# Data Processing Agreement

Version: 03.04.2025

## Introduction

With the Customer Contract, the Parties entered into a data processing relationship pursuant to the Swiss Federal Act on Data Protection (‘FADP’) and the EU General Data Protection Regulation (‘EU-GDPR’). In order to spell out the rights and obligations arising from their data processing relationship in the context of the provisions of the FADP and EU-GDPR, the Parties enter into the following Agreement. This Agreement supplements the Customer Contract.

The terminology pursuant to Art. 5 FADP is used.

With "Skribble," the following refers to both Skribble AG, Förrlibuckstrasse 190, 8005 Zurich, Switzerland ("Skribble Switzerland"), and Skribble Deutschland GmbH, An der Raumfabrik 29, 76227 Karlsruhe, Germany ("Skribble Germany"). This applies regardless of which of the two entities you have entered into the customer contract with.

## 1. Scope

(1) This Agreement applies to all activities that form the subject matter of the Customer Contract and during the performance of which Skribble or Sub-Processors of Skribble under this Agreement process personal data relating to the Customer. This Agreement is only valid insofar as (i) the Customer is either the Controller or Processor within the scope of the FADP and/or the EU-GDPR and (ii) in the Customer Contract, the Customer commissions Skribble as Processor or Sub-Processor of personal data that fall within the scope of the FADP and/or EU-GDPR (‘personal data’).

(2) If the Customer acts as Processor for its own customers and Skribble acts as Sub-Processor, Skribble hereby grants the Customer’s own customers the same rights as are due to the Customer under this Agreement.

## 2. Specification of contractual obligations

(1) The data processing agreed upon by the Parties comprises activities described in the Customer Contract. The detailed scope of the individual activities follows from the Customer Contract. This Agreement supplements the contractual agreements in the Customer Contract and makes them explicit in the context of the provisions of the FADP and EU-GDPR.

(2) The following personal data/categories of personal data is/are or could be the object of data processing by Skribble:

* Personal master data of system users (e.g. first name/last name, e-mail address, mobile phone number, country).
* Communication data (e.g. first name/last name, e-mail address, mobile phone number, landline number, IP address)
* Third-party disclosures (e.g. whether an identification check for QES has been conducted by Swisscom)
* Personal data in documents uploaded to the Skribble platform

(3) The categories of data subjects are:

* System users of the Customer, i.e. individuals within the sphere of the Customer who use Skribble’s services (especially employees of the Customer)
* Other system users, i.e. individuals invited by the Customer to use Skribble’s services (e.g. employees of a contract partner of the Customer)

## 3. Responsibility and authority

(1) Skribble processes the personal data solely for purposes of contract fulfilment and/or for the purposes identified in the Customer Contract. Skribble will not process the personal data for any other purposes and, in particular, is not entitled to disclose it to third parties (with the exception of Sub-Processors).

(2) The Customer is responsible for complying with the provisions of data protection law, particularly for the legality of data transfer to Skribble and the legality of data processing by Skribble.

(3) Skribble may only process personal data within the limits of the Customer’s instructions. An instruction is a written order from the Customer regarding how Skribble is to handle personal data. The Customer’s instructions are set down in this Agreement and in the Customer Contract. The Customer has the right to issue written instructions to Skribble at any time that supplement, amend or replace the existing instructions. Skribble must follow these instructions, provided that this is feasible and it is objectively reasonable to expect Skribble to do so in the context of the contractually stipulated services. Skribble’s requirement to follow instructions only ceases to apply if Skribble is subject to a legal duty to process. This must be communicated to the customer immediately and documented accordingly.

(4) Customer instructions should be directed to Skribble’s Customer Happiness Team (dataprocessing@skribble.com). The Customer will inform Skribble of the employees that have the authority to issue instructions and will do so by suitable means (e.g. by email). Any change in the designated recipient of instructions (Skribble) or the employees authorised to issue instructions (Customer) must be reported to the respective other Party.

(5) Skribble must inform the Customer without delay if Skribble believes an instruction violates the requirements of data protection law. Skribble is entitled to suspend execution of such an instruction until the Customer confirms or changes it.

## 4. Obligations of Skribble

(1) Skribble will only process the personal data in a manner that is compliant with the provisions of this Agreement and the Customer Contract, subject to the fulfilment of statutory, regulatory or governmental provisions and obligations. The Customer will inform Skribble without delay if the Customer discovers a violation of the requirements of data protection law in the course of service provision by Skribble.

