ART. 28 DSGVO

Auftragsverarbeitungsvertrag (AVV)

swipesign GmbH · Fassung vom 18. November 2026

Dieser Auftragsverarbeitungsvertrag („AVV“) regelt, wie swipesign personenbezogene Daten im Auftrag seiner Kunden nach Art. 28 der Verordnung (EU) 2016/679 („DSGVO“) verarbeitet. Begriffe, die in den Allgemeinen Geschäftsbedingungen („AGB“) definiert sind, etwa Kunde, Konto, Benutzer, Unterzeichner, Empfänger, Dokument und Dienste, haben in diesem AVV dieselbe Bedeutung.

---

1. Parteien und Geltungsbereich

1.1 Dieser AVV wird zwischen der swipesign GmbH, Elisabethstraße 15, Top 5A, 1010 Wien, Österreich, FN 664099 t, Handelsgericht Wien („swipesign“, „wir“) als Auftragsverarbeiter und dem Kunden („Kunde“, „Sie“) als Verantwortlichem geschlossen.

1.2 Dieser AVV gilt für die swipesign-Plattform unter app.swipesign.io und die nach den AGB erbrachten Dienste. Er gilt nicht für andere Produkte von swipesign.

1.3 Dieser AVV ist nach Abschnitt 18.1 der AGB Bestandteil des Vertrags. Er gilt ohne gesonderte Unterzeichnung. Ein gegengezeichnetes Exemplar ist auf Anfrage über support@swipesign.io erhältlich.

1.4 Weichen dieser AVV und die AGB in einer Frage personenbezogener Daten voneinander ab, geht dieser AVV vor.

2. Rollen

2.1 Als Auftragsverarbeiter verarbeiten wir die personenbezogenen Daten von Unterzeichnern, Empfängern, Adressbuchkontakten und Benutzern, die wir zur Erbringung der Dienste im Auftrag des Kunden verarbeiten („Kundendaten“).

2.2 Für Kontodaten, Abrechnungsdaten sowie die Signaturnachweise und den Audit-Trail nach den Abschnitten 5.5 und 18.2 der AGB sind wir selbst Verantwortlicher, weil wir diese Nachweise unabhängig von Weisungen des Kunden aufbewahren müssen, um die Gültigkeit von Signaturen nachzuweisen. Diese Daten fallen nicht unter diesen AVV. Wie wir sie verarbeiten, beschreibt die Datenschutzerklärung.

2.3 Der Kunde ist für die Rechtmäßigkeit der von ihm beauftragten Verarbeitung verantwortlich, einschließlich ihrer Rechtsgrundlage und der Information der betroffenen Personen (Abschnitt 6.1 der AGB).

---

3. Gegenstand, Dauer, Art und Zweck

3.1 Gegenstand, Art und Zweck der Verarbeitung, die Arten personenbezogener Daten und die Kategorien betroffener Personen ergeben sich aus Anlage 1.

3.2 Die Verarbeitung dauert für die Laufzeit des Vertrags und nach seinem Ende, bis die Kundendaten nach Abschnitt 12 gelöscht sind.

---

4. Weisungen

4.1 Wir verarbeiten Kundendaten nur auf dokumentierte Weisung des Kunden, auch in Bezug auf die Übermittlung an ein Drittland oder eine internationale Organisation.

4.2 Der Vertrag, dieser AVV und die Nutzung und Konfiguration der Dienste durch den Kunden sind die dokumentierten Weisungen des Kunden.

4.3 Wir informieren den Kunden unverzüglich, wenn wir der Auffassung sind, dass eine Weisung gegen die DSGVO oder andere Datenschutzbestimmungen der Europäischen Union oder eines Mitgliedstaats verstößt.

4.4 Sind wir nach dem Recht der Europäischen Union oder eines Mitgliedstaats, dem wir unterliegen, zur Verarbeitung von Kundendaten verpflichtet, teilen wir dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

---

5. Vertraulichkeit

5.1 Wir gewährleisten, dass sich die zur Verarbeitung der Kundendaten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen, einschließlich des Datengeheimnisses nach § 6 Datenschutzgesetz (DSG).

