ART. 28 GDPR

Data processing agreement

swipesign GmbH · Version 18 November 2026

This Data Processing Agreement (“DPA”) sets out how swipesign processes personal data on behalf of its Customers under Art. 28 of Regulation (EU) 2016/679 (“GDPR”). Terms defined in the Terms and Conditions (“Terms”), such as Customer, Account, User, Signer, Recipient, Document and Services, have the same meaning in this DPA.

---

1. Parties and scope

1.1 This DPA is concluded between swipesign GmbH, Elisabethstraße 15, Top 5A, 1010 Vienna, Austria, company register FN 664099 t, Commercial Court of Vienna (“swipesign”, “we”), as processor, and the Customer (“Customer”, “you”), as controller.

1.2 This DPA applies to the swipesign platform at app.swipesign.io and the Services provided under the Terms. It does not apply to other products of swipesign.

1.3 This DPA forms part of the contract under section 18.1 of the Terms. It applies without separate signature. A countersigned copy is available on request from support@swipesign.io.

1.4 Where this DPA and the Terms differ on a matter of personal data, this DPA prevails.

---

2. Roles

2.1 We process as processor the personal data of Signers, Recipients, address-book contacts and Users that we process on the Customer's behalf to provide the Services (“Customer Personal Data”).

2.2 We are ourselves the controller for Account data, billing data and the signature evidence and audit trail under sections 5.5 and 18.2 of the Terms, because we must retain this evidence to prove the validity of signatures regardless of the Customer's instructions. This data is outside this DPA. The Privacy Policy describes how we process it.

2.3 The Customer is responsible for the lawfulness of the processing it instructs, including its legal basis and the information of data subjects (section 6.1 of the Terms).

---

3. Subject matter, duration, nature and purpose

3.1 The subject matter, nature and purpose of the processing, the types of personal data and the categories of data subjects are set out in Annex 1.

3.2 The processing lasts for the term of the contract and, after it ends, until Customer Personal Data has been deleted under section 12.

---

4. Instructions

4.1 We process Customer Personal Data only on documented instructions from the Customer, including with regard to transfers to a third country or an international organisation.

4.2 The contract, this DPA and the Customer's use and configuration of the Services are the Customer's documented instructions.

4.3 We inform the Customer without undue delay if we believe that an instruction infringes the GDPR or other data protection law of the European Union or a Member State.

4.4 Where the law of the European Union or a Member State to which we are subject requires us to process Customer Personal Data, we inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

5. Confidentiality

5.1 We ensure that persons authorised to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, including data secrecy under § 6 of the Austrian Data Protection Act (DSG).

5.2 Access to Customer Personal Data is limited to persons who need it to provide, secure or support the Services.

---

6. Security

6.1 We implement the technical and organisational measures under Art. 32 GDPR described in Annex 2.

6.2 We may update these measures as technology develops, provided the level of protection does not fall below that described in Annex 2.

---

7. Sub-processors

7.1 The Customer gives us general written authorisation to engage the sub-processors listed in Annex 3.

7.2 We impose on each sub-processor by contract the same data protection obligations as set out in this DPA, in particular sufficient guarantees to implement appropriate technical and organisational measures.

7.3 We remain liable to the Customer for the performance of each sub-processor's obligations.

7.4 We notify the Customer of any intended addition or replacement of a sub-processor by email to the Account email address at least 30 days before the change takes effect.

7.5 The Customer may object to the change in writing within that period on reasonable grounds relating to data protection. The parties then seek a solution in good faith. If no solution is found, the Customer may terminate the affected Services with effect from the date the change takes effect, and we refund prepaid fees for the period after termination pro rata.

7.6 The current list of sub-processors is always available in Annex 3 of this DPA at swipesign.io/dpa.

---

8. International transfers

8.1 We process Customer Personal Data in the European Union or the European Economic Area by default.

8.2 We transfer Customer Personal Data to a third country or an international organisation only where the conditions of Chapter V GDPR are met, namely on the basis of an adequacy decision of the European Commission, including the EU-US Data Privacy Framework for certified recipients, or of the Standard Contractual Clauses adopted by the European Commission (Art. 46(2)(c) GDPR).

