Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO

Heina
Einzelunternehmerin Nathalie Heilmann
Lohkoppel 3, 23867 Sülfeld
(nachfolgend auch „Auftragnehmer")

Der vorliegende Auftragsverarbeitungsvertrag gilt für die Verarbeitungsmaßnahmen personenbezogener Daten durch den Auftragnehmer, die gegenüber Kunden (nachfolgend „Auftraggeber") in Erfüllung des Hauptvertrages erbracht werden.

Präambel

Der Auftragnehmer erbringt für den Auftraggeber Leistungen gemäß dem SaaS-Vertrag (im Folgenden: „Hauptvertrag"). Teil der Durchführung des Hauptvertrags ist die Verarbeitung von personenbezogenen Daten im Sinne der DSGVO. Zur Erfüllung der Anforderungen der DSGVO schließen die Parteien den nachfolgenden Auftragsverarbeitungsvertrag, der mit Wirksamwerden des Hauptvertrages zustande kommt.

§ 1 Gegenstand/Umfang der Beauftragung

1. Im Rahmen der Zusammenarbeit hat der Auftragnehmer Zugriff auf personenbezogene Daten des Auftraggebers („Auftraggeberdaten"). Diese verarbeitet der Auftragnehmer im Auftrag und nach Weisung des Auftraggebers i.S.v. Art. 4 Nr. 8 und Art. 28 DSGVO.

2. „Auftraggeberdaten" sind alle personenbezogenen Daten, die der Auftragnehmer im Rahmen der Leistungserbringung verarbeitet.

3. Die Verarbeitung erfolgt in der in den Anlagen beschriebenen Art und dem dort spezifizierten Umfang und Zweck.

4. Die Verarbeitung findet grundsätzlich in der EU/EWR statt.

5. Eine Verarbeitung in einem Drittland erfolgt nur mit vorheriger Zustimmung des Auftraggebers und unter Einhaltung der Art. 44–49 DSGVO.

§ 2 Weisungsbefugnisse des Auftraggebers

1. Der Auftragnehmer verarbeitet die Daten im Auftrag und nach Weisung des Auftraggebers. Der Auftraggeber hat das alleinige Weisungsrecht.

2. Weisungen werden grundsätzlich schriftlich oder in elektronischer Form erteilt.

3. Bei Verstoß einer Weisung gegen Datenschutzrecht hat der Auftragnehmer den Auftraggeber darauf hinzuweisen.

§ 3 Schutzmaßnahmen

1. Der Auftragnehmer beachtet die gesetzlichen Datenschutzbestimmungen und gibt Informationen nicht an Dritte weiter.

2. Alle mit der Verarbeitung betrauten Personen werden zur Vertraulichkeit verpflichtet (Art. 28 Abs. 3 lit. b DSGVO).

3. Der Auftragnehmer ergreift geeignete technische und organisatorische Maßnahmen gem. Art. 32 DSGVO.

§ 4 Informations- und Unterstützungspflichten

1. Bei Störungen oder Verdacht auf Datenschutzverletzungen informiert der Auftragnehmer unverzüglich (in der Regel binnen 24 Stunden).

§ 5 Subunternehmerverhältnisse

1. Der Auftragnehmer darf Unterauftragnehmer einsetzen.

2. Die in Anlage 1 genannten Unternehmen sind genehmigt.

3. Neue Unterauftragnehmer werden 4 Wochen vorab angekündigt.

§ 6 Kontrollrechte

1. Der Auftraggeber ist berechtigt, die Einhaltung zu überprüfen. Überprüfungen erfolgen vorrangig als Remote-Audit.

§ 7 Rechte Betroffener

1. Der Auftragnehmer unterstützt bei der Erfüllung der Pflichten nach Art. 12–22 und Art. 32–36 DSGVO.

§ 8 Laufzeit und Kündigung

1. Die Laufzeit entspricht der Laufzeit des Hauptvertrags.

§ 9 Löschung und Rückgabe nach Vertragsende

1. Nach Beendigung werden alle Daten zurückgegeben oder gelöscht. Eine Löschbestätigung wird in Textform ausgestellt.

§ 10 Haftung

1. Die Haftung richtet sich nach Art. 82 DSGVO.

§ 11 Vertraulichkeit & Datengeheimnis

1. Es besteht eine umfassende Verschwiegenheitspflicht, die auch nach Vertragsende fortbesteht.

§ 12 Schlussbestimmungen

1. Die Regelungen dieses Vertrags gehen im Zweifel denen des Hauptvertrags vor.

2. Diese Vereinbarung unterliegt deutschem Recht. Gerichtsstand ist der Sitz des Auftragnehmers.

Anlage 1 — Festlegungen zum Vertrag

Hauptvertrag	SaaS-Vertrag
Gegenstand	All-in-one Handwerkersoftware für Betriebe
Zweck	Erfüllung der Pflichten aus dem Hauptvertrag
Art der Daten	Stamm-, Kontakt-, Inhalts-, Vertrags-, Zahlungs-, Nutzungs-, Verbindungs-, Standortdaten
Betroffene	Beschäftigte, Kunden, Lieferanten, Geschäftspartner, Berater

Unterauftragnehmer

Nr.	Unterauftragnehmer	Leistung	Ort	Transfer
1	Abacus.AI, Inc. — San Francisco, USA	Hosting, DB, KI	USA (AWS/GCP)	SCC 2021/914
2	Stripe Payments Europe, Ltd. — Dublin, IE	Zahlungsabwicklung	EU	DPF
3	Expo — San Francisco, USA	Push-Benachrichtigungen	USA (GCP)	DPF

Anlage 2 — Technische und organisatorische Maßnahmen

1. Organisation der Informationssicherheit

2. Privacy by Design & Default
3. Zugriffskontrolle und Zugangskontrolle
4. Kryptographie und Pseudonymisierung
5. Schutz von Gebäuden und Betriebsmitteln
6. Betriebsverfahren und Zuständigkeiten
7. Datensicherungen
8. Schutz vor Malware und Patchmanagement
9. Protokollierung und Überwachung
10. Netzwerksicherheit
11. Informationsübertragung
12. Netztrennung
13. Lieferantenbeziehungen
14. Informationssicherheitsvorfälle
15. Business Continuity / Notfallmanagement
16. Einhaltung gesetzlicher Anforderungen
17. Datenschutzanforderungen und -management
18. Informationssicherheitsüberprüfungen

Stand: Juni 2026
Mit freundlicher Unterstützung vom Startup-Anwalt Nils Bremann (derstartupanwalt.de)