5.2 Zugriff auf Kundendaten haben nur Personen, die ihn zur Erbringung, Absicherung oder Unterstützung der Dienste benötigen.

---

6. Sicherheit

6.1 Wir treffen die in Anlage 2 beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO.

6.2 Wir können diese Maßnahmen dem technischen Fortschritt anpassen, sofern das Schutzniveau nicht unter das in Anlage 2 beschriebene sinkt.

---

7. Sub-Auftragsverarbeiter

7.1 Der Kunde erteilt uns die allgemeine schriftliche Genehmigung, die in Anlage 3 genannten Sub-Auftragsverarbeiter in Anspruch zu nehmen.

7.2 Wir erlegen jedem Sub-Auftragsverarbeiter vertraglich dieselben Datenschutzpflichten auf, die in diesem AVV festgelegt sind, insbesondere hinreichende Garantien dafür, dass geeignete technische und organisatorische Maßnahmen durchgeführt werden.

7.3 Wir haften gegenüber dem Kunden für die Einhaltung der Pflichten jedes Sub-Auftragsverarbeiters.

7.4 Jede beabsichtigte Hinzuziehung oder Ersetzung eines Sub-Auftragsverarbeiters teilen wir dem Kunden mindestens 30 Tage vor ihrem

Wirksamwerden per E-Mail an die Konto-E-Mail-Adresse mit.

7.5 Der Kunde kann der Änderung innerhalb dieser Frist aus berechtigten datenschutzrechtlichen Gründen schriftlich widersprechen. Die Parteien suchen dann nach Treu und Glauben eine Lösung. Wird keine Lösung gefunden, kann der Kunde die betroffenen Dienste mit Wirkung zum Wirksamwerden der Änderung kündigen, und wir erstatten vorausbezahlte Entgelte für den Zeitraum nach der Kündigung anteilig.

7.6 Die aktuelle Liste der Sub-Auftragsverarbeiter ist jederzeit in Anlage 3 dieses AVV unter swipesign.io/de/avv abrufbar.

---

8. Übermittlung in Drittländer

8.1 Wir verarbeiten Kundendaten grundsätzlich in der Europäischen Union oder im Europäischen Wirtschaftsraum.

8.2 Kundendaten übermitteln wir an ein Drittland oder eine internationale Organisation nur, wenn die Voraussetzungen von Kapitel V DSGVO erfüllt sind, nämlich auf Grundlage eines Angemessenheitsbeschlusses der Europäischen Kommission, einschließlich des EU-US Data Privacy Framework für zertifizierte Empfänger, oder der von der Europäischen Kommission erlassenen Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO).

8.3 Die betroffenen Sub-Auftragsverarbeiter sind in Anlage 3 gekennzeichnet.

---

9. Anträge betroffener Personen

9.1 Richtet eine betroffene Person einen Antrag zu Kundendaten an uns, leiten wir ihn unverzüglich an den Kunden weiter.

9.2 Wir unterstützen den Kunden nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen auf Wahrnehmung der Rechte betroffener Personen nach Kapitel III DSGVO. Über das Konto kann der Kunde Kundendaten selbst einsehen, berichtigen, exportieren und löschen.

10. Unterstützung

10.1 Unter Berücksichtigung der Art der Verarbeitung und der uns zur Verfügung stehenden Informationen unterstützen wir den Kunden bei der Einhaltung seiner Pflichten nach Art. 32 bis 36 DSGVO: Sicherheit der Verarbeitung, Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und Benachrichtigung der betroffenen Personen, Datenschutz-Folgenabschätzung und vorherige Konsultation der Aufsichtsbehörde.

---

11. Verletzungen des Schutzes personenbezogener Daten

11.1 Wir melden dem Kunden eine Verletzung des Schutzes personenbezogener Daten, die Kundendaten betrifft, unverzüglich, nachdem sie uns bekannt geworden ist.