8.3 The sub-processors concerned are marked in Annex 3.

---

9. Data subject requests

9.1 If a data subject sends us a request concerning Customer Personal Data, we forward it to the Customer without undue delay.

9.2 We assist the Customer by appropriate technical and organisational measures, insofar as possible, in responding to requests to exercise data subjects' rights under Chapter III GDPR. The Account lets the Customer access, correct, export and delete Customer Personal Data itself.

---

10. Assistance

10.1 Taking into account the nature of the processing and the information available to us, we assist the Customer in meeting its obligations under Art. 32 to 36 GDPR: security of processing, notification of personal data breaches to the supervisory authority and communication to data subjects, data protection impact assessments and prior consultation of the supervisory authority.

11. Personal data breaches

11.1 We notify the Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data.

11.2 The notification contains, as far as available, the information under Art. 33(3) GDPR: the nature of the breach, including where possible the categories and approximate number of data subjects and records concerned; a contact point for further information; the likely consequences of the breach; and the measures taken or proposed to address the breach and to mitigate its possible adverse effects.

11.3 Where it is not possible to provide all information at the same time, we provide it in phases without undue further delay.

---

12. Deletion and return

12.1 We permanently delete Documents and all intermediate versions 14 days after a workflow is completed, cancelled or expires (section 7.2 of the Terms). Temporary files produced by conversions are deleted within hours.

12.2 Where the Customer has ordered the long-term archive, archived Documents remain stored for the duration of the add-on. When the add-on ends, they remain available for export for 30 days and are then deleted (section 7.4 of the Terms).

12.3 Templates, address-book entries, drafts and unsent Documents remain in the Account until the Customer deletes them or the Account ends (section 7.5 of the Terms).

12.4 The Customer can export its Documents, audit trails and evidence from the Account at any time during the contract and for 30 days after it ends (section 7.6 of the Terms). This export is the return of Customer Personal Data. After that period we delete the remaining Customer Personal Data.

12.5 Sections 12.1 to 12.4 do not apply to data we must retain under the law of the European Union or a Member State, or to the signature evidence and audit trail we hold as controller (section 2.2).

12.6 Deleted data is removed from backups when the backups are overwritten in their regular cycle.

---

13. Audits and information

13.1 We make available to the Customer the information necessary to demonstrate compliance with Art. 28 GDPR and this DPA.

13.2 We allow for and contribute to audits, including inspections, by the Customer or an auditor mandated by the Customer. Audits are first satisfied by documentation and written answers to the Customer's questions.

13.3 Where documentation and written answers are not sufficient, the Customer may carry out an on-site audit itself or through an independent auditor bound to confidentiality. An on-site audit may take place at most once per contract year, or more often after a personal data breach or where a supervisory authority requires it. The Customer gives at least 30 days' written notice. The audit takes place during business hours, without disrupting our operations and without access to the data of other customers. The Customer bears its own costs and those of its auditor.

---

14. Liability

14.1 Liability under this DPA is governed by section 16 of the Terms.

14.2 Nothing in this DPA limits the rights of data subjects or liability towards data subjects under Art. 82 GDPR.

---

15. Final provisions

15.1 This DPA applies for the term of the contract and, after it ends, for as long as we process Customer Personal Data.

15.2 Changes to this DPA are made as set out in section 21 of the Terms.

15.3 This DPA is governed by Austrian law. Jurisdiction is as set out in section 22 of the Terms.

15.4 This DPA is provided in English and German. The English version is authoritative (section 22.3 of the Terms).

Annexes

Annex 1: Processing details

Subject matter and nature

We host, store, process, transmit, display, convert and delete Customer Personal Data to provide the Services.

Purposes

- preparing, sending, signing, delivering and storing Documents;
- verifying the identity of Signers and Recipients where a verified signature or a verified transfer is chosen;
- safe transfer of Documents to Recipients (eDelivery, shown in the platform as Safe Transfer);
- the Customer's address book;
- document tools, including conversion, field detection and summaries by AI that runs on our own infrastructure.

Data subjects

- Signers;
- Recipients;
- reviewers the Customer asks to approve a Document;
- address-book contacts;
- the Customer's Users.

