AutomatusLabs

Privacy Policy

How AutomatusLabs collects, uses, stores, and protects personal information when you use our AI-powered voice calling and SMS automation platform.

Document	Privacy Policy
Version	3.0
Last Updated	April 2026
Effective Date	1 April 2026
Data Controller	AutomatusLabs Ltd, London, United Kingdom
Contact	support@automatuslabs.com
Website	https://automatuslabs.com

This Privacy Policy is issued under the UK General Data Protection Regulation (UK GDPR), the EU General Data Protection Regulation (EU GDPR 2016/679), the Data Protection Act 2018, and the California Consumer Privacy Act (CCPA) as amended by the CPRA. It also incorporates the commitments required by the Google API Services User Data Policy.

Table of Contents

At a glance

We collect only what we need to deliver our service, we never sell your personal data, we never use your data or Google user data to train artificial-intelligence models, and we never share it with third parties for advertising. You can export, correct, or delete your data at any time by contacting support@automatuslabs.com.

1. Introduction and Who We Are

AutomatusLabs Ltd ("**AutomatusLabs**", "**we**", "**us**", or "**our**") is a private company limited by shares registered in England and Wales with its principal place of business in London, United Kingdom. AutomatusLabs operates the website https://automatuslabs.com, the AutomatusLabs desktop application (a Microsoft Windows Electron application), and the associated cloud backend that together constitute the "**Service**".

The Service provides small-business customers with an AI-powered voice-calling and SMS-automation platform. Using the Service, a business client can (a) synchronise its calendar, (b) configure artificial-intelligence voice agents that place outbound calls to its customers to confirm, remind, or reschedule appointments, (c) answer inbound calls from its customers with an AI agent that can book appointments directly into the calendar, and (d) send outbound SMS reminders and follow-ups.

This Privacy Policy explains what personal information we collect from users of the Service, the purposes for which we use it, the legal bases on which we rely, the third parties with whom we share it, how we protect it, and the rights you have in relation to it. It applies to the business clients who subscribe to AutomatusLabs ("**Clients**"), to visitors of our website ("**Visitors**"), and to the individual end-customers of our Clients whose personal data we may process on the Client's behalf ("**End-Customers**").

Our role under data protection law

In respect of information about Clients (for example account details and billing information) and Visitors, AutomatusLabs acts as a **data controller**. In respect of information relating to End-Customers that Clients upload, import, or otherwise cause to flow through the Service, AutomatusLabs acts as a **data processor** on behalf of the Client, who remains the data controller. Where we act as a processor, our processing is governed both by this Policy and by the Data Processing Addendum incorporated into our Terms of Service.

Contacting our privacy team

If you have any questions about this Policy or about how we handle your personal information, please contact our privacy team at support@automatuslabs.com. Because AutomatusLabs is established in the United Kingdom, our lead supervisory authority is the UK Information Commissioner's Office (ico.org.uk).

2. Information We Collect

We collect personal information in three ways: (i) information you provide to us directly; (ii) information we receive from third-party services you connect to the Service, such as Google; and (iii) information we collect automatically when you use the Service. The categories below describe each source in detail.

2.1 Account Information

When a Client creates an AutomatusLabs account, either directly or through our WordPress-based registration flow, we collect:

- full name and preferred display name of the account holder and any authorised users;
- business name, trading address, and country of operation;
- email address and optional phone number used for authentication and service notices;
- hashed authentication credentials (we never store passwords in plain text);
- membership tier, subscription status, and billing identifiers maintained by MemberPress;
- profile photo or avatar, if you choose to upload one.

2.2 Google Calendar Data

> **Detailed disclosure — required for Google OAuth verification**
>
> This section describes exactly what Google user data AutomatusLabs accesses, why we access it, how it is stored, and how you can revoke access at any time. Section 4 sets out the separate Limited Use commitment that governs our handling of all Google user data.

When a Client elects to connect a Google account to AutomatusLabs, we use Google's OAuth 2.0 authorisation framework. During this flow, Google presents you with a consent screen that lists the scopes we request. You may review and accept or decline each scope before any data is shared with us.

Scopes requested

We request the following Google OAuth scope to deliver calendar functionality:

Scope	Purpose
https://www.googleapis.com/auth/calendar	Read and write access to the Client's Google Calendar events and free/busy information, used solely to check availability and to create, update, move, or cancel appointment events on behalf of the Client.

