Privacy Policy

Last updated: May 22, 2025

Your privacy matters to Stellar Technology B.V. We comply with all relevant privacy laws and regulations, including the General Data Protection Regulation (GDPR). This means we:

- **Clearly define our purposes** before processing your personal data, as outlined in this privacy policy
- **Collect only necessary data** and limit it to what we need for our stated purposes
- **Request explicit consent** when required for processing your personal data
- **Implement appropriate security measures** to protect your data, and require the same from parties that process data on our behalf
- **Respect your rights**, including your right to access, correct, or delete personal data we hold about you

Your data is safe with us. This privacy policy explains what Stellar Technology B.V. does with the information we collect and how we handle it.

If you have questions or want to know what data we hold about you, please contact us at the details provided at the end of this document.

How We Use Personal Data

Stellar operates in two distinct roles, and it's important to understand the difference:

When we are a Data Controller: We determine what data to collect and why (for example, when you create an account on our platform or contact us).

When we are a Data Processor: Our clients determine what data to collect and why. We process it on their behalf according to their instructions (for example, when our AI voice agents handle calls for their customers).

The sections below explain each role in detail.

1. When We Are Data Controller

1.1 Platform Access

When you use our platform, you must create an account. You'll provide information about yourself and may set login credentials. This creates an account that you can access anytime.

What data we collect:

- Name, address, and company details
- Email address
- Usage logs (what you've done and when, for audit purposes)

Why we need it: This is necessary to fulfill our contract with you. We keep this information so you don't have to re-enter it each time, and so we can reach you when needed.

How long we keep it: Until three months after you close your account.

Your control: You can update this information anytime through your account settings, or by contacting us directly.

1.2 Business Communications

When you contact us through our website or by email, we collect the information you provide to respond to your inquiry.

What data we collect:

- Name, address, and company details
- Phone number
- Email address
- The content of your message

Why we need it: We have a legitimate interest in responding to your questions and providing customer service. We also use this information to improve our service quality.

How long we keep it: Until we're confident you're satisfied with our response, plus three months. This allows us to reference previous conversations if you have follow-up questions.

1.3 Website Analytics

We use privacy-friendly and GDPR-compliant analytics tools, such as Umami, to understand how visitors use our website. Umami does not track individuals or use cookies for tracking purposes. It collects only aggregated, anonymous data about page views and navigation patterns.

2. When We Are Data Processor

This section is the heart of what Stellar does: processing voice calls, chats, e-mails and other customer interactions on behalf of our business clients.

2.1 Our Role

When our AI voice agents answer calls for our clients, **they are the data controllers** and **we are the data processor**. This means:

- Our clients determine what data to collect and for what purposes
- We process data according to their instructions
- Our clients are responsible for ensuring lawful processing
- Our relationship is governed by separate Data Processing Agreements (DPAs)

Important for end-customers: If you're calling one of our clients and speaking with an AI voice agent powered by Stellar, your privacy rights must be exercised directly with that company. They control your data; we only process it on their behalf.

2.2 What Data We Process

When handling customer support for our clients, we process:

- **Voice recordings** of customer calls
- **Real-time transcripts** of conversations
- **Chat transcripts** of conversations
- **E-mails**
- **AI-generated summaries** of call, chat, and e-mail outcomes
- **Customer identification data** provided by client systems (such as customer names, account numbers, or other identifiers)

- **Interaction metadata** (duration, timestamp, phone numbers)

2.3 Data Storage and Retention

We offer flexible data storage options based on client needs:

Default retention: Call recordings, transcripts, and summaries are stored on our platform for **30 days**, then automatically and permanently deleted.

Client CRM storage: When agreed, we store data directly in the client's CRM system and immediately delete it from our platform. This is our "zero data retention" option.

Custom agreements: For proof-of-concept projects, pilots, or specific client requirements, we may agree to different retention periods. These are always documented in writing.

After the retention period: All data is automatically and irreversibly deleted from our systems.

2.4 When We Access Call Data

We maintain strict limits on when our team can access call recordings or transcripts. Access only occurs when:

- **Troubleshooting is needed** to resolve technical issues
- **Quality improvement** requires reviewing conversation flows
- **The client explicitly requests** that we review specific calls
- **Legal obligation** requires us to access the data

All access is logged and monitored.

2.5 Client Responsibilities

Because our clients are the data controllers, they have important responsibilities:

- **Informing end-customers** that they're interacting with an AI agent
- **Obtaining necessary consent** for recording calls, in compliance with local laws
- **Ensuring lawful processing** of their customers' personal data
- **Determining purposes and means** of data processing
- **Providing accurate configuration** for the AI agents
- **Implementing escalation procedures** for sensitive or complex matters

2.6 How We Protect Your Data

We never use call data for model training: Your conversations are never used to train AI models for other clients.

No commercial use beyond agreed services: We use client data solely for delivering the contracted services.

No sharing with third parties: Except for subprocessors (see below) necessary to deliver our services, we never share client data with anyone.

Purpose limitation: Data is used only for the purposes agreed with each client in their contract.