(2) Skribble will ensure that the employees involved in processing the personal data are prohibited from processing the personal data for purposes other than those stated in the Customer Contract or in a way that deviates from this Agreement. Skribble will further ensure that employees involved in data processing are obligated to maintain confidentiality and are familiar with those provisions of data protection law that are relevant for them. This includes familiarising them with the obligation to follow instructions established in this Data Processing Agreement.

(3) Skribble will make the contact information of the contact person responsible for data protection issues (who is also the data protection consultant resp. data protection officer pursuant to FADP and EU-GDPR) available to the Customer on the website.

(4) Skribble will inform the Customer without delay of audits, measures or investigations by supervisory authorities.

(5) On request, Skribble will provide the Customer with all relevant information the Customer needs, for example, to carry out a data protection impact assessment or in connection with consultation of or a report to a supervisory authority.

(6) Skribble will maintain a record of processing activities (Art. 12 FADP and Art. 30(2) EU-GDPR) and disclose the most recent applicable version to the Customer on request. At the Customer’s request, Skribble will provide the Customer with information for inclusion in the Customer’s record.

(7) Other mandatory legal obligations of Skribble remain unaffected by this agreement.

## 5. Technical and organisational measures (TOM)

(1) Skribble will implement the technical and organisational measures listed in Annex 1 to protect the processed personal data and to guarantee a degree of data security proportionate to the risk (Art. 8 FADP and Art. 32(1) EU-GDPR). The security concept described in Annex 1 presents state-of-the-art technical and organisational measures appropriate for the identified risk, taking into account the security objectives and, in particular, the IT systems and processing procedures used by Skribble.

(2) Technical and organisational measures change as technology evolves. For this reason, Skribble may adjust the agreed technical and organisational measures or implement appropriate alternative measures at any time. However, the agreed level of security must always be maintained. Critical changes must be documented. The implementation of additional measures can be agreed upon in a contract addendum.

## 6. Queries by data subjects

If a data subject contacts Skribble directly to exercise their rights (Chapter 4 FADP and Chapter III EU-GDPR, e.g. right to access, erasure, rectification or data portability), Skribble will immediately forward this request to the Customer or refer the data subject to the Customer if the information provided by the data subject makes it possible to associate the data subject with the Customer. Skribble may only make direct disclosures to the data subject or to third parties with the prior written consent of the Customer. However, Skribble will provide reasonable assistance to the Customer in responding to requests and enforcing data subjects' rights.

## 7. Evidence and audits

(1) On request, Skribble will provide the Customer with all relevant information needed to document compliance with the obligations established under the FADP/EU-GDPR and this Agreement.

(2) For auditing purposes, the Customer or an auditor appointed by the Customer may verify compliance with the obligations established under this Agreement, especially compliance with the agreed technical and organisational measures, on Skribble’s business premises during usual business hours without interrupting the course of business. The principle of proportionality must be observed during such an audit and Skribble’s legitimate interests (especially relating to confidentiality) must be appropriately safeguarded. The audit must be announced at least 2 weeks in advance. Skribble is under no obligation to tolerate or cooperate with the audit if it is carried out without such advance notice, unless the customer proves good cause for not complying with the obligation to provide advance notice or the obligation to comply with the lead time. The Customer will bear all costs of such audits.

(3) Any compulsory statutory auditing rights of the Customer or the Customer’s supervisory authorities are unaffected.

(4) If the presentation of evidence or reports or the performance of an audit shows that Skribble has failed to comply with obligations under this Agreement at all or to the required standard, Skribble must take suitable measures to remedy the defects without delay and at own cost.

## 8. Notification in case of data breach

Skribble will notify the Customer without delay if Skribble becomes aware of breaches in personal data protection by Skribble or one of its Sub-Processors and will provide the Customer with all relevant information in text form (nature and extent of the breach, possible remedial actions, etc.). In such a case, the Parties will take the necessary steps to ensure the protection of the affected personal data and to reduce any negative consequences for the data subjects and for the Parties.

## 9. Place of processing, disclosure abroad, remote work

(1) The Processor will preferably process the personal data in Switzerland and in the EU/EEA. Switzerland possesses an adequacy decision of the EU Commission pursuant to Art. 45(1) EU-GDPR.