Data we receive from Google

Once you consent, AutomatusLabs receives the following data elements from the Google Calendar API, and no others:

- event identifiers, titles, descriptions, start and end times, time-zone information, and attendee email addresses on calendars you have authorised;
- free/busy availability information for the authorised calendars;
- the identifier and summary of each authorised calendar;
- OAuth access tokens and refresh tokens issued by Google to AutomatusLabs; and
- basic profile identifiers (email address and Google account ID) required to associate tokens with your AutomatusLabs account.

Why we access this data

We access Google Calendar data solely to perform the calendar-dependent features of the Service that you have requested. Specifically, AutomatusLabs uses calendar data to (i) determine whether a proposed appointment time is available before an AI voice agent confirms that time with an End-Customer; (ii) create, update, or cancel events in response to inbound and outbound AI calls; (iii) read attendee and location information so that reminder messages contain accurate details; and (iv) detect conflicts between existing events and proposed changes. We do not access Google Calendar data for any other purpose.

How Google data is stored

Google OAuth refresh tokens and any cached calendar payloads are stored server-side in the AutomatusLabs WordPress backend database, which runs on encrypted volumes managed by our infrastructure provider. Refresh tokens are additionally encrypted at rest at the application layer using AES-256 with keys held in a managed secret store; only the services that need the tokens to call the Google Calendar API can decrypt them. Traffic between your browser or desktop application, our backend, and Google is protected by TLS 1.2 or higher. We do not copy your Google Calendar data into any analytics warehouse, marketing system, or machine-learning training corpus.

Revoking access

You can disconnect AutomatusLabs from your Google account at any time. The fastest method is to visit https://myaccount.google.com/permissions, select “AutomatusLabs”, and click “Remove access”. You can also disconnect from within the AutomatusLabs desktop application by opening Settings → Integrations → Google Calendar → Disconnect. Finally, you may email support@automatuslabs.com and request that we revoke your tokens and delete any cached Google Calendar data. Once access is revoked, our stored refresh tokens for your account are invalidated and any cached calendar data is deleted within 30 days.

2.3 Call and SMS Data

When the Service places or receives a voice call on behalf of a Client, or sends or receives an SMS message, we process:

- the End-Customer's phone number and, where supplied by the Client, the End-Customer's name;
- call metadata such as start and end timestamps, duration, call direction, and final disposition (answered, no-answer, voicemail, etc.);
- the audio recording of the call, where the Client has enabled recording and where recording is lawful in the jurisdiction;
- transcripts of the call produced by our speech-to-text pipeline, together with AI-generated summaries;
- the content of SMS messages sent and received, together with their delivery status.

Voice functionality is delivered through our processor VAPI, which in turn uses ElevenLabs for voice synthesis and a selection of speech-recognition and large-language-model providers to generate responses. SMS messages are transmitted through our processor Twilio. See Section 6 for details of each sub-processor.

2.4 Usage Data and Analytics

When you use the Service we automatically collect diagnostic and analytical information, including IP address, browser or Electron-runtime user-agent string, operating-system version, device identifiers, pages or screens viewed, features used, approximate geolocation derived from IP, and crash or error reports. We use this information to operate, secure, and improve the Service. We do not combine usage data with Google user data, call content, or SMS content.

2.5 Payment Information

Subscription billing is handled by MemberPress running on our WordPress backend, with card processing performed by our payment-service providers (currently Stripe and, for selected regions, PayPal). AutomatusLabs itself does not store full payment-card numbers, CVC codes, or bank-account credentials. We retain only the limited billing metadata needed to operate subscriptions, such as the last four digits of the card, the card brand, the billing country, the subscription plan, invoice history, and the payment processor's customer and subscription identifiers.

2.6 Communications with Us

When you contact AutomatusLabs by email or through an in-product support channel we retain a record of the correspondence, including the content of your message and any attachments, so that we can respond to your enquiry and improve our support.

3. How We Use Your Information

We process personal information only for the purposes set out below and only where we have a lawful basis to do so under the UK GDPR and EU GDPR. The following table summarises each purpose and the legal basis we rely on.

Purpose	Legal basis (UK/EU GDPR)
Providing the Service, including account provisioning, authentication, and subscription management.	Performance of a contract (Art. 6(1)(b))
Connecting Google, Microsoft, or Apple accounts and calling third-party APIs on your instruction.	Performance of a contract; consent where required (Art. 6(1)(a) and (b))
Placing or receiving AI voice calls and sending SMS messages on behalf of a Client.	Performance of a contract between the Client and AutomatusLabs; Client's documented instructions as processor
Billing, invoicing, fraud prevention, and tax compliance.	Performance of a contract and legal obligation (Art. 6(1)(b) and (c))
Securing the Service, detecting abuse, and responding to incidents.	Legitimate interests in keeping the Service safe (Art. 6(1)(f))
Analytics and product improvement using aggregated or de-identified data.	Legitimate interests in improving the Service (Art. 6(1)(f))
Sending service emails, product updates, and, where permitted, marketing communications.	Legitimate interests and, where required, consent (Art. 6(1)(a) and (f))
Complying with legal and regulatory obligations and responding to lawful requests.	Legal obligation (Art. 6(1)(c))

