

Vereinbarung über die Auftragsbearbeitung von Personendaten (AVV)

gemäss Art. 9 des Schweizerischen Datenschutzgesetzes (DSG) und Art. 28 der Datenschutz-Grundverordnung (DSGVO)

zwischen dem Kunden (nachfolgend «Verantwortlicher») und der FireStorm ISP GmbH, Kirchenrainstrasse 27, 8632 Tann, Schweiz (nachfolgend «FireStorm» oder «Auftragsbearbeiter»)

Version Oktober 2026

1. Gegenstand und Dauer

- 1.1 Diese Vereinbarung regelt die Bearbeitung von Personendaten, die FireStorm im Auftrag des Verantwortlichen im Rahmen der vereinbarten Dienstleistungen (Hauptvertrag) bearbeitet, insbesondere Webhosting, E-Mail-Dienste, vServer, Rootserver, dedizierte Server, Speicher- und Backup-Dienste sowie Domain- und DNS-Dienste.
- 1.2 Die Dauer dieser Vereinbarung richtet sich nach der Dauer des Hauptvertrags. Die Beendigung des Hauptvertrags beendet auch diese Vereinbarung; die Pflichten nach Ziffer 12 (Rückgabe und Löschung) und die Vertraulichkeit gelten darüber hinaus.
- 1.3 Diese Vereinbarung ergänzt die Allgemeinen Geschäftsbedingungen (AGB) von FireStorm. In Fragen des Datenschutzes geht diese Vereinbarung den AGB vor.

2. Art, Zweck und Umfang der Bearbeitung

- 2.1 FireStorm stellt dem Verantwortlichen die Infrastruktur für die Speicherung und Bearbeitung seiner Daten zur Verfügung (Hosting, Server, Speicher, Backup, Netzwerk). Die Bearbeitung umfasst insbesondere das Speichern, Sichern, Übermitteln, Wiederherstellen und Löschen von Daten, ausschliesslich zur Erbringung der vereinbarten Dienstleistungen.
- 2.2 Art der Personendaten und Kreis der betroffenen Personen bestimmt allein der Verantwortliche durch die Nutzung der Dienste. Dazu können Personenstammdaten, Kommunikationsdaten, Vertragsdaten, Protokolldaten sowie, je nach Anwendung des Verantwortlichen, besonders schützenswerte Personendaten (z. B. Gesundheitsdaten) gehören. Betroffene Personen können insbesondere Kunden, Patienten, Mitarbeitende und Lieferanten des Verantwortlichen sein.
- 2.3 Bei vServern, Rootservern und dedizierten Servern verwaltet der Verantwortliche Betriebssystem, Anwendungen und Daten selbst. FireStorm hat keine Zugangsdaten zu diesen Systemen und greift nicht auf die darin gespeicherten Daten zu. Die Bearbeitung durch FireStorm beschränkt sich auf den Betrieb der Infrastruktur sowie die Erstellung und Aufbewahrung der vereinbarten Backups. Dedizierte Server verfügen über keine Backup-Funktion; für deren Datensicherung ist ausschliesslich der Verantwortliche zuständig.

3. Ort der Bearbeitung

- 3.1 Daten aus Webhosting, E-Mail-Diensten, vServern, Rootservern, dedizierten Servern sowie sämtliche Backups und Snapshots werden ausschliesslich in Rechenzentren in der Schweiz gespeichert und bearbeitet.
- 3.2 Für die georedundante Namensauflösung betreibt FireStorm DNS-Server zusätzlich an Standorten in Deutschland und Frankreich. Dort werden ausschliesslich DNS-Zonendaten (Domainnamen, IP-Adressen und weitere DNS-Einträge) gespeichert, keine Inhalte aus Hosting, E-Mail oder Servern. Diese Staaten verfügen gemäss Anhang 1 der Datenschutzverordnung (DSV) über einen angemessenen Datenschutz.

- 3.3 Für Produkte von Drittanbietern, die der Verantwortliche über FireStorm bezieht (z. B. Domainnamen, SSL-Zertifikate, Microsoft 365), gelten die in Anhang 2 genannten Bearbeitungsorte.
- 3.4 Administration und Support erfolgen durch Mitarbeitende von FireStorm in der Schweiz. Externe Hersteller-Supports (z. B. Software- oder Hardwarehersteller) erhalten im Einzelfall, soweit für die Behebung einer Störung erforderlich, einen zeitlich begrenzten und überwachten Zugriff auf die Infrastruktur, nie jedoch auf Daten innerhalb von vServern, Rootservern und dedizierten Servern.

