only if you separately and expressly opt in through the Sysevo SMS updates form. That consent is optional and is not required to purchase or use any Sysevo service. The SMS program covers recurring marketing messages about Sysevo's AI voice agent and business software products, demos, product news, and promotional offers. Message frequency varies and message and data rates may apply. The signup form records your choice and confirms it on the webpage; it does not send a text at signup. We will send marketing texts only when the program is active and the required messaging registration is approved. When messages are sent, you may reply STOP to opt out or HELP for help. You may also withdraw SMS consent by contacting privacy@sysevo.io. We will stop marketing texts to an opted-out number; opting out of marketing does not stop essential service messages about an account where those are otherwise permitted.

SMS data and sharing. We do not sell or share your SMS opt-in data or personal information with third parties for marketing purposes. We do not sell, rent, or transfer SMS opt-in consent to affiliates or other senders. If the SMS program is active, we may provide a messaging service provider such as Twilio with the phone number, message content, delivery details, and reply or opt-out information needed to transmit messages you requested, handle replies and opt-outs, protect the service, and keep required records. These providers act as service providers for these purposes and may not use this information for their own marketing or promotional purposes. We also store the consent wording/version, timestamp, and source form with our application database provider so we can administer the subscription and retain proof of consent.

6. AI Processing and Voice Data

The Services use AI to power Voice Agents and features such as transcription, summaries, caller memory, and call scoring. To deliver these, relevant content (for example call audio and text) may be processed by our AI-model, speech-to-text, and text-to-speech sub-processors strictly on our instructions and to provide the Services to you. We do not sell personal data, and we **do not use your Customer Data to train our own or third parties' general AI models** except where you have expressly opted in or the law requires. AI output can be imperfect and should be reviewed before you rely on it (see our Terms).

7. Automated Decision-Making and Profiling

Some features (such as AI call scoring and sentiment) analyse calls to produce insights and may involve a degree of profiling. As a controller, we do not make decisions producing legal or similarly significant effects about you based solely on automated processing without a lawful basis and appropriate safeguards, including the ability to obtain human review. Where a platform customer uses such features on their End Users, that customer is the controller and is responsible for meeting these requirements.

8. How We Share Personal Data

We do not sell your personal data. We share it only as needed to run the Services and as described here:

- **Sub-processors / service providers** who process data on our behalf, covering: cloud application and database hosting and authentication; website hosting and privacy-preserving analytics; payment processing; transactional email; AI model providers; speech-to-text and text-to-speech; and telephony, number verification, and integration connectors. A full, named list of sub-processors is available on request under a signed DPA, and we give at least 30 days' notice before adding or replacing one for customers under a signed DPA. All are bound by contract to protect personal data and to process it only on our instructions.
- **Payment processor** (such as Stripe), which handles card data under its own terms; we do not store full card details.
- **Professional advisers** (lawyers, accountants, auditors, insurers) where reasonably necessary.
- **Legal, safety, and compliance** — where required by law, valid legal process, or to establish, exercise, or defend legal claims, or to protect our rights, users, or the public.
- **Business transfers** — in connection with a merger, acquisition, financing, reorganisation, or sale of assets, subject to this policy.

9. International Data Transfers

We are based in the UK, and some of our providers are located outside the UK/EEA, including in the United States. Where we transfer personal data internationally, we rely on an adequacy decision or adequacy regulations where one exists, or on appropriate safeguards such as the UK International Data Transfer Agreement (IDTA), the UK Addendum to the EU Standard Contractual Clauses (SCCs), or the SCCs, together with additional technical and organisational safeguards where needed. You can request more information about a specific transfer or a copy of the relevant safeguards by contacting privacy@sysevo.io.