Things we never do

AutomatusLabs does not:

- sell personal information to third parties (as "sell" is defined under the CCPA or any other law);
- share personal information with third parties for their own advertising or direct-marketing purposes;
- use Google user data, End-Customer data, call content, SMS content, or any other personal information to train, fine-tune, or otherwise develop generalised artificial-intelligence or machine-learning models;
- allow human beings at AutomatusLabs to read Google user data, call content, or SMS content except where strictly necessary to provide or secure the Service, to comply with the law, or where you have given us specific consent to do so.

4. Google API Services — Limited Use Disclosure

Limited Use commitment

AutomatusLabs' use of information received from Google APIs will adhere to the Google API Services User Data Policy, including the Limited Use requirements.

In practical terms, the Limited Use commitment means the following specific things about Google user data obtained from Google Workspace APIs (including the Google Calendar API and any Google OAuth identity claims):

4.1 Allowed uses only

AutomatusLabs uses Google user data solely to provide and improve the user-facing features of the Service that are visible and prominent in our product — specifically, the calendar synchronisation, appointment booking, availability checking, and event-management features described in Section 2.2. Google user data is not used for any other purpose.

4.2 No transfer to others

AutomatusLabs does not transfer Google user data to third parties except (a) as necessary to provide or improve the user-facing features that are prominent in the Service, (b) to comply with applicable law, or (c) as part of a merger, acquisition, or sale of assets with the user's explicit consent. In particular, we do not transfer Google user data to data brokers, advertising networks, or information resellers.

4.3 No human reading

AutomatusLabs does not allow humans to read Google user data unless (i) we have obtained the user's affirmative agreement to view specific messages or events, (ii) it is necessary for security purposes such as investigating abuse, (iii) it is necessary to comply with applicable law, or (iv) the data (including derivations) has been aggregated and anonymised for internal operations. Engineers with access to production systems operate under strict contractual confidentiality obligations and their access is logged.

4.4 No advertising use

Google user data is never used to serve advertisements, whether contextual, behavioural, retargeted, or otherwise, and is never shared with advertising intermediaries.

4.5 No use in AI or ML model training

AutomatusLabs does not use Google user data — whether in raw, transformed, or derived form — to develop, improve, or train generalised artificial-intelligence or machine-learning models. Where AutomatusLabs uses third-party AI services (for example large-language-model providers consumed through VAPI) to generate real-time responses during a call or chat session, those services are contractually prohibited from retaining or training on the Google user data that is passed to them.

4.6 Incident response

If AutomatusLabs becomes aware of any unauthorised access to or misuse of Google user data, we will notify affected users and Google promptly in accordance with the Google API Services User Data Policy and applicable law, and we will cooperate fully with any resulting investigation.

5. Microsoft and Apple Authentication Services

5.1 Microsoft Outlook and Microsoft 365 (upcoming)

We are developing an integration with Microsoft 365 and Outlook Calendar that will allow Clients to synchronise Outlook calendars using Microsoft's OAuth 2.0 authorisation framework. When this integration is released, it will request only the minimum Microsoft Graph scopes needed to read availability and create, update, or cancel calendar events (anticipated scopes include Calendars.ReadWrite and offline_access). Data received from Microsoft Graph will be handled in the same manner as Google Calendar data described in Sections 2.2 and 4 of this Policy: stored encrypted at rest, transmitted over TLS, not used for advertising, not used to train AI models, and retained only for as long as the integration is connected or as needed to comply with the law. This Policy will be updated and a notice will be issued to existing Clients before the Microsoft integration is enabled.

5.2 Sign in with Apple

Clients may choose to register or sign in to the Service using "Sign in with Apple". When you use this option, Apple shares with us only the limited identity information you authorise — typically your name and an email address (which may be a private-relay address generated by Apple). We use this information solely to create and authenticate your AutomatusLabs account. If you use Apple's private-relay feature, we treat the relay address as your primary contact email and will honour relay deliverability requirements. You can disconnect "Sign in with Apple" from your AutomatusLabs account under Settings → Security, and you can revoke it at any time via your Apple ID settings at appleid.apple.com.