4. Weisungen des Verantwortlichen

- 4.1 FireStorm bearbeitet Personendaten ausschliesslich im Rahmen des Hauptvertrags, dieser Vereinbarung und der dokumentierten Weisungen des Verantwortlichen, es sei denn, FireStorm ist durch Schweizer Recht zu einer Bearbeitung verpflichtet. In diesem Fall teilt FireStorm dem Verantwortlichen diese rechtlichen Anforderungen vorgängig mit, soweit dies gesetzlich zulässig ist.
- 4.2 Weisungen erteilt der Verantwortliche per Ticket oder schriftlich. Ist FireStorm der Ansicht, dass eine Weisung gegen Datenschutzvorschriften verstösst, informiert FireStorm den Verantwortlichen unverzüglich und darf die Ausführung bis zur Bestätigung oder Änderung der Weisung aussetzen.
- 4.3 Weisungen, die über den vereinbarten Leistungsumfang hinausgehen, werden nach Aufwand verrechnet.

5. Pflichten von FireStorm

- 5.1 FireStorm wahrt die Vertraulichkeit der Personendaten. Alle Mitarbeitenden, die Zugang zur Infrastruktur haben, sind schriftlich zur Verschwiegenheit verpflichtet, auch über das Ende des Arbeitsverhältnisses hinaus, und werden regelmässig in Datenschutz und Informationssicherheit geschult.
- 5.2 Kopien von Daten werden ohne Wissen des Verantwortlichen nicht erstellt. Ausgenommen sind die vereinbarten Backups sowie Kopien, die für einen ordnungsgemässen Betrieb technisch erforderlich sind.
- 5.3 FireStorm gibt Personendaten nur heraus, wenn eine gesetzliche Pflicht oder eine Anordnung einer zuständigen Schweizer Behörde oder eines Schweizer Gerichts besteht. Soweit gesetzlich zulässig, informiert FireStorm den Verantwortlichen vorgängig. Anfragen ausländischer Behörden werden nur auf dem Weg der Rechtshilfe beantwortet.
- 5.4 Als Datenschutzberater von FireStorm ist Herr Christian Geissler bestellt (support@firestorm.ch, 0844 300 200). Ein Wechsel wird dem Verantwortlichen mitgeteilt.

6. Technische und organisatorische Massnahmen

- 6.1 FireStorm trifft die in Anhang 1 beschriebenen technischen und organisatorischen Massnahmen, um eine dem Risiko angemessene Datensicherheit gemäss Art. 8 DSG und Art. 32 DSGVO zu gewährleisten.
- 6.2 Die Massnahmen werden regelmässig überprüft und dem Stand der Technik angepasst. Das Schutzniveau darf dabei nicht unterschritten werden. Wesentliche Änderungen teilt FireStorm dem Verantwortlichen mit.
- 6.3 Für die Sicherheit innerhalb von vServern, Rootservern und dedizierten Servern (Betriebssystem, Anwendungen, Zugangsdaten, Verschlüsselung der Anwendungsdaten) ist der Verantwortliche selbst verantwortlich.

7. Meldung von Verletzungen der Datensicherheit

- 7.1 FireStorm informiert den Verantwortlichen unverzüglich, in der Regel innert 24 Stunden, nachdem eine Verletzung der Datensicherheit in der Infrastruktur von FireStorm (Virtualisierungsplattform, Speicher- und Backup-Systeme, Kundenpanel, Netzwerk) bestätigt ist, welche die Daten des Verantwortlichen betreffen könnte.
- 7.2 Die Meldung enthält, soweit bekannt, die Art der Verletzung, die betroffenen Systeme und Datenkategorien, die voraussichtlichen Folgen sowie die ergriffenen oder vorgeschlagenen Massnahmen. Noch nicht bekannte Angaben werden laufend nachgereicht.
- 7.3 FireStorm unterstützt den Verantwortlichen bei dessen Meldepflichten gegenüber dem EDÖB (Art. 24 DSG) bzw. der Aufsichtsbehörde (Art. 33 und 34 DSGVO), insbesondere mit Protokollen und Zeitstempeln.
- 7.4 Stellt FireStorm auffälligen Verkehr aus Systemen des Verantwortlichen fest, beispielsweise Angriffe auf Dritte oder Spam, informiert FireStorm den Verantwortlichen. Eine Pflicht zur Überwachung der Systeme des Verantwortlichen besteht nicht.

8. Unterstützung des Verantwortlichen

- 8.1 Wendet sich eine betroffene Person direkt an FireStorm, leitet FireStorm das Gesuch unverzüglich an den Verantwortlichen weiter.
- 8.2 FireStorm unterstützt den Verantwortlichen im Rahmen des Zumutbaren bei der Erfüllung der Rechte betroffener Personen sowie bei Datenschutz-Folgenabschätzungen. Aufwände, die über die Bereitstellung vorhandener Informationen hinausgehen, werden nach Aufwand verrechnet.