11.2 Die Meldung enthält, soweit verfügbar, die Informationen nach Art. 33 Abs. 3 DSGVO: die Art der Verletzung, soweit möglich mit den Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze; eine Anlaufstelle für weitere Informationen; die wahrscheinlichen Folgen der Verletzung; und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

11.3 Können nicht alle Informationen zur gleichen Zeit bereitgestellt werden, stellen wir sie ohne unangemessene weitere Verzögerung schrittweise zur Verfügung.

---

12. Löschung und Rückgabe

12.1 Dokumente und alle Zwischenversionen löschen wir 14 Tage nachdem ein Vorgang abgeschlossen oder abgebrochen wurde oder abgelaufen ist endgültig (Abschnitt 7.2 der AGB). Temporäre Dateien aus Konvertierungen werden innerhalb von Stunden gelöscht.

12.2 Hat der Kunde das Langzeitarchiv bestellt, bleiben archivierte Dokumente für die Dauer des Zusatzmoduls gespeichert. Nach Ende des Zusatzmoduls bleiben sie 30 Tage lang zum Export verfügbar und werden danach gelöscht (Abschnitt 7.4 der AGB).

12.3 Vorlagen, Adressbucheinträge, Entwürfe und nicht versendete Dokumente bleiben im Konto, bis der Kunde sie löscht oder das Konto endet (Abschnitt 7.5 der AGB).

12.4 Der Kunde kann seine Dokumente, Audit-Trails und Nachweise während der Vertragslaufzeit und 30 Tage nach ihrem Ende jederzeit aus dem Konto exportieren (Abschnitt 7.6 der AGB). Dieser Export ist die Rückgabe der Kundendaten. Nach Ablauf dieser Frist löschen wir die verbleibenden Kundendaten.

12.5 Die Abschnitte 12.1 bis 12.4 gelten nicht für Daten, die wir nach dem Recht der Europäischen Union oder eines Mitgliedstaats aufbewahren müssen, und nicht für die Signaturnachweise und den Audit-Trail, die wir als Verantwortlicher führen (Abschnitt 2.2).

12.6 Gelöschte Daten werden aus Backups entfernt, wenn die Backups in ihrem regulären Zyklus überschrieben werden.

---

13. Prüfungen und Informationen

13.1 Wir stellen dem Kunden die Informationen zur Verfügung, die zum Nachweis der Einhaltung von Art. 28 DSGVO und dieses AVV erforderlich sind.

13.2 Wir ermöglichen Überprüfungen, einschließlich Inspektionen, durch den Kunden oder einen von ihm beauftragten Prüfer und tragen dazu bei. Prüfungen werden zunächst durch Dokumentation und schriftliche Antworten auf die Fragen des Kunden erfüllt.

13.3 Reichen Dokumentation und schriftliche Antworten nicht aus, kann der Kunde eine Vor-Ort-Prüfung selbst oder durch einen unabhängigen, zur Verschwiegenheit verpflichteten Prüfer durchführen. Eine Vor-Ort-Prüfung kann höchstens einmal je Vertragsjahr stattfinden, nach einer Verletzung des Schutzes personenbezogener Daten oder auf Verlangen einer Aufsichtsbehörde auch öfter. Der Kunde kündigt sie mindestens 30 Tage im Voraus schriftlich an. Die Prüfung findet während der Geschäftszeiten statt, ohne unseren Betrieb zu stören und ohne Zugriff auf Daten anderer Kunden. Der Kunde trägt seine eigenen Kosten und die seines Prüfers.

14. Haftung

14.1 Die Haftung nach diesem AVV richtet sich nach Abschnitt 16 der AGB.

14.2 Dieser AVV schränkt weder die Rechte betroffener Personen noch die Haftung gegenüber betroffenen Personen nach Art. 82 DSGVO ein.

---

15. Schlussbestimmungen

15.1 Dieser AVV gilt für die Laufzeit des Vertrags und nach seinem Ende, solange wir Kundendaten verarbeiten.

15.2 Änderungen dieses AVV erfolgen nach Abschnitt 21 der AGB.

15.3 Dieser AVV unterliegt österreichischem Recht. Der Gerichtsstand richtet sich nach Abschnitt 22 der AGB.

15.4 Dieser AVV liegt in englischer und deutscher Sprache vor. Maßgeblich ist die englische Fassung (Abschnitt 22.3 der AGB).