6. Third-Party Service Providers

To deliver the Service, AutomatusLabs relies on a small number of carefully selected sub-processors, each bound by written data-protection obligations equivalent to those we owe our Clients. The table below lists the principal sub-processors, the data they process, and their function.

Provider	Function	Data processed
VAPI	AI voice-calling infrastructure that orchestrates outbound and inbound calls for the Service.	End-Customer phone numbers, call audio, call transcripts, AI prompt metadata.
Twilio	SMS and telephony carrier used to send and receive text messages and to route voice traffic.	End-Customer phone numbers, SMS message content, delivery metadata.
ElevenLabs	AI voice-synthesis provider used by VAPI to generate lifelike speech on calls.	Generated speech payloads; no raw End-Customer identifiers beyond what is strictly required for a call.
MemberPress	WordPress membership and subscription management plugin used to control Client access tiers.	Client account identifiers, subscription status, invoice metadata.

Provider	Function	Data processed
Google LLC	Google Calendar API and Google OAuth identity provider.	Events, free/busy information, tokens, profile identifiers (see Sections 2.2 and 4).
Microsoft Corp.	Microsoft Graph and Microsoft OAuth identity provider (upcoming).	Events, free/busy information, tokens, profile identifiers (planned).
Apple Inc.	Sign in with Apple authentication provider.	Name, email or private-relay email, Apple user identifier.
Stripe / PayPal	Payment-card processors that handle card authorisation and settlement.	Billing metadata and payment tokens (AutomatusLabs does not handle card numbers).
Hosting and infrastructure providers	Cloud hosting, managed database, CDN, and email delivery for the Service.	Any personal data processed through the Service, encrypted at rest.

An up-to-date list of sub-processors is available on request by emailing support@automatuslabs.com. Where any sub-processor is located outside the United Kingdom or the European Economic Area, we rely on the UK International Data Transfer Agreement, the UK Addendum to the EU Standard Contractual Clauses, or an adequacy decision to safeguard the transfer.

7. Data Storage and Security

AutomatusLabs maintains a written information-security programme that is proportionate to the volume, sensitivity, and nature of the personal data we process. Our controls include, without limitation:

- **Encryption in transit** — all connections between the desktop application, our WordPress backend, and third-party APIs (Google, Microsoft, VAPI, Twilio, ElevenLabs, Stripe) are protected using TLS 1.2 or higher;
- **Encryption at rest** — production databases, object storage, and backups are encrypted using AES-256;
- **Application-layer encryption** — Google and Microsoft OAuth refresh tokens and similar high-sensitivity secrets are separately encrypted before being written to the database, with keys held in a managed secret store;
- **Access controls** — role-based access, multi-factor authentication for all administrative accounts, and the principle of least privilege for all production systems;
- **Segregation** — Client tenants are logically separated so that one Client cannot access another Client's data;
- **Network security** — firewalled production networks, vulnerability scanning, managed patching, and continuous monitoring;
- **Personnel** — background-checked staff, written confidentiality obligations, and role-appropriate security training;
- **Incident response** — documented procedures for detecting, investigating, notifying, and remediating personal-data breaches, aligned with the 72-hour notification obligation under Article 33 UK GDPR.

No security programme is perfect, but we regularly review and improve our controls. If you believe you have discovered a security vulnerability in the Service, please report it responsibly to support@automatuslabs.com.

8. Data Retention

We retain personal information only for as long as is necessary to fulfil the purposes for which we collected it, including to satisfy any legal, accounting, or reporting requirements. Our standard retention periods are set out below. Retention periods may be extended where necessary to comply with the law, to enforce our agreements, or to resolve disputes.

Category	Retention period
Active account and subscription data	For the lifetime of the account, plus 6 months after closure.
Google / Microsoft OAuth tokens and cached calendar data	Until the integration is disconnected; cached data deleted within 30 days of revocation.
Call audio recordings (where enabled)	90 days by default; configurable by the Client down to 7 days or up to the maximum period permitted by applicable law.
Call transcripts and AI-generated summaries	Up to 12 months, unless the Client configures a shorter period.

Category	Retention period
SMS message content and metadata	Up to 12 months, subject to carrier and legal requirements.
Billing and tax records	7 years, in line with UK HMRC requirements.
Website and in-product analytics logs	Up to 14 months, typically in aggregated form.
Support correspondence	Up to 3 years after the matter is closed.
Security and audit logs	Up to 2 years.

On request, and at any time, a Client can ask AutomatusLabs to delete specific records before the periods above expire, subject to our legal retention obligations.

