Data Processing Agreement (DPA)

Version 2026-10-10

Version of 3 October 2026. Before Sityro launches, the text will be reviewed by a lawyer. If anything substantial changes, you confirm the new version at your next sign-in.

1. Parties

Processor: Silicon Planet GmbH, Pestalozzistr. 25, 22305 Hamburg, Germany, commercial register Hamburg HRB 56004, VAT ID DE164312327. Silicon Planet operates Sityro. Contact for data protection: help@sityro.com.

Controller: the customer who uses Sityro for their websites – the organization in Sityro Central, represented by its admins.

This agreement sets out the obligations under Art. 28 GDPR. It supplements Sityro's terms and conditions and applies from its confirmation in Sityro (when connecting a website, when registering, or at sign-in after a new version). Where it conflicts with the terms on data protection, this agreement prevails.

2. Subject, nature and purpose, duration

Silicon Planet processes personal data on the customer's behalf to monitor the customer's websites (availability, certificates), check them for vulnerabilities and malware, protect them against attacks (Sityro Protect), repair them after an attack and – on paid plans – back them up and restore them. There are no other purposes; the data is not used for Silicon Planet's own purposes, not sold and not used for advertising.

The agreement runs as long as the customer uses Sityro and ends when the organization is deleted. The deletion duties (section 13) continue beyond that.

3. Types of data and data subjects

All plans: metadata of the website's administrators (user names, roles, email addresses of admin accounts), technical metadata of the website (versions of WordPress, plugins and themes, checksums, paths, sizes and modification times of files, results of the checks from outside). With Sityro Protect: hourly counts of blocked requests with aggregated, pseudonymised details (kind of attack, IP addresses); Sityro does not store individual requests.

Checks and repair: single program files that Sityro has identified as changed, foreign or suspicious are read on demand to assess them and compare them with the original; they are not stored permanently. Before a repair, Sityro creates a safety point once on request (also on the Free plan, 7 days, for restoring only); it contains files and database.

Paid plans with backup: the complete files and the database of the website, and with them personal data of its visitors, customers and users – e.g. orders, customer accounts, form entries, comments. Data subjects are the visitors, customers, users and employees of the customer whose data is on the website.

Notifications (email, push in the Sityro app if wanted) contain the name of the website and the reason; recipients are the people the customer enters for them.

4. Place of processing

The data is processed and stored in Germany, in data centres of Hetzner Online GmbH. The exception is the AI-assisted assessment of single program files (section 5) by a sub-processor in the USA. Any further transfer to countries outside the EU takes place only if the conditions of Art. 44 ff. GDPR are met and the customer has been informed in advance (section 9).

5. AI-assisted assessment of program files

On paid plans, Sityro has single program files (PHP, JavaScript) that were identified as suspicious assessed by an AI model: is this malware, and what does it do? Only the file content, its path and its origin are sent – never the database, website content, orders or form data. Program files usually contain no personal data; it cannot be ruled out (e.g. an email address written into the code).

The provider is Anthropic, PBC (USA). The transfer is based on the EU standard contractual clauses (Art. 46(2)(c) GDPR). Under its commercial terms, Anthropic does not use data sent through the API to train its models and keeps it only for a limited time to detect abuse.

Each file is assessed once; Sityro stores the verdict (malicious, suspicious, harmless) with its reasoning, not the file. The verdict alone never changes anything on the website. The customer can switch the AI assessment off at any time in the settings of the organization; the other checks remain.

6. Instructions

Silicon Planet processes the data only on the customer's documented instructions. Instructions are the settings and orders the customer gives in Sityro (e.g. a restore, a repair, the retention of backups, deleting a website or the organization) and requests in text form to help@sityro.com.

If Silicon Planet considers an instruction unlawful, it informs the customer without undue delay and may suspend it until the customer confirms or changes it. Processing without an instruction only takes place where EU or German law requires it; Silicon Planet then informs the customer beforehand, where the law allows.

7. Confidentiality

Everyone at Silicon Planet with access to the data is bound to confidentiality. Access is limited to the people who need it to run, maintain and support Sityro.