Anlagen

Anlage 1: Angaben zur Verarbeitung

Gegenstand und Art

Wir hosten, speichern, verarbeiten, übermitteln, zeigen an, konvertieren und löschen Kundendaten, um die Dienste zu erbringen.

Zwecke

Vorbereiten, Versenden, Unterzeichnen, Zustellen und Speichern von Dokumenten;

Identitätsprüfung von Unterzeichnern und Empfängern, wenn eine verifizierte Signatur oder eine verifizierte Übermittlung gewählt wird;

sichere Übermittlung von Dokumenten an Empfänger (eDelivery, in der Plattform als Safe Transfer bezeichnet);

das Adressbuch des Kunden;

Dokumentwerkzeuge, einschließlich Konvertierung, Felderkennung und Zusammenfassungen durch KI, die auf unserer eigenen Infrastruktur läuft.

Betroffene Personen

Unterzeichner;

Empfänger;

Prüfer, die der Kunde um Freigabe eines Dokuments ersucht;

Adressbuchkontakte;

die Benutzer des Kunden.

Arten personenbezogener Daten

Name, E-Mail-Adresse und Mobilnummer;

IP-Adresse sowie Browser- und Gerätedaten (User-Agent);

Signatur-, Prüf- und Zugriffshandlungen und deren Zeitpunkte, einschließlich der Zustimmung zu den Bedingungen bei Safe Transfer;

Methode und Ergebnis der Identitätsprüfung, die vom Anbieter übermittelten Identitätsdaten und bei der Videoidentifikation zusätzlich Geburtsdatum, Geschlecht und Postanschrift;

der Inhalt von Dokumenten und von über Safe Transfer versendeten Dateien. Diese können nach Festlegung des Kunden jede Art personenbezogener Daten enthalten, einschließlich besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO.

Dauer und Speicherfristen

Dokumente: Löschung 14 Tage nachdem ein Vorgang abgeschlossen oder abgebrochen wurde oder abgelaufen ist; mit dem Langzeitarchiv für die Dauer des Zusatzmoduls und 30 Tage nach dessen Ende.

Temporäre Dateien aus Konvertierungen: Löschung innerhalb von Stunden.

Safe-Transfer-Links: laufen nach 14 Tagen ab oder früher, wenn der Kunde sie zurückzieht.

Vorlagen, Adressbucheinträge, Entwürfe und nicht versendete Dokumente: bis der Kunde sie löscht oder das Konto endet.

Nach Vertragsende: 30 Tage zum Export verfügbar, danach Löschung (Abschnitt 12.4).

Signaturnachweise und Audit-Trail: von uns als Verantwortlichem mindestens sieben Jahre aufbewahrt, außerhalb dieses AVV.

Anlage 2: Technische und organisatorische Maßnahmen

Zugriffskontrolle

Administrative Schnittstellen (die Cluster-API, die Quellcode-Plattform und interne Verwaltungswerkzeuge) sind nur über unser Unternehmens-VPN erreichbar.

Zugriff auf Kundendaten haben nur Mitarbeiter, die ihn benötigen.

Für Konten steht eine Zwei-Faktor-Authentifizierung zur Verfügung.

Registrierung, Anmeldung, SMS und Identitätsprüfungen unterliegen Ratenbegrenzungen. Wiederholte fehlgeschlagene Anmeldungen führen zu einer vorübergehenden Kontosperre.

Verschlüsselung

Alle Verbindungen sind mit TLS verschlüsselt.

Gespeicherte Daten sind verschlüsselt (Encryption at Rest).

Safe-Transfer-Dateien sind mit AES-GCM verschlüsselt.

Netzwerk und Trennung

Die Plattform läuft auf einem dedizierten Kubernetes-Cluster, den OVH in der EU hostet. Die Rechenzentren von OVH sind nach ISO 27001 zertifiziert; die Zertifizierung ist jene von OVH.

Netzwerkrichtlinien verbieten standardmäßig den Datenverkehr zwischen Workloads und lassen nur das Nötige zu.