9. Your Rights (UK/EU GDPR and CCPA)

9.1 UK and EU residents

If you are located in the United Kingdom or the European Economic Area, you have the following rights in relation to the personal data we hold about you:

- **Right of access** — to be told whether we are processing your personal data and, if so, to receive a copy of it;
- **Right to rectification** — to have inaccurate or incomplete personal data corrected;
- **Right to erasure** — to have your personal data deleted in certain circumstances (often called the "right to be forgotten");
- **Right to restrict processing** — to ask us to pause processing your personal data while a dispute is resolved;
- **Right to data portability** — to receive your personal data in a structured, commonly used, machine-readable format;
- **Right to object** — to object to processing based on legitimate interests and to object to direct marketing at any time;
- **Rights in relation to automated decision-making** — not to be subject to solely automated decisions that produce legal or similarly significant effects, except where permitted by law;
- **Right to withdraw consent** — where we rely on your consent, to withdraw it at any time without affecting the lawfulness of processing carried out before withdrawal;
- **Right to lodge a complaint** — with the UK Information Commissioner's Office or with the supervisory authority of your EU member state of residence.

To exercise any of these rights, email support@automatuslabs.com. We will respond without undue delay and in any event within one month of receipt, unless the request is complex, in which case we may extend the period by a further two months and will let you know.

9.2 California residents (CCPA/CPRA)

If you are a California resident, the California Consumer Privacy Act as amended by the California Privacy Rights Act gives you the following rights in relation to your personal information:

- the right to **know** what personal information we collect, the sources from which it is collected, the purposes of collection, and the categories of third parties with whom it is shared;
- the right to **access** the specific pieces of personal information we hold about you;
- the right to **delete** personal information we have collected from you, subject to certain exceptions;
- the right to **correct** inaccurate personal information;
- the right to **limit the use or disclosure of sensitive personal information**;
- the right to **opt out of the "sale" or "sharing"** of personal information — AutomatusLabs does not sell or share personal information as those terms are defined under the CCPA, so no opt-out is necessary, but you may still submit a request and we will confirm this in writing;
- the right to **non-discrimination** for exercising any of these rights.

You may submit a CCPA request by emailing support@automatuslabs.com with the subject line "CCPA Request". We will verify your identity using the contact information associated with your account and will respond within 45 days, extendable by a further 45 days where reasonably necessary. You may use an authorised agent to make a request on your behalf, provided the agent

furnishes proof of authority.

9.3 Requests concerning End-Customer data

Where AutomatusLabs acts as a data processor on behalf of a Client (for example, when an End-Customer asks us about a call or SMS they received from our Client), we will forward the request to the relevant Client, who is the data controller and the appropriate party to respond. We will support Clients in responding to such requests as required by the UK GDPR, the EU GDPR, and our Data Processing Addendum.

10. Cookies and Similar Technologies

The AutomatusLabs website and the authenticated web-portal components of the Service use a small number of cookies and similar technologies. We use:

- **Strictly necessary cookies** — needed for authentication, session management, and security. These cannot be disabled without breaking the Service.
- **Preference cookies** — remember your language, theme, and UI choices.
- **Analytics cookies** — used in aggregated form to understand how the Service is used. These are set only where you have given consent under the Privacy and Electronic Communications Regulations (PECR) or equivalent law.

You can control cookies through your browser settings and through the cookie banner presented on first visit. The desktop Electron application does not itself set third-party advertising cookies.

11. Children's Privacy

The Service is designed for use by businesses and is not directed to children under the age of 16. We do not knowingly collect personal information from children under 16. If you believe that a child has provided us with personal information in connection with the Service, please contact us at support@automatuslabs.com and we will take steps to delete it.

12. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in our services, in applicable law, or in the sub-processors and third-party integrations that we use. When we make a material change, we will notify active Clients at least 30 days before the change takes effect, either by email or through a prominent notice in the Service. The date at the top of this Policy shows when it was last revised. We encourage you to review this Policy periodically to stay informed.

13. Contact Us

If you have any questions, comments, or requests regarding this Privacy Policy or AutomatusLabs' privacy practices, please contact us using the details below.

Company	AutomatusLabs Ltd
Address	London, United Kingdom
Email (all privacy matters)	support@automatuslabs.com
Website	https://automatuslabs.com
UK supervisory authority	Information Commissioner's Office — ico.org.uk

© 2026 AutomatusLabs Ltd. All rights reserved. AutomatusLabs is a trade mark of AutomatusLabs Ltd. Google, Google Calendar, and the Google Workspace marks are trademarks of Google LLC. Microsoft, Outlook, and Microsoft 365 are trademarks of Microsoft Corporation. Apple and "Sign in with Apple" are trademarks of Apple Inc. All other marks belong to their respective owners.