(2) Skribble may disclose personal data to recipients outside Switzerland or outside the EU/EEA only if Skribble complies with the provisions of Art. 16 et seqq. FADP and/or Chapter V EU-GDPR.

(3) Skribble may permit its employees who are entrusted with processing personal data for the Customer to process personal data in coworking facilities, private residences or other suitable locations. Skribble must ensure that compliance with the contractually agreed technical and organisational measures is also guaranteed during remote working. In particular, Skribble must ensure that when personal data is processed outside the office premises, the storage locations are configured in such a way that local storage of data on the IT systems used is ruled out. If this is not possible, Skribble shall ensure that local storage is exclusively encrypted and that other persons do not have access to the data concerned.

## 10. Erasure and return of data

(1) Delivered data carriers and data sets remain the property of the Controller. No copies or duplicates can be made without the Customer’s knowledge. Exceptions include backup copies (when such copies are required to ensure proper processing of data) and data that is required to comply with Skribble’s statutory retention obligations.

(2) After completing the contractually agreed services or, prior to that, at the request of the Customer, but no later than the point in time when the Customer Contract is terminated, Skribble must hand over to the Customer or destroy, in a sufficiently secure procedure after receiving the Customer’s consent, all documents that have entered its possession, all results of processing and use, and all databases (as well as all copies or reproductions thereof) connected with the processing relationship. The same applies for testing material and waste material.

(3) Skribble can retain documentation intended to prove that data has been processed properly and in accordance with the contract for a suitable period of time after the termination of the Contract. Alternatively, to reduce its burden, it can hand over such documentation to the Customer when the Contract is terminated.

## 11. Sub-Processors

(1) Skribble is entitled to use Sub-Processors. The list of Sub-Processors at the time of entry into force of this Agreement is found in Annex 2. The Customer must be notified in advance if Skribble commissions new Sub-Processors or replaces existing Sub-Processors after this Agreement has come into force. The Customer may object to a new Sub-Processor or the replacement of an existing Sub-Processor for important reasons of data protection within 30 days (counted from receipt of notice). If an important reason of data protection is present and the Parties cannot come to an amicable agreement, the Customer may terminate the Customer Contract without notice.

(2) Skribble agrees to draft its contractual agreements with its Sub-Processors in such a way as to guarantee the obligations established under this Agreement, especially including the existence of adequate guarantees of a sufficient level of data security.

(3) The Customer has the right to request in writing that Skribble disclose information about the essential content of the contractual agreements with its Sub-Processors, the implementation of data protection obligations by the Sub-Processors, and the guarantees of a sufficient level of data security.

(4) For the purpose of this provision, services are not considered to be rendered by Sub-Processors if Skribble obtains them as incidental services from third parties to help with contract performance pursuant to the Customer Contract, such as telecommunications services and maintenance of data processing facilities during which access to personal data cannot be ruled out. Skribble is obliged, however, to take appropriate technical and/or organisational measures as well as control measures in order to ensure the security of the Customer’s personal data, even when third parties are hired for such incidental services.

## 12. Term

The term of this Agreement is the same as the term of the Customer Contract. This Agreement will end when the Customer Contract ends or the Customer stops using Skribble’s services, except where the provisions of this Agreement establish obligations of longer duration.

## 13. Liability

(1) Skribble’s liability to the Customer for culpable breaches of this Agreement is regulated by the Customer Contract, or secondarily by statutory regulations.

(2) Skribble is liable for damage culpably caused by its Sub-Processors as for damage caused by itself.

(3) Skribble bears the burden of proof that any damage is not the consequence of a circumstance for which it is responsible. Skribble satisfies its burden of proof if it can demonstrate that it observed the provisions of this Agreement when processing personal data and, in particular, that it implemented the technical and organisational measures.

## 14. Final provisions

(1) Changes and supplements to this Agreement require a written agreement and an express notice that the document is a change or supplement to this Agreement. The same applies to any waiver of this requirement of form.

(2) ‘Written’ for the purpose of this Agreement means (i) written (paper and original signatures) or (ii) an advanced or qualified electronic signature.

(3) Should individual provisions or parts of this agreement prove to be void or invalid or incomplete, this shall not affect the validity of the legal relationship established by this agreement in other respects. The invalidity and/or incompleteness of a provision shall not affect the validity of the other provisions. The void, ineffective and/or incomplete provision shall be replaced by a legally valid substitute provision of the parties which comes as close as possible to the ineffective or incomplete provision.

