Stänz Informatik AG
Tösstalstrasse 14 | 8360 Wallenwil
071 971 24 74 | support@sin.ch

Vereinbarung zur Auftragsbearbeitung (AVV)

nach dem Schweizer Datenschutzgesetz (nDSG)

zwischen der
Stänz Informatik AG, Tösstalstrasse 14, 8360 Wallenwil
(nachfolgend «Auftragnehmer»)

und dem Kunden (nachfolgend «Auftraggeber»)

1. Gegenstand und Anwendungsbereich

1. Diese Vereinbarung regelt die Rechte und Pflichten bei IT-Dienstleistungen (Support, Fernwartung, Netzwerk, Cloud-Services), bei denen der Auftragnehmer Zugriff auf Personendaten des Auftraggebers erhalten kann.
2. Sie ist integraler Bestandteil des Hauptvertrages bzw. der Offerte.
3. Der Umfang der Bearbeitung beschränkt sich auf technische Tätigkeiten zur Vertragserfüllung.

2. Verantwortlichkeiten & Risikoabgrenzung

1. Verantwortung des Auftraggebers: Der Auftraggeber ist alleiniger Verantwortlicher für die Rechtmässigkeit der Datenbearbeitung sowie für die Wahrung der Betroffenenrechte.
2. Backup-Pflicht: Die alleinige Verantwortung für die Datensicherung liegt beim Auftraggeber. Der Auftragnehmer haftet nicht für Datenverluste, die durch mangelhafte kundenseitige Sicherungen entstehen.
3. Datenqualität: Der Auftragnehmer prüft die Daten des Auftraggebers nicht auf inhaltliche Richtigkeit oder rechtliche Zulässigkeit.

3. Pflichten des Auftragnehmers

1. Weisungsbindung: Daten werden nur im Rahmen des Auftrags bearbeitet. Erscheint eine Weisung rechtswidrig, informiert der Auftragnehmer den Auftraggeber.
2. Vertraulichkeit: Alle Mitarbeiter sind zur Verschwiegenheit verpflichtet.
3. Sicherheit: Der Auftragnehmer setzt angemessene technisch-organisatorische Massnahmen (TOM) gemäss Anhang 1 um.
4. **Unterauftragsverhältnisse (Sub-Unternehmer)**

1. Der Auftraggeber erteilt die allgemeine Genehmigung zum Beizug spezialisierter Dritter (z. B. AnyDesk, Microsoft, Hostpoint, ALSO).
2. Der Auftragnehmer informiert über Änderungen (z. B. via Website oder E-Mail). Widerspricht der Auftraggeber nicht innerhalb von 14 Tagen, gilt die Änderung als genehmigt.
3. Ein Widerspruch kann zur Einstellung der entsprechenden Teilleistung führen, ohne dass Rückerstattungsansprüche entstehen.

5. Kontrollrechte und Unterstützung

1. Der Auftraggeber darf die Einhaltung einmal jährlich nach Voranmeldung (20 Tage) prüfen.
2. Für die Unterstützung bei Audits oder Auskunftsbegehren Dritter hat der Auftragnehmer einen Vergütungsanspruch nach Aufwand (aktueller Stundensatz), sofern kein grobfahrlässiges Fehlverhalten des Auftragnehmers vorliegt.

6. Haftungsbeschränkung

Die Haftung des Auftragnehmers richtet sich nach den AGB der Stänz Informatik AG. Jegliche Haftung für indirekte Schäden, Folgeschäden oder entgangenen Gewinn wird im gesetzlich zulässigen Mass ausgeschlossen.

7. Schlussbestimmungen

Es gilt ausschliesslich Schweizer Recht. Gerichtsstand ist der Sitz des Auftragnehmers (8360 Wallenwil).

Anhang 1: Technische und organisatorische Massnahmen (TOM)

Die Stänz Informatik AG setzt zum Schutz der Daten folgende Massnahmen um:

1. Vertraulichkeit (Schutz vor unbefugter Einsicht)
   - Zutritt: Geschäftsräume in Wallenwil sind durch mechanische Schliesssysteme gesichert.
   - Zugang: Einsatz individueller Benutzerkonten und starker Passwort-Richtlinien. Einsatz von Multi-Faktor-Authentifizierung (MFA), wo technisch möglich.
   - Zugriff: Berechtigungen nach dem „Need-to-know“-Prinzip.
   - Trennung: Daten verschiedener Kunden werden logisch strikt voneinander getrennt.
2. Integrität (Schutz vor Veränderung)
   - Übertragung: Fernwartung (AnyDesk) erfolgt über verschlüsselte Kanäle (TLS/AES). Nutzung gesicherter VPN-Tunnel oder HTTPS für Datenverkehr.
   - Eingabe: Protokollierung der Support-Zugriffe innerhalb der eingesetzten Fernwartungstools.
3. Verfügbarkeit und Belastbarkeit (Schutz vor Verlust)
   - Schutz: Einsatz professioneller Firewall- und Antiviren-Systeme (Endpoint Protection).
   - Wiederherstellung: Regelmässige Sicherung der vom Auftragnehmer verwalteten Datenbestände.
   - Wartung: Regelmässiges Einspielen von Sicherheits-Patches (Patch-Management) auf den Support-Systemen.
4. Verfahren zur Überprüfung
   - Regelmässige Sensibilisierung der Mitarbeiter für Datensicherheit.
   - Definierter Prozess zur Meldung von Sicherheitsvorfällen innerhalb von 72 Stunden an den Kunden.