

PRIVACY POLICY — VERSION 1.0 · 15.09.2026**1. Controller**

Simone Venneri, Föhrenweg 20, 5606 Dintikon, Switzerland, acting as an individual under the business name “Sympel Monitoring”. Privacy contact: info@sympel.ch.

2. Scope

This Privacy Policy describes processing for which Sympel determines its own purposes, in particular website/account operation, contract administration, billing, security, support and communications. Processing of monitoring data on behalf of a Customer is additionally governed by the DPA.

3. Data We Process

Depending on use, we process account/contact data, organisation/contract data, login/security metadata, support communications, billing/Stripe references, audit data and technical usage data. The service may additionally process PBX, Agent, network, location, trunk, provider and incident data.

4. Purposes

Providing and securing the service, account and contract administration, billing, support, notifications, abuse prevention, troubleshooting, compliance with legal obligations and, for instructed operational data, monitoring and operational intelligence according to Customer configuration.

5. Recipients

Data is disclosed only to authorised internal personnel and required service providers/subprocessors. The current Subprocessor List identifies providers used for the service.

6. International Transfers

Depending on the provider, data may be processed outside Switzerland or the EEA. Sympel assesses applicable transfer requirements and, where required, uses recognised safeguards such as Standard Contractual Clauses with Swiss adaptations or other permitted transfer mechanisms.

7. Retention

Data is retained only for as long as required for the relevant purposes, contractual obligations, security, dispute handling or legal retention. Terminated organisations are generally subject to a 30-day offboarding and recovery period. After that period, customer operational and monitoring data is released for deletion through the controlled deletion process unless legal, contractual or security-related retention requirements apply. Contractual, billing, audit and evidentiary records may be retained separately for longer where required. Data may remain in protected backups until the applicable backup lifecycle expires and is not further processed there for normal customer operations.

8. Security

Sympel uses risk-appropriate technical and organisational measures including tenant isolation, server-side authorisation, encryption of selected secrets, hashing of credentials/tokens, TLS, audit logging and security controls for web and Agent access.

9. Data Subject Rights

Data subjects may exercise rights available under applicable data-protection law. Where data is processed solely on behalf of a Customer, Sympel may refer requests to the relevant Customer/controller and assist that Customer in responding.

10. Legal Bases and Roles Depending on the processing, the Provider relies on performance of a contract or pre-contractual measures, legal obligations and legitimate interests, in particular in secure and reliable operation, support and abuse prevention; consent is used where required for a specific processing activity. For monitoring data, the Provider acts, depending on the circumstances, as processor/subprocessor under the DPA; the Customer remains responsible for its controller/processor obligations.

11. Specially Sensitive Data The standard service is not intended for intentional submission of call content/recordings, health/biometric data, data concerning criminal proceedings/sanctions or other specially sensitive/special-category data unless separately agreed in writing.

12. Cookies and Analytics Technically necessary session/security mechanisms may be used for login and secure operation. If non-essential analytics/marketing technologies are introduced in the future, transparency and any required consent mechanisms will be implemented before activation.

13. Supervisory Authority and Rights Data subjects may exercise rights under applicable data-protection law via info@sympel.ch. The competent Swiss supervisory authority is the Federal Data Protection and Information Commissioner (FDPIC), where it has jurisdiction. Any obligation to appoint an EU representative will be assessed according to the actual territorial scope of the GDPR and, if required, implemented before corresponding market activity.

14. Changes

This Privacy Policy may be updated when the service, law or processing materially changes. The current version will be published with a version/date identifier.