(4) This Agreement replaces all earlier agreements, accords or declarations regarding data processing.

(5) With respect to the processing of order data, this Agreement shall take precedence over Skribble's GTC or other agreements between the parties to the contrary.

(6) With respect to applicable law and jurisdiction, the law agreed upon in the Customer Agreement between Skribble and the Customer shall apply.

# Annex 1: Technical and organisational measures (TOM)

Version: 03.04.2025

This Annex 1 to the Data Processing Agreement under FADP and EU-GDPR describes the technical and organisational measures implemented by Skribble for protection of the processed personal data and to guarantee a degree of data security proportionate to the risk (Art. 8 FADP, Art. 3 DPO and Art. 32(1) EU-GDPR). The measures described below apply to cases in which Skribble processes personal data itself. If personal data is processed by Sub-Processors, Skribble will enter into suitable contractual agreements to ensure that these Sub-Processors take appropriate and suitable technical and organisational measures.

**1. Pseudonymisation**

How do we guarantee pseudonymisation of data?

*Pseudonymisation means processing personal data in a way that prevents that personal data from being connected with a specific data subject without bringing in additional information, if that additional information is stored separately and is subject to technical and organisational measures and that such personal data is not connected with an identified or identifiable person.*

* Personal data is replaced with random codes (for statistical analyses)
* Website tracking
* Requests from system users are pseudonymised when they come into the ticket system

**2. Encryption**

How do we guarantee encryption?

*Encryption transforms plain text, in conjunction with additional information called a key, into encoded text (cipher) that can only be deciphered by someone who knows the key.*

* Use of cryptographic libraries and software components
* Data hashing
* Transport encryption (SSL/TLS) - “in transit” encryption
* Hard-drive encryption
* Encryption of data in data centres - “at rest” encryption
* Multi-level encryption of data in software
* Use of key management system

**3. Ability to ensure confidentiality**

How do we guarantee our ability to ensure the ongoing confidentiality of data?

*Confidentiality means that personal data is protected against unauthorised disclosure.*

* Physical access control

The servers and database systems are installed in a data centre compliant with ISO 27001 certification. This prevents unauthorised access to those data processing facilities.

◦ Rack access only for authorised persons

◦ 24/7 surveillance by on-site security personnel

◦ Security fence with anti-tunnelling and anti-climbing features

◦ Attendance logs

◦ Visitor IDs accompanied by employees of the data centre operator

◦ Alarm systems

◦ Designated high-security areas

◦ Access control using contactless chip card and PIN or optional biometrics

◦ Doors secured by electric door closers and ID readers

* Security doors and/or windows
* Electronic access control

◦ Access for authorised personnel only

* Lock screen after brief period of inactivity
* Authorisation concept based on need-to-know principle
* Additional login for specific applications
* Encryption of communication and data
* Encryption of data carriers/hard drive encryption
* SSH access with key-based authentication only
* Transport encryption during web access
* Regular training and awareness measures
* Staff: Obligation of confidentiality
* Separation by role
* Network segmentation
* Contract design with service providers

**4. Ability to ensure integrity**

How do we guarantee our ability to ensure the ongoing integrity of data?

*Integrity means ensuring the correctness (completeness) of data and the correct functioning of systems. When integrity is used in the context of data, it means that data is complete and intact. Measures need to be taken to prevent protected data from being damaged or changed during processing and transmission.*

* Traceability of data entered in the portal
* Monitoring of data transmission

◦ TLS encryption

◦ Logging

* Functional responsibilities/Role concept
* Proxy arrangement
* Authorisation concept

◦ Sensitive authorisations are distributed among multiple persons

◦ Four-eyes principle

* Email encryption (if required)
* Encryption of mobile devices, separate work instruction for handling mobile data carriers
* Use of https connections
* Up-to-date antivirus system
* Firewall, WAF
* Network access control (NAC)
* Monitoring the network and system landscape for anomalies (e.g. with a SOC / SIEM)
* Logging and monitoring of relevant data entries and changes, relevant user activities and relevant administrative and service activities

**5. Ability to ensure availability**

How do we guarantee our ability to ensure the ongoing availability of data?

