

Auftragsverarbeitungsvertrag (AVV)

nach Art. 28 DSGVO

Vertragsparteien

zwischen

dem jeweiligen Vertragspartner, der diesen Vertrag entweder durch elektronische Bestätigung (Klick) oder durch schriftliche Bestätigung per E-Mail akzeptiert (im Folgenden: „**Auftraggeber**“)

und

Stampz

Adam Daghbouche

Georgstraße 11 30159 Hannover Deutschland E-Mail:

info@stampz.io

(im Folgenden: „**Auftragsverarbeiter**“)

§ 1 Gegenstand und Dauer der Verarbeitung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Auftraggebers im Rahmen der Bereitstellung und des Betriebs der Plattform „stampz.io“ zur Erstellung und Verwaltung digitaler Stempelkarten, Treueprogramme und Push-Benachrichtigungen über Apple Wallet.

Die Verarbeitung beginnt mit Vertragsbeginn (Registrierung auf der Plattform) und endet mit dessen Beendigung sowie spätestens mit der vollständigen Löschung der personenbezogenen Daten, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

§ 2 Art und Zweck der Verarbeitung

Die Verarbeitung personenbezogener Daten erfolgt zu folgenden Zwecken:

- Hosting und Speicherung von personenbezogenen Daten
 - Verwaltung von Endkundendaten (z. B. Name, E-Mail-Adresse)
 - Erstellung und Verwaltung digitaler Stempelkarten
 - Erfassung und Verwaltung von Stempeln/Punkten
 - Versand von Push-Benachrichtigungen über Apple Wallet
 - API-Übermittlung an Apple Wallet (PassKit)
 - Standortbasierte Benachrichtigungen (sofern aktiviert)
 - Bereitstellung von Statistiken und Analysen für den Auftraggeber
 - Sicherstellung der Stabilität und Sicherheit der Plattform
-

§ 3 Kategorien betroffener Personen

- Endkund:innen des Auftraggebers (Inhaber:innen der digitalen Stempelkarten)
 - Mitarbeiter:innen des Auftraggebers, falls im Rahmen der Nutzung erfasst
-

§ 4 Kategorien verarbeiteter Daten

- Vorname und/oder Name
 - E-Mail-Adresse
 - Seriennummer der digitalen Karte (Wallet-Pass-ID)
 - Geräte-Identifikator (Device Library Identifier)
 - Push-Token für Apple Wallet Benachrichtigungen
 - Stempel-/Punktestand und Transaktionsdaten
 - Zeitstempel der Kartennutzung
 - Marketing-Einwilligung (Opt-in/Opt-out Status)
 - Nutzungsstatistiken (z. B. eingelöste Prämien)
-

§ 5 Rechte und Pflichten des Auftraggebers

Der Auftraggeber erhält über die Plattform von Stampz Zugriff auf personenbezogene Daten von Endnutzer:innen, die diese bei der

Erstellung ihrer digitalen Stempelkarte über die Stampz-Plattform selbst angeben.

Der Auftraggeber verpflichtet sich, diese Daten ausschließlich zu den vertraglich vorgesehenen und rechtlich zulässigen Zwecken zu verwenden, sie vertraulich zu behandeln und durch geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO gegen unbefugten Zugriff, Verlust, Veränderung oder Weitergabe zu schützen.

Der Auftraggeber ist für die datenschutzkonforme Nutzung der übermittelten personenbezogenen Daten verantwortlich. Dies umfasst insbesondere:

- Die Kontrolle der internen Zugriffe auf die Daten
- Die Dokumentation der internen Datenverarbeitungsvorgänge
- Die Schulung und Sensibilisierung seiner Mitarbeitenden im Umgang mit personenbezogenen Daten
- Die Einholung erforderlicher Einwilligungen für Marketing-Benachrichtigungen

Stampz übernimmt keine Verantwortung für Datenschutzverstöße, unrechtmäßige Verarbeitung oder Weitergabe personenbezogener Daten durch den Auftraggeber oder durch Dritte, die außerhalb des Einflussbereichs von Stampz handeln.

Der Auftraggeber stellt Stampz von sämtlichen Ansprüchen Dritter frei, die aufgrund einer Pflichtverletzung des Auftraggebers im Zusammenhang mit dem Umgang mit personenbezogenen Daten entstehen – insbesondere bei Verstößen gegen Datenschutzvorgaben nach der DSGVO oder anderen anwendbaren Rechtsvorschriften.

§ 6 Pflichten des Auftragsverarbeiters

Die Verarbeitung personenbezogener Daten erfolgt grundsätzlich auf Weisung des Auftraggebers, soweit keine anderweitige gesetzliche Verpflichtung besteht.

Der Auftragsverarbeiter verpflichtet sich zu folgenden Maßnahmen:

- Vertraulichkeitsverpflichtung aller Mitarbeitenden, die Zugang zu personenbezogenen Daten haben

- Implementierung angemessener technischer und organisatorischer Maßnahmen (TOMs) gemäß Art. 32 DSGVO
- TLS-Verschlüsselung für alle Datenübertragungen
- Verschlüsselte Speicherung sensibler Daten
- Zugangsbeschränkungen und Berechtigungskonzepte
- Regelmäßige Datensicherungen
- Unterstützung des Auftraggebers bei der Erfüllung von Betroffenenrechten (Art. 15-22 DSGVO)

Sicherheitsvorfälle mit Bezug auf personenbezogene Daten werden dem Auftraggeber unverzüglich, spätestens jedoch innerhalb von 48 Stunden nach Kenntnisnahme gemeldet. Eine Bewertung, ob eine Meldepflicht gegenüber Aufsichtsbehörden oder betroffenen Personen besteht, obliegt dem Auftraggeber.

