Vereinbarung über die Auftragsdatenbearbeitung

siabit AG
Wambisterstrasse 1a
5412 Gebenstorf (Schweiz)

Version 250409.3 - Gültig ab 01.01.2025 – App Version 3.0

09.04.2025_250409.3_doc_8261

Inhalt

1 Einleitung

Die vorliegende Vereinbarung konkretisiert die Verpflichtungen der Parteien in Bezug auf die Vorgaben aus dem Schweizer Datenschutzgesetz (DSG) und der Datenschutzgrundverordnung der EU (EU-DSGVO). Sie ergänzt diesbezüglich die vertraglichen Vereinbarungen ("Vertrag") zwischen siabit AG und dem Kunden. Es kann sich dabei um einen einzelnen oder mehrere Verträge zwischen siabit AG und dem Kunden handeln, in welchen siabit AG als Leistungserbringerin gegenüber dem Kunden auftritt.

Die vorliegende Vereinbarung gilt nur insofern und insoweit als die nachfolgenden Voraussetzungen erfüllt sind:

- Der Kunde ist entweder Verantwortlicher oder Auftragsbearbeiter im Anwendungsbereich des DSG und/oder der EU-DSGVO und
- der Kunde zieht siabit AG im Rahmen des Vertrages als Auftragsbearbeiter oder Unter-Auftragsbearbeiter für die Bearbeitung von Personendaten bzw. von personenbezogenen Daten bei, welche vom Anwendungsbereich des DSG und/oder der EU-DSGVO erfasst sind ("relevante Daten").

2 Gegenstand, Dauer und Art der Datenbearbeitung

Gegenstand, Dauer sowie Art und Zweck der Bearbeitung ergeben sich aus dem Vertrag. Die Kategorien der bearbeiteten relevanten Daten, die Kategorien betroffener Personen sowie die zu treffenden technischen und organisatorischen Massnahmen ("TOM") sind im Anhang dieser Vereinbarung aufgeführt.

3 Anwendungsbereich und Verantwortlichkeit

siabit AG bearbeitet die relevanten Daten ausschliesslich zum Zweck der Vertragserfüllung bzw. zu den im Vertrag genannten Zwecken. Der Kunde ist für die Rechtmässigkeit der Datenbearbeitung an sich, inklusive der Zulässigkeit der Auftrags-/Unter-Auftragsbearbeitung, verantwortlich.

Die Weisungen des Kunden sind in dieser Vereinbarung und dem Vertrag dokumentiert. Der Kunde hat das Recht, siabit AG jederzeit schriftlich darüberhinausgehende Weisungen in Bezug auf die Bearbeitung der relevanten Daten zu erteilen. Führen solche Weisungen zu Mehrkosten von siabit AG oder einem geänderten Leistungsumfang, so ist das vertraglich vereinbarte Vertragsänderungsverfahren anwendbar.

siabit AG informiert den Kunden unverzüglich, wenn sie der Auffassung ist, dass eine Weisung gegen das DSG oder die EU-DSGVO verstösst. siabit AG darf diesfalls die Umsetzung der Weisung so lange aussetzen, bis sie vom Kunden bestätigt oder abgeändert wurde. Bei Weisungen des Kunden im Zusammenhang mit der Vergabe von Zugriffsberechtigungen oder der Herausgabe von relevanten Daten an den Kunden selbst gilt das Vorstehende nicht, und siabit AG darf jederzeit davon ausgehen, dass diese Weisungen gesetzeskonform sind. Sie ist jedoch berechtigt, vom Kunden entsprechende schriftliche Bestätigungen zu verlangen.

4 Pflichten von siabit AG

siabit AG bearbeitet die relevanten Daten ausschliesslich gemäss den Bestimmungen aus dem Vertrag und dieser Vereinbarung. Vorbehalten bleibt die Erfüllung gesetzlicher, regulatorischer oder behördlicher Verpflichtungen durch siabit AG.

siabit AG wird die im Vertrag und den Anhängen zu dieser Vereinbarung definierten TOM zum Schutz der relevanten Daten treffen. siabit AG ist berechtigt, die vereinbarten Technisch-Organisatorischen Maßnahmen (TOM) jederzeit anzupassen, sofern dadurch das vereinbarte Schutzniveau nicht unterschritten wird. Über vorgenommene Anpassungen wird der Auftraggeber unverzüglich, spätestens jedoch zehn Werktage vor deren Wirksamwerden, schriftlich informiert. Zudem überprüft siabit AG laufend die vereinbarten TOM auf den aktuellen Stand der Technik und schlägt dem Kunden gegebenenfalls die Implementierung zusätzlicher Massnahmen vor, welche im Rahmen eines Vertragsnachtrags vereinbart werden können.