*Availability of services, functions of an IT system, IT applications, IT networks, or information means that users can always use these things as intended.*

* Redundant data centres

◦ UPS

◦ Monitoring and alerting

* Climate systems
* Backup concept

 ◦ Separate storage/storage of backups

◦ Appropriate backup procedures (daily, weekly, monthly)

* Recovery plan
* Fire protection and water protection in the server rooms
* Proxy arrangements
* Overvoltage protection
* Uninterruptible power supply (UPS)
* Air conditioning
* Video surveillance
* Use of RAIDs, mirroring of hard disks
* Vulnerability management for regular identification, assessment and elimination of vulnerabilities (e.g. using a vulnerability scanning tool)
* Annual penetration tests of critical systems and applications
* Standard procedures/patch management for regular updates of protection software (e.g. virus scanners), endpoint hardening, update and patch management
* Change management to control and monitor all changes
* Use of hardened base images for endpoints
* Security baselining of the endpoints

**6. Ability to ensure resilience**

How do we guarantee our ability to ensure the ongoing resilience of data?

*Systems are resilient if they continue to function during periods of heavy access or heavy utilisation.*

* ISO/IEC 27001-certified data centre
* ISO/IEC 9001-certified data centre
* Redundant software components (high availability)
* Runtime scalability

**7. Ability to restore availability and access**

How do we guarantee that personal data is quickly made available and accessible again after a security incident?

* Established and tested incident management process
* Rapid restore
* Backup procedure
* Uninterrupted power supply (UPS)
* Emergency plan
* Proxy arrangements
* Recovery plan

**8. Procedure for regular testing, assessment and evaluation**

How do we guarantee regular testing of data security measures?

* Data protection through technology and data protection-friendly default settings as well as data protection management, expressly including (but not limited to)

◦ Measures to ensure data minimisation

◦ Measures to ensure data quality

◦ Measures to ensure limited data storage

◦ Measures to enable data portability and to ensure the erasure of data

* Order supervision or contract supervision
* Regular auditing by data protection officer
* Test reports are evaluated
* Implementation of a continual improvement process
* Orientated to information security standards (ISO 27001)

**9. Irregular access to personal data**

How do we prevent unauthorised persons from using data processing systems?

* Personalised login
* Creation of a user master record for each user
* Documented assignment, management, regular review and revocation of authorisations
* Logging and monitoring of relevant access to IT systems
* Password guideline for complex passwords
* Separate logins for different systems and applications
* Automatic logout on client side (defined time)
* Two-factor authentication (where possible)
* Access only given to persons who absolutely require it to do their job
* Remote deletion of employee work devices in the event of departure, disposal or loss

**10. Processing personal data only according to instructions**

How do we guarantee that personal data is only processed in accordance with the Controller’s instructions?

* Staff are obliged to follow a code of conduct
* Implementation of internal data protection guidelines
* Staff under obligation of confidentiality
* Training all staff with access rights
* Role concept
* Documentation of responsibilities
* Defining recipients of instructions

#

# Annex 2 – Sub-Processors

Version: 02.07.2025

This Annex 2 to the Data Processing Agreement under FADP and EU-GDPR lists the Sub-Processors used by Skribble. Any addition of new Sub-Processors or replacement of existing Sub-Processors must comply with the provisions of the above Agreement.

1. **Skribble Switzerland**

**Sub-processors engaged by Skribble Switzerland**

If you have concluded the Customer Contract with Skribble Switzerland, Skribble Switzerland will involve the following Sub-Processors:

| **Sub-Processor** | **Activity** | **Data processed** | **Warranty under EU-DSGVO** |
| --- | --- | --- | --- |
| **cloudscale.ch AG**Neugasse 6, 8005 Zurich, SwitzerlandPrivacy Policy:[Privacy Policy cloudscale](https://www.cloudscale.ch/de/datenschutz) | Data centre services: hosting/infrastructure operations. | IP addresses of the system users (incl. persons invited by the Customer to use the Skribble services). | Order processing contract / adequacy decision of Switzerland |
| **VSHN AG**Neugasse 10, 8005 Zurich, SwitzerlandPrivacy Policy:[Privacy Policy VSHN](https://legal.docs.vshn.ch/legal/privacy_policy_en.html) | Data centre services: hosting/infrastructure operations. | IP addresses of the system users (incl. persons invited by the Customer to use the Skribble services). | Order processing contract / adequacy decision of Switzerland |
| **Skribble Deutschland GmbH**An der Raumfabrik 29, 76227 Karlsruhe, Germany wholly owned subsidiary | Research and development services, support. | sResearch and Development Services:Personal Data processed by Skribble may be subject to data processing by Skribble Deutschland GmbH.Support:IP address, first names, names, e-mail addresses, telephone numbers of System Users (including persons invited by the Customer to use Skribble services). | Order processing contract / adequacy decision of Switzerland  |
| **Customer and Message Systems, Inc d/b/a SparkPost**9160 Guilford Road, Columbia, MD 21046, USAPrivacy Policy:[Privacy Policy SparkPost](https://www.sparkpost.com/gdpr/) | The platform’s notification emails are delivered via the SparkPost service.  | First names, surnames, email addresses of the System Users (incl. persons invited by the Customer to use the Skribble services). | Order processing contract incl. EU standard contractual clauses |
| **HubSpot, Inc.**2nd Floor 30 North Wall Quay, Dublin 1, IrelandPrivacy Policy:[Privacy Policy HubSpot](https://legal.hubspot.com/terms-of-service) | Newsletter dispatch, support chat, support email, and support ticketing | First names, surnames, email addresses, telephone numbers and, where applicable, other information needed to process the Customer's or System Users query. | Order processing contract incl. EU standard contractual clauses |
| **Google Mail** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, IrelandPrivacy Policy: [Privacy Policy Google Mail](https://cloud.google.com/privacy/gdpr) | Support requests by email. | First names, surnames, email addresses, telephone numbers of the system users (incl. persons invited by the Customer to use the Skribble services) | Order processing contract incl. EU standard contractual clauses |
| **Stripe Payments Europe, Ltd**C/O A&L Goodbody, Ifsc, North Wall Quay, Dublin 1, IrelandPrivacy Policy:[Privacy Policy Stripe](https://stripe.com/de/legal/dpa) | External payment services provider for credit card payments.Stripe acts as intermediary between the customer and Skribble | Credit card information of the cardholder (administrator of the Customer) | Order processing contract incl. EU standard contractual clauses |
| **CHARGEBEE, INC.**909 Rose Avenue, Suite 610, North Bethesda, MD 20852, USAServer Location: Germany/IrelandPrivacy Policy: [Privacy Policy CHARGEBEE](https://www.chargebee.com/privacy/) | External provider for billing and revenue management. Automation of billing and invoicing processes. | Customer's billing address, names, first names, and email addresses of the person responsible for accounting, credit card details of the cardholder (customer administrator), payment method, payment information (bank account details, tax ID), IP addresses. | Order processing contract incl. EU standard contractual clauses |
| **tyntec Ltd.**8th Floor, 20 Farringdon Street, London EC4A 4AB, United Kingdom [Privacy Policy](https://www.tyntec.com/data-privacy-statement)[Privacy Policy tyntec](https://www.tyntec.com/compliance-statement) | External text message provider for sending text message codes for confirmation of the advanced electronic signature (AES) and for two-factor authentication upon log-in. | Telephone numbers of the System Users (incl. persons invited by the customer to use the Skribble services) | Order processing contract / adequacy decision of the UK |
| **Userpilot, Inc.**2035 Sunset Lake Road, Newark,Delaware 19702, USAServer location: FrancePrivacy Policy:[Privacy Policy Userpilot](https://userpilot.com/privacy-policy) | In-app interactions with users with System Users on the Skribble platform primarily to provide contextualised help to users (e.g. via a help center) | Email addresses of Customers and System users (including persons invited by the Customer to use Skribble services), IP address, device type: desktop/mobile device, operating system, browser version, country code | Order processing contract including EU standard contractual clauses |
| **Cloudflare, Inc.**101 Townsend St, San Francisco, CA 94107, USAPrivacy Policy: [Privacy Policy Cloudflare](https://www.cloudflare.com/privacypolicy/) | Network and security services to protect Skribble applications. | IP addresses and connection data of System Users (including persons invited by the Customer to use the Skribble Services). | Order processing contract including EU standard contractual clauses |
| **Clay Labs, Inc.**119 North 11th, 3C, Brooklyn, NY 11249,USAPrivacy Policy: [Privacy Policy Clay Labs](https://privacy.clay.com) | Prospecting and data enrichment services. | First names, surnames, e-mail addresses, telephone numbers of System Users | Order processing contract including EU standard contractual clauses |