Nach Vertragsende löscht der Auftragsverarbeiter alle personenbezogenen Daten innerhalb von 30 Tagen, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

§ 7 Technische und organisatorische Maßnahmen (TOMs)

Der Auftragsverarbeiter hat folgende Maßnahmen implementiert:

Maßnahme	Beschreibung
Zutrittskontrolle	Cloud-basierte Infrastruktur mit physischer Sicherheit durch den Hosting-Anbieter
Zugangskontrolle	Authentifizierung mittels sicherer Passwörter, Session-Management
Zugriffskontrolle	Rollenbasiertes Berechtigungskonzept, Mandantentrennung
Weitergabekontrolle	TLS 1.3 Verschlüsselung für alle Übertragungen
Eingabekontrolle	Protokollierung von Datenänderungen mit Zeitstempeln
Auftragskontrolle	

Maßnahme	Beschreibung
	Verarbeitung nur nach dokumentierter Weisung
Verfügbarkeitskontrolle	Regelmäßige Backups, Redundanz, Notfallkonzept
Trennungsgebot	Logische Trennung der Kundendaten durch separate Datenbankeinträge

§ 8 Subunternehmer (Unterauftragsverarbeiter)

Der Auftragsverarbeiter kann zur Erbringung seiner Leistungen Subunternehmer einsetzen, sofern diese durch geeignete vertragliche Regelungen zur Einhaltung der datenschutzrechtlichen Vorgaben verpflichtet sind.

Der Auftraggeber wird über wesentliche Änderungen in der Subunternehmerliste per E-Mail informiert und kann dem Einsatz aus berechtigten datenschutzrechtlichen Gründen innerhalb von 14 Tagen widersprechen.

Aktuelle Unterauftragsverarbeiter:

Unternehmen	Standort	Zweck
Supabase Inc.	Singapur / USA	Datenbank-Hosting, Authentifizierung
Railway Corporation	San Francisco, USA	Application Hosting
Stripe, Inc.	San Francisco, USA	Zahlungsabwicklung
Upstash, Inc.	San Francisco, USA	Redis-Hosting (Rate Limiting)
Apple Inc.	Cupertino, USA	Apple Wallet / PassKit / APNs Push-Benachrichtigungen

Mit allen US-amerikanischen Unterauftragsverarbeitern bestehen Standardvertragsklauseln (SCCs) gemäß Art. 46 Abs. 2 lit. c DSGVO oder sie sind unter dem EU-US Data Privacy Framework zertifiziert.

§ 9 Kontrolle und Nachweispflichten

Der Auftraggeber ist berechtigt, sich im zumutbaren Umfang über die Einhaltung der vereinbarten Datenschutzpflichten durch den Auftragsverarbeiter zu informieren.

Der Auftragsverarbeiter stellt auf Anfrage geeignete Nachweise zur Verfügung, etwa:

- Technische Dokumentationen
- Aktuelle Liste der Unterauftragsverarbeiter
- Bestätigung über implementierte TOMs

Vor-Ort-Prüfungen sind nach vorheriger Abstimmung und unter Wahrung angemessener Vertraulichkeit möglich, wobei der Auftraggeber die Kosten trägt.

§ 10 Haftung

Die Haftung richtet sich nach den gesetzlichen Bestimmungen der DSGVO, insbesondere Art. 82 DSGVO.

Im Innenverhältnis haftet jede Partei für Schäden, die durch von ihr zu vertretende Verstöße gegen diesen Vertrag oder gegen datenschutzrechtliche Vorschriften entstanden sind.

§ 11 Schlussbestimmungen

- Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform (E-Mail ist ausreichend).
- Es gilt deutsches Recht unter Ausschluss des UN-Kaufrechts.
- Gerichtsstand für alle Streitigkeiten aus diesem Vertrag ist Hannover, soweit gesetzlich zulässig.

- Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.
 - Dieser AVV tritt mit Abschluss des Hauptvertrags (Nutzung der Stampz-Plattform) in Kraft und endet mit dessen Beendigung.
-

§ 12 Vertragsannahme

Der Auftraggeber bestätigt durch elektronische Zustimmung bei der Registrierung auf stampz.io, dass er diesen Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO sowie die Allgemeinen Geschäftsbedingungen des Auftragsverarbeiters gelesen, verstanden und akzeptiert hat.

Die elektronische Zustimmung ersetzt die handschriftliche Unterschrift und gilt als rechtsverbindliche Annahme des Vertrags.

Eine Kopie dieses AVV kann jederzeit unter stampz.io/avv eingesehen und heruntergeladen werden.

Stand: März 2026

Kontakt für Datenschutzanfragen:

datenschutz@stampz.io

Stampz – Digitale Stempelkarten direkt im Wallet