8. Security of processing (Art. 32 GDPR)

Transfer: always encrypted (TLS). The plugin signs every request; orders from Sityro to the website (repair, restore, protection rules) are cryptographically signed, have a fixed list of actions and never contain program code.

Storage: backups are stored encrypted (AES-256-GCM, a key of its own per organization). Silicon Planet manages the keys because a restore must be possible without the customer; the encryption protects against third-party access to the storage, not against Silicon Planet itself.

Access: sign-in to Sityro Central only with a password, two-factor sign-in available; critical actions require a fresh confirmation; strict separation of organizations; access and security-relevant actions are logged.

Availability and resilience: operation in data centres in Germany with DDoS protection, regular backups of Sityro's own database, separate test and production environments, continuous updates of the software used.

Changes to the website: before every repair and every restore Sityro creates a safety point in its own storage; files a repair replaces or removes are also kept in a quarantine on the website for 30 days and can be put back.

Silicon Planet adapts these measures to the state of the art without falling below the agreed level of protection.

9. Sub-processors

The customer approves the use of the following sub-processors:

Hosting of the application, database and object storage for backups: Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany – data centres in Germany.

Email delivery: Mailjet (Mailjet SAS, Sinch group), France – recipient addresses and content of notifications.

AI assessment of program files: Anthropic, PBC, USA – see section 5.

Error tracking of Sityro Central: Sentry (Functional Software, Inc., USA), data region EU (Frankfurt am Main) – technical error reports of the application. They may contain identifiers and addresses of organizations and websites; contents of files and backups, IP addresses of visitors, passwords and credentials are not transmitted.

Push notifications in the Sityro app (only when the app is used and push is switched on): Apple Inc. (Apple Push Notification service) or Google LLC (Firebase Cloud Messaging) – device identifier and, depending on the setting, the name of the website and the reason.

Silicon Planet informs the customer at least four weeks before engaging a new sub-processor or replacing one; the new version of this agreement is confirmed at the next sign-in. The customer may object for an important data protection reason; if no agreement can be reached, the customer may terminate the contract as of the change. Silicon Planet binds every sub-processor contractually to the same data protection obligations.

Billing is not processing on the customer's behalf: payments through Stripe (Stripe Payments Europe, Ltd., Ireland) concern the customer's own contract and payment data, not data of their websites. They are described in the privacy policy.

10. Rights of data subjects

Silicon Planet supports the customer with appropriate technical and organisational measures in answering requests from data subjects (access, rectification, erasure, restriction, portability, objection). If a data subject contacts Silicon Planet directly, Silicon Planet forwards the request to the customer without undue delay and does not answer it itself. The customer can download backups as a ZIP archive at any time.

11. Support with further obligations

Silicon Planet supports the customer in meeting the obligations of Art. 32 to 36 GDPR (security, notification of breaches, data protection impact assessment, prior consultation) and provides the information needed for this.

12. Personal data breaches

Silicon Planet notifies the customer of a personal data breach affecting the customer's data without undue delay, where possible within 24 hours of becoming aware of it, at the email addresses of the organization's admins. As far as known, the notification describes the nature and extent of the breach, the data concerned, the likely consequences and the measures taken. Silicon Planet takes measures without undue delay to remedy the breach and mitigate its effects.

13. Deletion and return

Backups are deleted continuously once the retention set by the customer has passed, and completely four weeks after the paid plan ends, including every Known Good. Until then the customer can download them. Safety points before a repair are deleted after seven days.

When the customer deletes a website, its data at Sityro is deleted, including its backups. When the customer deletes the organization, Silicon Planet deletes all data processed on the customer's behalf; user accounts remain as long as they belong to other organizations.

Statutory retention obligations remain unaffected.

14. Evidence and audits

On request, Silicon Planet provides the customer with all information needed to demonstrate compliance with this agreement and allows audits by the customer or an auditor appointed by the customer and bound to confidentiality. On-site audits are arranged with reasonable notice and take place during business hours; suitable certifications of the sub-processors (e.g. ISO 27001 of the data centres) can replace an on-site audit.

15. Final provisions

German law applies. Changes to this agreement are provided as a new version and confirmed at the next sign-in. If a provision is invalid, the rest of the agreement remains valid; the statutory provision takes its place.