9. Unterauftragsbearbeiter

- 9.1 Die zum Zeitpunkt des Vertragsabschlusses eingesetzten Unterauftragsbearbeiter sind in Anhang 2 aufgeführt. Mit Abschluss dieser Vereinbarung stimmt der Verantwortliche ihrem Einsatz zu.
- 9.2 Neue Unterauftragsbearbeiter, die Zugriff auf Daten aus Hosting, E-Mail, Servern oder Backups erhalten, zieht FireStorm nur mit vorgängiger schriftlicher Zustimmung des Verantwortlichen bei. Die Zustimmung kann per E-Mail erteilt werden und darf nur aus wichtigem datenschutzrechtlichem Grund verweigert werden.
- 9.3 Für Produkte von Drittanbietern (Domainnamen, SSL-Zertifikate, Microsoft 365 und vergleichbare Produkte) gilt die Zustimmung zum jeweiligen Anbieter mit der Bestellung des Produkts als erteilt. Über einen Wechsel dieser Anbieter informiert FireStorm vorgängig; der Verantwortliche kann widersprechen.
- 9.4 FireStorm wählt Unterauftragsbearbeiter sorgfältig aus und überbindet ihnen vertraglich Pflichten, die dieser Vereinbarung entsprechen.
- 9.5 Reine Hilfsleistungen ohne Zugriff auf Personendaten, insbesondere Fläche, Strom, Kühlung, physische Sicherheit und Netzanbindung durch Rechenzentrumsbetreiber, gelten nicht als Unterauftragsbearbeitung. Sie sind der Transparenz halber in Anhang 2 aufgeführt.

10. Kontrollrechte

- 10.1 FireStorm stellt dem Verantwortlichen auf Anfrage die Informationen zur Verfügung, die zum Nachweis der Einhaltung dieser Vereinbarung erforderlich sind.
- 10.2 Der Verantwortliche ist berechtigt, die Einhaltung dieser Vereinbarung nach vorgängiger Terminvereinbarung (in der Regel mindestens 14 Tage im Voraus) während der Geschäftszeiten selbst oder durch einen zur Verschwiegenheit verpflichteten Dritten zu kontrollieren. Kontrollen dürfen den Betrieb und die Sicherheit anderer Kunden nicht

beeinträchtigen. Der Aufwand von FireStorm wird nach den jeweils gültigen Stundenansätzen verrechnet.

11. Pflichten des Verantwortlichen

- 11.1 Der Verantwortliche ist allein verantwortlich für die Zulässigkeit der Datenbearbeitung und die Wahrung der Rechte der betroffenen Personen.
- 11.2 Der Verantwortliche informiert FireStorm unverzüglich, wenn er Fehler oder Unregelmässigkeiten bei der Bearbeitung feststellt.

12. Rückgabe und Löschung

- 12.1 Bis zum Vertragsende kann der Verantwortliche seine Daten jederzeit selbst exportieren, bei Servern mit vollem Root-Zugriff auch als vollständiges Abbild. Auf Wunsch unterstützt FireStorm den Verantwortlichen dabei gegen Verrechnung nach Aufwand.
- 12.2 Spätestens 30 Tage nach Vertragsende bzw. nach Freigabe durch den Verantwortlichen löscht FireStorm sämtliche Daten des Verantwortlichen, einschliesslich Server, Datenträger, Snapshots und Backups, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht. Auf Wunsch bestätigt FireStorm die Löschung schriftlich.
- 12.3 Die Daten werden verschlüsselt auf den Datenträgern gespeichert. Defekte oder ausgemusterte Datenträger werden vor der Entsorgung fachmännisch gelöscht oder physisch vernichtet.

13. Haftung

- 13.1 Für die Haftung gelten die Bestimmungen der AGB von FireStorm (insbesondere Ziffer 12).
- 13.2 Für Schäden, die eine betroffene Person wegen einer unzulässigen oder unrichtigen Datenbearbeitung erleidet, ist im Verhältnis zur betroffenen Person der Verantwortliche verantwortlich. Ein Rückgriff des Verantwortlichen auf FireStorm ist nur zulässig, wenn FireStorm vorsätzlich oder grobfahrlässig gegen diese Vereinbarung verstossen hat.
- 13.3 Vertragsstrafen sind ausgeschlossen.

14. Sonderkündigungsrecht

- 14.1 Bei schwerwiegenden Verstössen von FireStorm gegen diese Vereinbarung, insbesondere gegen anwendbare Datenschutzvorschriften, kann der Verantwortliche den Hauptvertrag für die betroffenen Dienstleistungen fristlos kündigen. Bei unerheblichen Verstössen setzt der Verantwortliche zuerst eine angemessene Frist zur Abhilfe.

