Auftragsverarbeitungsvertrag (AVV)

Fassung 2026-10-10

Fassung vom 3. Oktober 2026. Vor dem Start von Sityro wird der Text noch juristisch geprüft. Ändert sich dabei etwas Wesentliches, bestätigen Sie die neue Fassung beim nächsten Login.

1. Vertragsparteien

Auftragsverarbeiter: Silicon Planet GmbH, Pestalozzistr. 25, 22305 Hamburg, Deutschland, Handelsregister Hamburg HRB 56004, USt-ID DE164312327. Silicon Planet betreibt Sityro. Kontakt in Datenschutzfragen: help@sityro.com.

Verantwortlicher (Auftraggeber): der Kunde, der Sityro für seine Websites nutzt – die Organisation in Sityro Central, vertreten durch ihre Admins.

Dieser Vertrag konkretisiert die Pflichten nach Art. 28 DSGVO. Er ergänzt die Allgemeinen Geschäftsbedingungen von Sityro und gilt ab der Bestätigung in Sityro (beim Verbinden einer Website, bei der Registrierung oder beim Login nach einer neuen Fassung). Bei Widersprüchen in Fragen des Datenschutzes geht dieser Vertrag den AGB vor.

2. Gegenstand, Art und Zweck, Dauer

Silicon Planet verarbeitet personenbezogene Daten im Auftrag des Kunden, um dessen Websites zu überwachen (Erreichbarkeit, Zertifikate), auf Schwachstellen und Schadcode zu prüfen, vor Angriffen zu schützen (Sityro Protect), nach einem Angriff zu reparieren und – in bezahlten Tarifen – zu sichern und wiederherzustellen. Weitere Zwecke gibt es nicht; die Daten werden nicht für eigene Zwecke von Silicon Planet genutzt, nicht verkauft und nicht für Werbung verwendet.

Der Vertrag läuft, solange der Kunde Sityro nutzt, und endet mit der Löschung der Organisation. Die Pflichten zur Löschung (Abschnitt 13) gelten darüber hinaus.

3. Art der Daten und betroffene Personen

Alle Tarife: Metadaten der Administratoren der Website (Benutzernamen, Rollen, E-Mail-Adressen der Admin-Konten), technische Metadaten der Website (Versionen von WordPress, Plugins und Themes, Prüfsummen, Pfade, Größen und Änderungszeiten von Dateien, Ergebnisse der Prüfungen von außen). Mit Sityro Protect: je Stunde gezählte, aggregierte und pseudonymisierte Angaben zu abgewehrten Anfragen (Art des Angriffs, IP-Adressen); einzelne Anfragen speichert Sityro nicht.

Prüfung und Reparatur: Einzelne Programmdateien, die Sityro als verändert, fremd oder verdächtig erkannt hat, liest Sityro auf Abruf, um sie zu beurteilen und mit dem Original zu vergleichen; sie werden nicht dauerhaft gespeichert. Vor einer Reparatur legt Sityro auf Wunsch einmalig einen Sicherungspunkt an (auch im Tarif Free, 7 Tage, nur zum Zurückspielen); er enthält Dateien und Datenbank.

Bezahlte Tarife mit Backup: die vollständigen Dateien und die Datenbank der Website und damit personenbezogene Daten ihrer Besucher, Kunden und Nutzer – z. B. Bestellungen, Kundenkonten, Formulareingaben, Kommentare. Betroffen sind Besucher, Kunden, Nutzer und Mitarbeiter des Kunden, deren Daten auf der Website liegen.

Benachrichtigungen (E-Mail, auf Wunsch Push in der Sityro-App) enthalten den Namen der Website und den Anlass; Empfänger sind die Personen, die der Kunde dafür einträgt.

4. Ort der Verarbeitung

Die Daten werden in Deutschland verarbeitet und gespeichert, in Rechenzentren der Hetzner Online GmbH. Ausnahme ist die KI-gestützte Beurteilung einzelner Programmdateien (Abschnitt 5) bei einem Unterauftragsverarbeiter in den USA. Weitere Übermittlungen in Länder außerhalb der EU erfolgen nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind und der Kunde vorab informiert wurde (Abschnitt 9).