3. Subprocessors and Infrastructure

3.1 Where Your Data Lives

All personal data is stored in the European Union:

- **Primary infrastructure:** Google Cloud Platform, EU-West4 region (Netherlands)
- **No data transfers outside the EU** for storage or primary processing

3.2 Our Subprocessors

To deliver our services, we work with carefully selected subprocessors. All have Data Processing Agreements in place. Key subprocessors that may process personal data include:

Infrastructure:

- **Google Cloud Platform** – Cloud hosting (EU-West4, Netherlands)
- **Cloudflare** – Web application firewall
- **Clerk** – Authentication platform

AI Services:

- **OpenAI Ireland Ltd** – AI models with zero data retention policy and EU data processing
- **Google** – AI models, handles Personal Data only with zero data retention and EU data processing
- **Anthropic** – AI models, handles Personal Data only with zero data retention and EU data processing

Communication:

- **Twilio** – Phone connectivity infrastructure

Complete list: A full, up-to-date list of all subprocessors is available at trust.stellarcs.ai.

Notice of changes: We notify clients 30 days before adding new subprocessors. Clients have the right to object if they have legitimate concerns.

3.3 International Data Transfers

While our infrastructure is in the EU, some subprocessors may have operations outside the EU. When this occurs, we ensure appropriate safeguards are in place, including:

- Standard Contractual Clauses (SCCs) approved by the European Commission
- Data Processing Agreements with strong security commitments
- Regular assessments of transfer impact and security measures

4. Security Measures

Security is fundamental to everything we do.

4.1 ISO 27001 Certification

We are in the process of obtaining ISO 27001 certification, expected by in Q4 2025. This internationally recognized standard demonstrates our commitment to information security management.

4.2 Technical and Organizational Measures

Our security program includes:

- **Encryption:** Data encrypted in transit and at rest
- **Access controls:** Role-based access with multi-factor authentication
- **Network security:** Firewalls, intrusion detection, and monitoring
- **Audit logging:** Comprehensive logs of system access and data processing

- **Incident response:** Documented procedures for security incidents
- **Regular testing:** Penetration testing and vulnerability assessments
- **Vendor management:** Security reviews of all subprocessors
- **Employee training:** Regular security awareness training for all staff

4.3 Detailed Security Documentation

For comprehensive information about our security practices, including our security policies and compliance documentation, visit trust.stellarcs.ai.

5. Your Privacy Rights

You have the following rights regarding your personal data:

- **Right to access:** Request information about what personal data we hold about you
- **Right to rectification:** Request correction of inaccurate data
- **Right to erasure:** Request deletion of your data ("right to be forgotten")
- **Right to data portability:** Receive your data in a structured, machine-readable format
- **Right to object:** Object to certain types of processing
- **Right to restrict processing:** Request that we limit how we use your data
- **Right to withdraw consent:** Where processing is based on consent, you can withdraw it at any time

Important note for end-customers: If you're a customer of one of our business clients (i.e., you called a company that uses Stellar's AI voice agents), you must exercise these rights directly with that company, not with Stellar. They are the data controller; we only process data on their behalf.

5.1 How to Exercise Your Rights

To exercise any of these rights, contact our Data Protection Officer (see contact details below). Please clearly identify yourself to ensure we can act on the right person's data.

We will respond to your request within one month. This period may be extended due to the complexity of the request or the specific rights involved. If we need more time, we'll let you know promptly.

6. Data Protection Officer

We have appointed a Data Protection Officer who is responsible for privacy within our organization:

Dennis de Reus

Email: dpo@stellarcs.ai

Phone: +31 6 24 54 55 54

Our DPO is available for all your questions, requests, and concerns about privacy and data protection.

7. Third-Party Disclosure

We do not sell, trade, or share your personal data with third parties, except:

- **Subprocessors** necessary to deliver our services (as listed in Section 3)
- **Legal obligations** when required by law or court order (e.g., law enforcement requests with proper legal basis)
- **Client instructions** when we're acting as a data processor and the client (as controller) directs us to share data

8. Changes to This Privacy Policy

As our business evolves, we may need to update this privacy policy. When we make changes:

- We update the "Last updated" date at the top of this document
- For material changes affecting how we use personal data, we'll notify affected parties
- We recommend checking this page periodically for updates

Previous versions of this policy are available upon request.

9. Questions and Complaints

9.1 Contact Us

If you have questions about this privacy policy or how we handle your data:

Stellar Technology B.V.

Fort Diemerdamstraat 3

1384 AH Weesp

The Netherlands

Email: dpo@stellarcs.ai

Phone: +31 6 24 54 55 54

Chamber of Commerce (KvK): 97274542

9.2 Filing a Complaint

If you're unhappy with how we've handled your personal data:

1. Contact us first: Email dpo@stellarcs.ai. We take every complaint seriously and will work to resolve it promptly.

2. Supervisory authority: If you're not satisfied with our response, you have the right to file a complaint with the Dutch Data Protection Authority (Autoriteit Persoonsgegevens):

Autoriteit Persoonsgegevens

P.O. Box 93374

2509 AJ The Hague

The Netherlands

Website: autoriteitpersoonsgegevens.nl