15. Schlussbestimmungen

- 15.1 Beide Parteien behandeln alle im Rahmen dieser Vereinbarung erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmassnahmen der anderen Partei vertraulich, auch über das Vertragsende hinaus.
- 15.2 Für diese Vereinbarung wird kein zusätzliches Entgelt erhoben, soweit nicht ausdrücklich anders geregelt.
- 15.3 Änderungen und Ergänzungen bedürfen der Schriftform; E-Mail genügt. Individuelle Vereinbarungen mit einzelnen Verantwortlichen gehen dieser Vereinbarung vor.
- 15.4 Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An ihre Stelle tritt eine wirksame Regelung, die dem wirtschaftlichen Zweck am nächsten kommt.
- 15.5 Es gilt ausschliesslich Schweizer Recht. Gerichtsstand ist Hinwil.

15.6 Begriffe werden im Sinne des DSG verwendet; soweit die DSGVO anwendbar ist, im Sinne der DSGVO.

Anhang 1: Technische und organisatorische Massnahmen

Physische Sicherheit (Zutrittskontrolle)

- Betrieb der Server in nach ISO/IEC 27001 zertifizierten Rechenzentren in der Schweiz
- Zutritt nur für berechtigte Personen, Überwachung der Rechenzentren rund um die Uhr
- Redundante Stromversorgung und Netzanbindung
- Backup-Server in einem separaten Rechenzentrum in der Schweiz

Zugangs- und Zugriffskontrolle

- Administrativer Zugang zur Infrastruktur durch eigene Mitarbeitende von FireStorm in der Schweiz; externe Hersteller-Supports nur im Einzelfall, zeitlich begrenzt und überwacht
- Verwaltungsschnittstellen der Virtualisierungs- und Backup-Plattform sind aus dem Internet nicht direkt erreichbar
- Zwei-Faktor-Authentifizierung für das Kundenpanel verfügbar
- Keine Zugangsdaten von FireStorm zu vServern, Rootservern und dedizierten Servern der Kunden; Zugangsdaten setzt der Kunde selbst
- Protokollierung von Aktionen auf Plattformebene (Konsolenzugriff, Start und Stopp, Snapshots, Backups, Wiederherstellungen) mit Benutzer und Zeitstempel

Verschlüsselung und Trennung

- Verschlüsselte Speicherung der Daten auf den Datenträgern
- Verschlüsselte Übertragung (TLS) für Kundenpanel, E-Mail-Dienste und Verwaltung
- Logische Trennung der Kunden durch eigene virtuelle Maschinen bzw. eigene Hosting-Konten

Verfügbarkeit und Belastbarkeit

- Tägliche Backups auf separate Backup-Systeme, aus den Kundensystemen heraus nicht erreichbar (inbegriffen: tägliches Backup mit mehreren Sicherungsständen der letzten Woche; häufigere Sicherungen und längere Aufbewahrung gegen Aufpreis). Dedizierte Server verfügen über keine Backup-Funktion.
- DDoS-Schutz auf Netzwerkebene, vorgelagerte Firewall mit Basis-WAF
- Überwachung der Systeme rund um die Uhr, Störungsdienst 24/7

Integrität und Wartung

- Einspielen von Sicherheitsupdates der Hersteller für die Infrastruktur umgehend, spätestens sobald ein Patch verfügbar ist
- Fachmännische Löschung oder physische Vernichtung defekter und ausgemusterter Datenträger

Organisation

- Schriftliche Verschwiegenheitsverpflichtung aller Mitarbeitenden
- Mitarbeitende mit persönlicher Zertifizierung ISO/IEC 27001 Foundation
- Bestellter Datenschutzberater
- Berufshaftpflichtversicherung für IT- und Telekommunikationsdienstleister inklusive Cyber-Deckung

Anhang 2: Unterauftragsbearbeiter und Dienstleister

Für alle Produkte

- Rechenzentrumsbetreiber in der Schweiz (Colocation, ISO/IEC 27001): Fläche, Strom, Kühlung, physische Sicherheit und Netzanbindung. Kein logischer Zugriff auf Systeme oder

Daten. Kein Unterauftragsbearbeiter im Sinne von Ziffer 9.5; Angaben auf Anfrage unter Vertraulichkeit.

Nur für DNS-Dienste

- DNS-Server an Standorten in Deutschland und Frankreich (Georedundanz). Gespeichert werden ausschliesslich DNS-Zonendaten.

Nur bei Bestellung des jeweiligen Produkts

- Domainnamen: die für die jeweilige Domainendung zuständigen Registrierungsstellen und Registrare (z. B. SWITCH für .ch und .li, DENIC für .de, nic.at für .at, ICANN-akkreditierte Registrare). Bearbeitet werden die Inhaberdaten der Domain.
- SSL-Zertifikate: die jeweilige Zertifizierungsstelle und deren Vertriebspartner. Bearbeitet werden die Antragsdaten des Zertifikats.
- Microsoft 365: Microsoft und der Distributor Pax8. Es gelten die Datenschutzbestimmungen von Microsoft.