5. KI-gestützte Beurteilung von Programmdateien

In bezahlten Tarifen lässt Sityro einzelne Programmdateien (PHP, JavaScript), die als verdächtig erkannt wurden, von einem KI-Modell beurteilen: Ist das Schadcode, und was tut er? Übermittelt werden nur der Dateiinhalt, der Pfad und die Herkunft der Datei – nie die Datenbank, Inhalte der Website, Bestellungen oder Formulardaten. Programmdateien enthalten in der Regel keine personenbezogenen Daten; ausgeschlossen ist es nicht (z. B. eine im Code hinterlegte E-Mail-Adresse).

Anbieter ist Anthropic, PBC (USA). Grundlage der Übermittlung sind die EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO). Anthropic verwendet über die API übermittelte Daten nach seinen kommerziellen Bedingungen nicht zum Training seiner Modelle und speichert sie nur befristet zur Missbrauchserkennung.

Jede Datei wird nur einmal beurteilt; Sityro speichert das Urteil (schädlich, verdächtig, unbedenklich) mit Begründung, nicht die Datei. Das Urteil allein löst nie eine Änderung an der Website aus. Der Kunde kann die KI-Beurteilung in den Einstellungen seiner Organisation jederzeit abschalten; die übrigen Prüfverfahren bleiben.

6. Weisungen

Silicon Planet verarbeitet die Daten nur auf dokumentierte Weisung des Kunden. Weisungen sind die Einstellungen und Aufträge, die der Kunde in Sityro gibt (z. B. eine Wiederherstellung, eine Reparatur, die Aufbewahrungsdauer der Backups, das Löschen einer Website oder der Organisation), sowie Anfragen in Textform an help@sityro.com.

Hält Silicon Planet eine Weisung für rechtswidrig, weist sie den Kunden unverzüglich darauf hin und darf die Ausführung aussetzen, bis der Kunde sie bestätigt oder ändert. Eine Verarbeitung ohne Weisung erfolgt nur, wenn das Recht der EU oder Deutschlands sie verlangt; dann informiert Silicon Planet den Kunden vorher, soweit das Recht es erlaubt.

7. Vertraulichkeit

Alle Personen, die bei Silicon Planet Zugang zu den Daten haben, sind zur Vertraulichkeit verpflichtet. Zugang haben nur die Personen, die ihn für Betrieb, Wartung und Support von Sityro brauchen.

8. Sicherheit der Verarbeitung (Art. 32 DSGVO)

Übertragung: ausschließlich verschlüsselt (TLS). Das Plugin signiert jede Anfrage; Aufträge von Sityro an die Website (Reparatur, Wiederherstellung, Schutzregeln) sind kryptografisch signiert, haben eine feste Aktionsliste und enthalten nie Programmcode.

Speicherung: Backups werden verschlüsselt gespeichert (AES-256-GCM, ein eigener Schlüssel je Organisation). Die Schlüssel verwaltet Silicon Planet, weil eine Wiederherstellung ohne den Kunden möglich sein muss; die Verschlüsselung schützt gegen Zugriff Dritter auf den Speicher, nicht gegen Silicon Planet selbst.

Zugang: Anmeldung in Sityro Central nur mit Passwort, Zwei-Faktor-Anmeldung möglich; kritische Aktionen verlangen eine erneute Bestätigung; strikte Trennung der Organisationen; Zugriffe und sicherheitsrelevante Aktionen werden protokolliert.

Verfügbarkeit und Belastbarkeit: Betrieb in Rechenzentren in Deutschland mit DDoS-Schutz, regelmäßige Sicherung der Datenbank von Sityro, getrennte Test- und Produktionsumgebung, laufende Aktualisierung der eingesetzten Software.

Änderungen an der Website: Vor jeder Reparatur und jeder Wiederherstellung legt Sityro einen Sicherungspunkt in seinem eigenen Speicher an; Dateien, die eine Reparatur ersetzt oder entfernt, bleiben zusätzlich 30 Tage in einer Quarantäne auf der Website und lassen sich zurücklegen.

Silicon Planet passt diese Maßnahmen dem Stand der Technik an; das vereinbarte Schutzniveau wird dabei nicht unterschritten.

9. Unterauftragsverarbeiter

Der Kunde genehmigt den Einsatz der folgenden Unterauftragsverarbeiter:

Hosting der Anwendung, Datenbank und Objektspeicher für Backups: Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland – Rechenzentren in Deutschland.

E-Mail-Versand: Mailjet (Mailjet SAS, Sinch-Gruppe), Frankreich – Empfängeradressen und Inhalte der Benachrichtigungen.

KI-Beurteilung von Programmdateien: Anthropic, PBC, USA – siehe Abschnitt 5.