Jeder Speicher-Bucket hat einen eigenen Speicher-Zugriffsschlüssel.

Die Daten jedes Kunden sind logisch nach Konto getrennt.

Dokumenten-KI, Dateikonvertierung und die Länderermittlung aus der IP-Adresse laufen auf unserer eigenen Infrastruktur, ohne externen Anbieter.

Missbräuchliche IP-Adressen werden automatisch gesperrt.

Protokollierung und Überwachung

Logs werden zentral erfasst und mit Alarmierung überwacht.

Signaturhandlungen werden in einem Audit-Trail aufgezeichnet, der mit qualifizierten Zeitstempeln versiegelt wird.

Verfügbarkeit, Backup und Löschung

Datenbanken werden regelmäßig gesichert. Die Backups werden in der EU gespeichert, und ihre Wiederherstellung wird getestet.

Dokumente werden 14 Tage nach Ende eines Vorgangs gelöscht. Temporäre Dateien aus Konvertierungen werden innerhalb von Stunden gelöscht.

Umgang mit Vorfällen

Verletzungen des Schutzes personenbezogener Daten werden nach Abschnitt 11 behandelt und dem Kunden gemeldet.

Mitarbeiter

Mitarbeiter sind zur Vertraulichkeit verpflichtet, und der Zugriff folgt dem Need-to-know-Prinzip.

Dienstleister

Sub-Auftragsverarbeiter werden nach Abschnitt 7 in Anspruch genommen und vertraglich verpflichtet.

Anlage 3: Sub-Auftragsverarbeiter

OVH SAS, 2 rue Kellermann, 59100 Roubaix, Frankreich. Zweck: Hosting, Datenbank, Speicher. Daten: alle Kundendaten. Ort: EU (Frankreich, Deutschland).

Sendinblue GmbH (Brevo), Köpenicker Straße 126, 10179 Berlin, Deutschland. Zweck: transaktionale E-Mails an Unterzeichner, Empfänger und Benutzer. Daten: E-Mail-Adresse, Name, Inhalt der Nachricht. Ort: Deutschland.

Twilio Ireland Ltd, 3 Dublin Landings, Dublin 1, Irland. Zweck: SMS-Bestätigungscodes. Daten: Mobilnummer, Code. Ort: Irland; Muttergesellschaft Twilio Inc., USA. Grundlage der Übermittlung: Standardvertragsklauseln und EU-US Data Privacy Framework.

Functional Software Inc. (Sentry), San Francisco, USA. Zweck: Fehlerüberwachung. Daten: technische Fehlerdaten (Fehlermeldungen, Stacktraces, Browser- und Geräteinformationen, Benutzer-ID), die beiläufig weitere personenbezogene Daten enthalten können. Ort: gespeichert in der EU Region von Sentry (Frankfurt, Deutschland); Unternehmen in den USA. Grundlage der Übermittlung: Standardvertragsklauseln und EU-US Data Privacy Framework.

eID Easy OÜ, Tallinn, Estland. Zweck: Aggregation elektronischer Identitäten und Signaturen. Daten: Identitätsdaten von Unterzeichnern. Ort: Estland.

WebID Solutions GmbH, Friedrichstraße 88, 10117 Berlin, Deutschland. Zweck: Videoidentifikation von Unterzeichnern und Empfängern. Daten: Identitätsdaten und Ergebnis der Identifikation. Ort: Deutschland.

Qualifizierte Vertrauensdiensteanbieter und Identitätsanbieter, die ein Unterzeichner nutzt, handeln nach ihren eigenen gesetzlichen Pflichten und Bedingungen als eigenständige Verantwortliche und sind keine Sub-Auftragsverarbeiter. Dazu gehören die A-Trust GmbH für qualifizierte Zertifikate und qualifizierte Zeitstempel sowie ID Austria, die staatliche elektronische Identität Österreichs.

Dienstleister, die wir als Verantwortlicher für eigene Zwecke einsetzen, etwa für Zahlungen, Webanalyse und Support, sind in der Datenschutzerklärung angeführt.