10. How Long We Keep Data

We keep personal data only as long as necessary for the purposes above, to meet legal, tax, and regulatory requirements, and to establish or defend legal claims. General retention periods are:

Data	Retention
Account & profile data	For the life of your account, then up to 2 years after closure
Call recordings & transcripts (platform)	Per your activated plan, settings and lawful processing instructions. Self-Serve recording-history targets are up to 30 days for Voice, 90 days for Connect, six calendar months for Scale, nine for Core and twelve for Pro. Where history or deletion controls are marked pending, these targets are still being verified and do not confirm that longer history or automatic deletion is active. Contact privacy@sysevo.io to confirm current handling, request an export or request earlier deletion. A maximum history allowance does not require keeping data longer than necessary.

Data	Retention
Payment & invoicing records	Up to 7 years (tax and accounting law)
KYC / verification records	As required by the relevant carrier or regulatory requirement
Support & communications	Up to 3 years after the interaction
Marketing data	Until you unsubscribe or object, then suppression-list only
SMS consent and compliance records	While consent remains active and at least until you withdraw it; after withdrawal, only the limited consent and suppression information needed to honour the opt-out and demonstrate compliance is retained for as long as necessary, then deleted or anonymised.
Backups & logs	Rolling short-term retention, then overwritten

When data is no longer needed, we securely delete or irreversibly anonymise it.

11. How We Protect Data

We use appropriate technical and organisational measures, including: encryption in transit (TLS) and at rest; tenant data isolation using row-level security; access controls, least-privilege credentials, and authentication; secure payment handling via our processor (we do not store card numbers); regular automated backups; logging and monitoring; and vendor-managed, patched cloud infrastructure. See our security page for detail. No system is perfectly secure; you are responsible for keeping your credentials safe and for the security of your own devices and integrations.

12. Personal Data Breaches

We maintain procedures to detect, investigate, and respond to personal-data breaches. Where a breach is likely to result in a risk to individuals' rights, we will notify the ICO within 72 hours where required, and affected individuals without undue delay where the risk is high. Where we act as your processor, we will notify you without undue delay so you can meet your own obligations, as set out in the DPA.

13. Your Rights

Subject to conditions under UK GDPR, you have the right to:

- **Be informed** — about how we use your data (this policy);
- **Access** — obtain confirmation and a copy of your personal data;

- **Rectification** — correct inaccurate or incomplete data;
- **Erasure** — ask us to delete your data in certain circumstances;
- **Restriction** — limit how we process your data;
- **Portability** — receive certain data in a structured, machine-readable format, or have it transmitted to another controller;
- **Object** — object to processing based on legitimate interests, and to direct marketing at any time (which we always honour);
- **Rights around automated decisions** — as described in section 7;
- **Withdraw consent** — where processing is based on consent.

To exercise your rights, contact privacy@sysevo.io. We respond within one month (extendable by two further months for complex or numerous requests, with notice). We may need to verify your identity, and requests are usually free unless manifestly unfounded or excessive. If you are an End User of one of our customers, please contact that customer, who is the controller of your data.

14. Your Responsibilities as a Controller (Platform Customers)

If you use the platform to process personal data about your End Users, you are the controller of that data. You are responsible for: having a lawful basis; providing your own privacy notice to your End Users; obtaining any consents and giving any notices required (including for call recording and automated/AI interaction); honouring your End Users' rights; and instructing us lawfully. Our processing on your behalf is governed by the DPA.

15. Third-Party Links and Services

Our Services may link to, or integrate with, third-party sites and services we do not control (for example telephony, payment, and integration providers). Their processing is governed by their own privacy notices, and we are not responsible for them. Please review their policies.

16. Changes to This Policy

We may update this policy from time to time. For material changes we will give reasonable notice by email or through the Services, and we will update the "Last updated" date above. Your continued use of the Services after changes take effect indicates acceptance where permitted by law.

17. Contact, Data Protection Contact, and Complaints

For privacy enquiries or to exercise your rights, contact our data protection contact at privacy@sysevo.io.

Sysevo Ltd, Suite Ra01, 195-197 Wood Street, London, United Kingdom, E17 3NU.

Our lead supervisory authority is the UK Information Commissioner's Office (ICO). You have the right to complain to the ICO at ico.org.uk or by calling its helpline, though we would appreciate the chance to resolve your concern first. If you are in the EEA, you may also complain to your local supervisory authority.