siabit AG verpflichtet sich, in Bezug auf die relevanten Daten ein Verzeichnis von Bearbeitungstätigkeiten im Einklang mit Art. 12 Abs. 1 DSG bzw. Art. 30 Abs. 2 EU-DSGVO zu führen. siabit AG wird dem Kunden jederzeit auf Anfrage Einblick in die Teile dieses Verzeichnis gewähren, die von der Leistungserbringung von siabit AG ihm gegenüber betroffen sind.

siabit AG stellt sicher, dass es den mit der Bearbeitung der relevanten Daten des Kunden befassten Mitarbeitenden und anderen Hilfspersonen von siabit AG untersagt ist, die relevanten Daten zu anderen als den im Vertrag genannten Zwecken und abweichend von dieser Vereinbarung zu bearbeiten. Ferner stellt siabit AG sicher, dass sich die zur Bearbeitung der relevanten Daten befugten Personen zur Vertraulichkeit verpflichtet haben und/oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/Verschwiegenheitspflicht besteht auch nach Beendigung des Vertrages fort.

siabit AG unterrichtet den Kunden unverzüglich, wenn ihr Verletzungen des Schutzes der relevanten Daten bei siabit AG oder einem ihrer Unter-Auftragsbearbeiter bekannt werden (Data Breach). siabit AG informiert den Kunden schriftlich (E-Mail ausreichend) in angemessener Weise über Art und Ausmass der Verletzung sowie mögliche Abhilfemassnahmen. Die Parteien treffen in so einem Fall die erforderlichen Massnahmen zur Sicherstellung des Schutzes der relevanten Daten und zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen sowie die Parteien und sprechen sich hierzu unverzüglich ab.

siabit AG nennt dem Kunden den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen sowie in den Fällen, in denen dies gemäss Art. 37 EU-DSGVO vorgeschrieben ist, den Datenschutzbeauftragten.

siabit AG verpflichtet sich, den Kunden auf Wunsch und gegen vorgängig vereinbarte separate Vergütung im Rahmen ihrer Möglichkeiten bei der Erfüllung der Rechte der betroffenen Personen gegenüber dem Kunden gemäss Kapitel 4 des DSG bzw. Kapitel III der EU-DSGVO zu unterstützen. Darüber hinaus kann siabit AG dem Kunden auf Wunsch weitergehende Unterstützung anbieten, z.B. im Zusammenhang mit Konsultationen mit der Aufsichtsbehörde oder Meldungen an diese. Die Unterstützung im Rahmen einer Datenschutzfolgeabschätzung erfolgt kostenneutral, soweit sie ausschließlich Informationen zu den vom Auftragnehmer umgesetzten technischen und organisatorischen Maßnahmen betrifft.

Relevante Daten sind nach Vertragsende gemäss den vertraglichen Bestimmungen herauszugeben oder zu löschen. siabit AG setzt hierfür Verfahren ein, die dem in der IT-Branche anerkannten Stand der Technik entsprechen. Die Löschung einer Lizenz erfolgt spätestens sechs Monate nach Kündigung automatisch. Der Kunde hat die Möglichkeit, eine vorzeitige Löschung anzuordnen, wodurch der Löschprozess unmittelbar ausgelöst wird. Nach Löschung verbleiben die Daten bis zu 30 Tage im aktiven System, um eine etwaige Wiederherstellung zu ermöglichen. Anschliessend beginnt ein automatisierter Löschprozess, im Rahmen dessen die Daten endgültig entfernt werden. Gemäss den Richtlinien von Google kann die vollständige Löschung, einschliesslich aller Sicherungskopien, bis zu zwei Monate beanspruchen.

5 Pflichten und Obliegenheiten des Kunden

Der Kunde trifft in seinem Verantwortungsbereich (z.B. auf seinen eigenen Systemen, Gebäuden, Applikationen/Umgebungen in seiner Betriebsverantwortung) selbständig angemessene technische und organisatorische Massnahmen zum Schutz der relevanten Daten.

Der Kunde hat siabit AG unverzüglich zu informieren, wenn er in der Leistungserbringung von siabit AG Verletzungen datenschutzrechtlicher Bestimmungen feststellt.