Fehlererfassung von Sityro Central: Sentry (Functional Software, Inc., USA), Datenregion EU (Frankfurt am Main) – technische Fehlerberichte der Anwendung. Sie können Kennungen und Adressen von Organisationen und Websites enthalten; Inhalte von Dateien und Backups, IP-Adressen von Besuchern, Passwörter und Zugangsdaten werden nicht übermittelt.

Push-Benachrichtigungen in der Sityro-App (nur wenn die App genutzt und Push eingeschaltet ist): Apple Inc. (Apple Push Notification Service) bzw. Google LLC (Firebase Cloud Messaging) – Geräte-Kennung und, je nach Einstellung, Name der Website und Anlass.

Silicon Planet informiert den Kunden mindestens vier Wochen vor dem Einsatz eines neuen oder dem Austausch eines Unterauftragsverarbeiters; die neue Fassung dieses Vertrags wird beim nächsten Login bestätigt. Der Kunde kann aus wichtigem datenschutzrechtlichem Grund widersprechen; ist eine Einigung

nicht möglich, kann er den Vertrag zum Zeitpunkt des Wechsels kündigen. Silicon Planet verpflichtet jeden Unterauftragsverarbeiter vertraglich auf dieselben Datenschutzpflichten.

Keine Auftragsverarbeitung ist die Abrechnung: Die Zahlungsabwicklung über Stripe (Stripe Payments Europe, Ltd., Irland) betrifft die Vertrags- und Zahlungsdaten des Kunden selbst, nicht Daten seiner Websites. Sie ist in der Datenschutzerklärung beschrieben.

10. Rechte der betroffenen Personen

Silicon Planet unterstützt den Kunden mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anfragen betroffener Personen zu beantworten (Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch). Wendet sich eine betroffene Person direkt an Silicon Planet, leitet Silicon Planet die Anfrage unverzüglich an den Kunden weiter und beantwortet sie nicht selbst. Backups kann der Kunde jederzeit als ZIP-Archiv herunterladen.

11. Unterstützung bei weiteren Pflichten

Silicon Planet unterstützt den Kunden bei der Einhaltung seiner Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, vorherige Konsultation) und stellt dafür die nötigen Informationen bereit.

12. Verletzungen des Schutzes personenbezogener Daten

Silicon Planet meldet dem Kunden eine Verletzung des Schutzes personenbezogener Daten, die seine Daten betrifft, unverzüglich, möglichst innerhalb von 24 Stunden nach Kenntnis, an die E-Mail-Adressen der Admins der Organisation. Die Meldung enthält, soweit bekannt, Art und Umfang der Verletzung, die betroffenen Daten, die wahrscheinlichen Folgen und die ergriffenen Maßnahmen. Silicon Planet ergreift unverzüglich Maßnahmen, um die Verletzung zu beheben und ihre Folgen zu mildern.

13. Löschung und Rückgabe

Backups werden nach Ablauf der vom Kunden eingestellten Aufbewahrung laufend gelöscht, vier Wochen nach dem Ende des bezahlten Tarifs vollständig, einschließlich aller Known Goods. Bis dahin kann der Kunde sie herunterladen. Sicherungspunkte vor einer Reparatur werden nach sieben Tagen gelöscht.

Löscht der Kunde eine Website, werden ihre Daten bei Sityro gelöscht, einschließlich ihrer Backups. Löscht der Kunde die Organisation, löscht Silicon Planet alle Daten im Auftrag; die Benutzerkonten bleiben bestehen, solange sie zu anderen Organisationen gehören.

Gesetzliche Aufbewahrungspflichten bleiben unberührt.

14. Nachweise und Kontrollen

Silicon Planet stellt dem Kunden auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Einhaltung dieses Vertrags nötig sind, und ermöglicht Überprüfungen durch den Kunden oder einen von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer. Kontrollen vor Ort werden mit angemessenem

Vorlauf abgestimmt und finden während der Geschäftszeiten statt; Hinweise auf geeignete Zertifizierungen der Unterauftragsverarbeiter (z. B. ISO 27001 der Rechenzentren) können eine Kontrolle vor Ort ersetzen.

15. Schlussbestimmungen

Es gilt deutsches Recht. Änderungen dieses Vertrags werden als neue Fassung bereitgestellt und beim nächsten Login bestätigt. Ist eine Bestimmung unwirksam, bleibt der übrige Vertrag wirksam; an ihre Stelle tritt die gesetzliche Regelung.