Types of personal data

- name, email address and mobile number;

IP address and browser and device data (user agent);

signing, review and access actions and their timestamps, including the acceptance of terms in Safe Transfer;

the method and result of identity verification, the identity data the provider returns and, for video identification, also date of birth, sex and postal address;

the content of Documents and of files sent through Safe Transfer. These may contain any type of personal data, including special categories of personal data under Art. 9 GDPR, as determined by the Customer.

Duration and retention

Documents: deleted 14 days after a workflow is completed, cancelled or expires; with the long-term archive, for the duration of the add-on and 30 days after it ends.

Temporary files from conversions: deleted within hours.

Safe Transfer links: expire after 14 days or earlier if the Customer withdraws them.

Templates, address-book entries, drafts and unsent Documents: until the Customer deletes them or the Account ends.

After the contract ends: available for export for 30 days, then deleted (section 12.4).

Signature evidence and audit trail: kept by us as controller for at least seven years, outside this DPA.

Annex 2: Technical and organisational measures

Access control

Administrative interfaces (the cluster API, the source code platform and internal admin tools) are reachable only through our company VPN.

Access to Customer Personal Data is restricted to staff who need it.

Two-factor authentication is available for Accounts.

Sign-up, login, SMS and identity checks are rate-limited. Repeated failed logins lead to a temporary account lockout.

Encryption

All connections are encrypted with TLS.

Stored data is encrypted at rest.

Safe Transfer files are encrypted with AES-GCM.

Network and separation

The platform runs on a dedicated Kubernetes cluster hosted by OVH in the EU. OVH's data centres are ISO 27001 certified; the certification is OVH's.

Network policies deny traffic between workloads by default and allow only what is needed.

Each storage bucket has its own storage access key.

Each Customer's data is logically separated by Account.

Document AI, file conversion and IP country lookup run on our own infrastructure, without an external provider.

Abusive IP addresses are blocked automatically.

Logging and monitoring

Logs are collected centrally and monitored with alerting.

Signing actions are recorded in an audit trail sealed with qualified timestamps.

Availability, backup and deletion

Databases are backed up regularly. Backups are stored in the EU, and restoring them is tested.

Documents are deleted 14 days after a workflow ends. Temporary files from conversions are deleted within hours.

Incident handling

Personal data breaches are handled and notified to the Customer as set out in section 11.

Staff

Staff are bound to confidentiality, and access follows the need-to-know principle.

Suppliers

Sub-processors are engaged and bound by contract as set out in section 7.

Annex 3: Sub-processors

OVH SAS, 2 rue Kellermann, 59100 Roubaix, France. Purpose: hosting, database, storage. Data: all Customer Personal Data. Location: EU (France, Germany).

Sendinblue GmbH (Brevo), Köpenicker Straße 126, 10179 Berlin, Germany. Purpose: transactional email to Signers, Recipients and Users. Data: email address, name, message content. Location: Germany.

Twilio Ireland Ltd, 3 Dublin Landings, Dublin 1, Ireland. Purpose: SMS verification codes. Data: mobile number, code. Location: Ireland; parent company Twilio Inc., USA. Transfer basis: Standard Contractual Clauses and EU-US Data Privacy Framework.

Functional Software Inc. (Sentry), San Francisco, USA. Purpose: error monitoring. Data: technical error data (error messages, stack traces, browser and device information, user ID), which may incidentally contain other personal data. Location: stored in Sentry's EU region (Frankfurt, Germany); company in the USA. Transfer basis: Standard Contractual Clauses and EU-US Data Privacy Framework.

eID Easy OÜ, Tallinn, Estonia. Purpose: electronic identity and signature aggregation. Data: identity data of Signers. Location: Estonia.

WebID Solutions GmbH, Friedrichstraße 88, 10117 Berlin, Germany. Purpose: video identification of Signers and Recipients. Data: identity data and identification result. Location: Germany.

Qualified trust service providers and identity providers that a Signer uses act under their own legal obligations and terms as independent controllers and are not sub-processors. These include A-Trust GmbH for qualified certificates and qualified timestamps and ID Austria, the Austrian state electronic identity.

Providers we use for our own purposes as controller, for example for payments, analytics and support, are listed in the Privacy Policy.