Der Kunde nennt siabit AG den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen sowie in den Fällen, in denen dies gemäss Art. 37 EU-DSGVO vorgeschrieben ist, den Datenschutzbeauftragten.

6 Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung, Auskunft oder anderen Ansprüchen zu relevanten Daten direkt an siabit AG, wird siabit AG die betroffene Person an den Kunden verweisen, sofern eine Zuordnung an den Kunden nach Angaben der betroffenen Person möglich ist. Die Unterstützung des Kunden seitens siabit AG bei Anfragen betroffener Personen richtet sich nach Ziffer 4.

7 Nachweismöglichkeiten, Berichte und Audits

siabit AG ist verpflichtet, dem Kunden auf Verlangen Informationen zur Verfügung zu stellen, um die Einhaltung der Pflichten gemäss dieser Vereinbarung zu dokumentieren.

Die Parteien halten fest, dass die Einhaltung dieser Verpflichtung grundsätzlich dadurch belegt wird, dass siabit AG nach ISO 27001 zertifiziert ist oder siabit AG dem Kunden zu bestimmten Bereichen Berichte oder ähnliche durch einen unabhängigen Dritten erstellte Auditberichte oder Bestätigungen über im Vertrag speziell erwähnte Zertifizierungen etc. zur Verfügung stellt. Im Vertrag allfällig definierte Audit-Rechte sowie gesetzlich zwingend vorgeschriebene Prüfrechte des Kunden oder seiner Aufsichtsbehörden bleiben vorbehalten. Auf jeden Fall sind im Rahmen solcher Audits der Grundsatz der Verhältnismässigkeit einzuhalten sowie die schutzwürdigen Interessen von siabit AG (namentlich an Geheimhaltung) angemessen zu berücksichtigen. Vorbehältlich einer abweichenden Regelung trägt der Kunde sämtliche Kosten solcher Audits (inklusive nachgewiesene interne Kosten von siabit AG, die bei der Mitwirkung am Audit entstehen).

Werden nach Vorlage von Nachweisen oder Berichten oder im Rahmen eines Audits Verletzungen dieser Vereinbarung oder Mängel bei der Umsetzung der Pflichten von siabit AG festgestellt, so hat siabit AG unverzüglich und kostenlos geeignete Korrekturmassnahmen zu implementieren.

8 Beizug von Unter-Auftragsbearbeitern

Soweit der Vertrag keine einschränkenderen Bestimmungen zum Beizug Dritter enthält, ist siabit AG zum Beizug von Unter-Auftragsbearbeitern berechtigt, hat jedoch den Kunden vorgängig darüber zu informieren, wenn sie nach Inkrafttreten dieser Vereinbarung neue Unter-Auftragsbearbeiter beizieht oder bestehende Unter-Auftragsbearbeiter austauscht. Der Kunde kann gegen den Beizug eines neuen oder den Austausch eines bestehenden Unter-Auftragsbearbeiters aus wichtigen datenschutzrechtlichen Gründen schriftlich innerhalb einer Frist von 30 Tagen Einspruch erheben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Kunden ein Kündigungsrecht in Bezug auf die hiervon betroffene Leistung eingeräumt. siabit AG wird mit ihren Unter-Auftragsbearbeitern im erforderlichen Umfang Vereinbarungen treffen, um die Verpflichtungen gemäss vorliegender Vereinbarung sicherzustellen.

9 Liste der Unter-Auftragsbearbeiter Stand 09.04.2025

Unternehmen	Standort	Zweck	Kundenkontakte	Kundendaten	Besondere personenbezogene Daten gem. DSGVO (Art. 9 Abs. 1)
Google Cloud Services Zürich, Region europe-west6	Zürich, Schweiz	Hosting der Software Applikation ForstControl, Timedoo, MRControl	Ja	Ja	Nein
Pius Gutzwiller	Märstetten, Schweiz	Management-Mandat, Cybersecurity-Supervisor	Ja	Ja	Nein
Cloudflare	San Francisco USA	Internet-Sicherheitsdienste, Verschlüsselung	Nein	Nein	Nein
Atlassian PTY	Sydney, Australien	Aufgaben- und Projektmanagement, Dokumentation	Nein	Nein	Nein
Exxas AG	Zürich, Schweiz	ERP / CRM System	Ja	Nein	Nein
Brevo (Sendinblue GmbH)	Berlin, Deutschland	Newsletter Tool Marketing	Ja (Teils)	Nein	
Zapier Inc.	Columbia, USA	Workflow-Automatisierung Marketing	Nein	Nein	Nein
cyon GmbH	Basel, Schweiz	Hosting von Landingpages	Nein	Nein	Nein
Hostpoint AG	Rapperswil-Jona, Schweiz	Hosting von Landingpages	Nein	Nein	Nein
GitHub	San Francisco, USA	Code - Versionsverwaltungs-Software	Nein	Nein	Nein

10 Bekanntgabe ins Ausland

Jedwede Bekanntgabe von relevanten Daten durch siabit AG ins Ausland oder an eine internationale Organisation ist nur zulässig, wenn siabit AG die Bestimmungen von Art. 16 ff. DSG bzw. von Kapitel V EU-DSGVO einhält. Soweit hingegen eine solche Bekanntgabe von relevanten Daten vom Kunden gewünscht bzw. in seinem Auftrag erfolgt, obliegt die Einhaltung der entsprechenden Bestimmungen ausschliesslich dem Kunden.

11 Schlussbestimmungen

Die Artikelnummern des DSG beziehen sich auf das revidierte DSG (BBl 2020 7639) sowie das DSGVO (Verordnung (EU) 2016/679). Vor dessen Inkrafttreten gelten die vorliegend vereinbarten Bestimmungen sinngemäss. Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit aller Verträge zwischen siabit AG und dem Kunden, unter welchen siabit AG für den Kunden relevante Daten bearbeitet, sofern sich aus den Bestimmungen dieser Vereinbarung nicht länger dauernde Verpflichtungen ergeben.

In Abweichung allfälliger Schriftformvorbehalte im Vertrag kann die vorliegende Vereinbarung auch auf elektronischem Weg zwischen den Parteien vereinbart oder geändert werden.

Die Pflichten aus dieser Vereinbarung gelten zusätzlich zu den im Vertrag festgelegten Pflichten und schränken letztere nicht ein. In Bezug auf die in einem Anhang zu dieser Vereinbarung generisch festgelegten TOM gehen im Widerspruchsfall die Regelungen des Vertrages vor. Im Übrigen gelten die Regelungen des Vertrages unverändert weiter.

Anhang

Verwendete Datenelemente

Generell
Der Kunde überlässt siabit AG im Rahmen der Verträge in seinem eigenen Ermessen und in seinem Auftrag Personendaten zur Bearbeitung.

Betroffene Personen
Es kann sich dabei um Personendaten insbesondere folgender betroffener Personen handeln:

- Potenzielle Kunden, Kunden, Geschäftspartner, Verkäufer und Händler des Kunden – welche natürlichen Personen sind
- Mitarbeitende oder andere Hilfspersonen von potenziellen Kunden, Kunden, Geschäftspartnern, Verkäufern, oder Händlern
- Mitarbeitende oder andere Hilfspersonen des Kunden, welche durch den Kunden berechtigt wurden die Services zu nutzen

Art von Personendaten
Es kann sich dabei insbesondere um folgende Arten von Personendaten handeln:

- Persönliche Informationen wie Vorname, Name, Geburtsdatum, Alter, Geschlecht, Nationalität etc.
- Geschäftliche Kontaktdaten wie E-Mailadresse, Telefonnummer, Adresse

- Private Kontaktdaten wie E-Mailadresse, Telefonnummer, Adresse
- Informationen über das Berufsleben wie Stellenbezeichnung, Funktion etc.
- Benutzerinformationen wie Logindaten, Kundennummer, Personalnummer etc.
- Technische Informationen wie IP-Adresse, Geräteinformationen etc.

Besonders schützenswerte Personendaten
Bei diesen Datenkategorien handelt es sich um Personendaten aus denen die rassische und ethnische Herkunft, politische Meinung, religiöse oder weltanschauliche Überzeugung oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten oder biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.

Geheimnisgebundene Daten
Bei diesen Daten kann es sich beispielsweise um das Berufsgeheimnis, dem Bankgeheimnis, dem Amtsgeheimnis, der Verschwiegenheitspflicht gemäss Sozialversicherungsrecht unterliegende Daten handeln.

Technische und organisatorische Massnahmen (TOM)

Die folgenden Kapitel beschreiben die von der siabit AG getroffenen Massnahmen in Bezug auf den Schutz von Personendaten im Rahmen der Auftragsdatenbearbeitung. Die nachstehend aufgeführten Massnahmen sind generisch zu verstehen und kommen jeweils dann zur Anwendung, wenn im Vertrag nichts Abweichendes definiert ist.

Zutrittskontrolle (Gebäude/Büroräumlichkeiten)
siabit AG hat (unter anderem) die folgenden Massnahmen ergriffen, um den unerlaubten Zugriff auf IT-Systeme zu vermeiden, in denen personenbezogene Daten verarbeitet werden:

- 7/24 Kameraüberwachung der Büroräume mit mehrfacher Alarmsicherung
- Mehrfach Authentifizierung auf allen Systemen
- Zugriffskontrolle auf die IT-Landschaft
- Schlüssel-Management
- Besucherregistrierung
- Sicherheitsschlösser
- Sorgfältige Auswahl des Reinigungspersonals

Zugriffskontrolle (System)
siabit AG hat (unter anderem) die folgenden Massnahmen ergriffen, um den Zugriff Unberechtigter auf Datenverarbeitungssysteme zu vermeiden:

- Vergabe von Benutzerrechten
- Zugriff nach Berechtigungskonzept gemäss Need-to-Know Prinzip
- Passwortvergabe mit Mindestanforderungen an Passwortkomplexität
- Authentifizierung mit Benutzername / Passwort und Multifaktor Authentifizierung
- Verwendung von Intrusion-Prevention-Systemen und von Firewalls
- Verwendung von mehreren Netzwerkzonen
- Verwendung von personalisierten Benutzerprofilen
- Einsatz von Web Application Firewalls
- Regelmässige externe Vulnerability Scans
- Patch Management
- Verwendung von Virenscannern
- Verwendung von VPN-Technologie
- Anzahl Administratoren auf nötiges Minimum reduziert

- Verschlüsselung transportierter Daten mit TLS
- Kontrolle der Berechtigungen bei Eintritt und Austritt von Mitarbeitenden

Zugriffskontrolle (Daten)
siabit AG hat (unter anderem) die folgenden Massnahmen ergriffen, um sicherzustellen, dass Nutzer nur auf diejenigen Daten Zugriff haben, für die sie autorisiert sind und um zu vermeiden, dass personenbezogene Daten ohne Autorisierung gelesen werden können:

- Einsatz rollenbasierten Autorisierungskonzept nach Need-to-Know Prinzip
- Anzahl Administratoren auf nötiges Minimum reduziert
- Protokollierung von Applikationszugriffen
- Sichere Medienbereinigung vor der Wiederverwendung
- Keine Verwendung von Papierunterlagen
- Verschlüsselung transportierter Daten mit TLS
- Rechteverwaltung durch Systemadministratoren
- Passwort-Richtlinie mit geltenden Mindestanforderungen an Passwortkomplexität
- Sichere Aufbewahrung von Backup-Datenträgern in einem Banksafe
- Konforme Zerstörung von Datenträgern

Übertragungskontrolle
siabit AG hat (unter anderem) die folgenden Massnahmen ergriffen, um sicherzustellen, dass personenbezogene Daten nicht gelesen, kopiert, oder modifiziert werden können während der elektronischen Übermittlung, des Transports oder der Speicherung:

- Einsatz einer Standleitung und/oder VPN-Verbindungen
- Verschlüsselung transportierter Daten mit TLS
- Dokumentation der Datenempfänger und der Übertragungszeiten
- Für den physischen Transport, sorgfältige Auswahl des Transportpersonals und der Fahrzeuge und sowie Verschlüsselung des genutzten Speichermediums
- Datenoffenbarung nur in anonymisierter oder pseudonymisierter Form

Eingabekontrolle
siabit AG hat (unter anderem) die folgenden Massnahmen ergriffen, um sicherzustellen, dass es möglich ist nachzuvollziehen und zu kontrollieren, ob und wer personenbezogene Daten eingibt, modifiziert oder aus Datenverarbeitungssystem löscht:

- Protokollierung der Eingabe, Modifikation und Löschung von Daten
- Rückverfolgbarkeit der Eingabe, Modifikation und Löschung von Daten durch individuelle Benutzerprofile
- Rechtevergabe für Eingabe, Modifikation und Löschung von Daten basierend auf einem Autorisierungskonzept

Auftragskontrolle
siabit AG hat (unter anderem) die folgenden Massnahmen ergriffen, um sicherzustellen, dass in seinem Auftrag und im Einvernehmen mit dem Verantwortlichen weiterverarbeitete Daten nur auf dessen Weisung hin verarbeitet werden:

- Sorgfältige Auswahl nach hohen Sicherheitskriterien der Unterauftragnehmer unter Berücksichtigung ihrer Historie (insbesondere hinsichtlich Informationssicherheit)