**Trust Service Providers engaged by Skribble Switzerland**

If you have concluded the Customer Contract with Skribble Switzerland, Skribble Switzerland may involve the following Trust Service Providers, if applicable to your specific services:

| **Trust Service Provider** | **Activity** | **Data processed** |
| --- | --- | --- |
| **Swisscom Trust Services AG**Hardturmstrasse 3,8005 Zurich, Switzerland  | Creation of electronic seals, advanced and qualified electronic signatures.Identification services of the Smart Registration Service. | First name, surname, telephone number and issuing country on the identifying document of the system users (incl. persons invited by the Customer to use the Skribble services), biometric data (e.g. selfie-video) |
| **GMO GlobalSign, Ltd.**Springfield House, Sandling Road, Maidstone, Kent, ME12 2LP, United Kingdom | Creation of electronic seals and advanced electronic signatures. | First name, surname, email address of the system users (incl. persons invited by the Customer to use the Skribble Services) |
| **A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH**1030 Vienna, Landstrasser Hauptstrasse 1b, Austria | Creation of advanced and qualified electronic signatures. | Telephone numbers of the system users (incl. persons invited by the Customer to use the Skribble Services) |

**Identification service providers engaged by Skribble Switzerland**

To use certain Skribble Services (such as AES or QES), System Users must first be legally identified. Skribble Switzerland enables identification through the independent providers listed below as required. These services are not part of the Skribble Services, and the providers are not considered subprocessors under Swiss or EU law. They are listed here for transparency.

| **Identification service providers** | **Activity** | **Data processed** |
| --- | --- | --- |
| **PXL Vision AG**Rautistrasse 338047 ZürichSwitzerlandPrivacy Policy:[Privacy Policy PXL Vision](https://pxl-vision.com/hubfs/Terms_and_Conditions/PXL_Ident_CoBranding_Privay_Policy/PrivacyPolicy_CB_EN.pdf?hsLang=en) | Identity verification services (e.g., PXL Ident), including biometric verification, required for signing with Qualified Electronic Signature (QES). | No personal data is transferred from Skribble to PXL Vision.  |
| **Intrum AG**Eschenstrasse 128603 SchwerzenbachSwitzerlandPrivacy Policy:[Privacy Policy Intrum](https://www.intrum.ch/de/business-solutions/uber-intrum/datenschutzerklarung-fur-kunden/) | Identity verification services (Intrum VideoIdent, AutoIdent and OnlineIdent), including biometric verification, required for signing with Advanced (AES) and Qualified Electronic Signatures (QES).  | No personal data is transferred from Skribble to Intrum.  |
| **Nect GmbH**Großer Burstah 2120457 Hamburg GermanyPrivacy Policy:[Privacy Policy Nect](https://nect.com/de/privacy-policy/) | Identity verification services (Nect Ident), including biometric verification, required for signing with Advanced (AES) and Qualified Electronic Signatures (QES).  | No personal data is transferred from Skribble to Nect.  |

1. **Skribble Germany**

**Sub-processors engaged by Skribble Germany:**

If you have concluded the Customer Contract with Skribble Germany, Skribble Germany will involve the following Sub-Processors:

| **Sub-Processor** | **Activity** | **Data processed** | **Warranty under EU-DSGVO** |
| --- | --- | --- | --- |
| **IONOS SE**Elgendorfer Str. 5756410 Montabaur, GermanyPrivacy Policy:[Privacy Policy Ionos](https://www.ionos.de/terms-gtc/datenschutzerklaerung/) | Data center services, hosting / infrastructure operation. | IP addresses of system users (including individuals invited by the customer to use Skribble services). | Order processing contract / adequacy decision of Switzerland |
| **Skribble AG**Förrlibuckstrasse 190, 8005 Zurich(100% parent company of Skribble Deutschland GmbH) | Management of the customer database (CRM), accounting services, research and development services, support, help center. | Personal data processed by Skribble Germany may be subject to processing by Skribble Switzerland. This particularly concerns: IP addresses, first names, last names, email addresses, and telephone numbers of system users (including individuals invited by the customer to use Skribble services). | Order processing contract / adequacy decision of Switzerland |
| **Customer and Message Systems, Inc d/b/a SparkPost**9160 Guilford Road, Columbia, MD 21046, USAPrivacy Policy:[Privacy Policy SparkPost](https://www.sparkpost.com/gdpr/) | The platform’s notification emails are delivered via the SparkPost service.  | First names, surnames, email addresses of the System Users (incl. persons invited by the Customer to use the Skribble services). | Order processing contract incl. EU standard contractual clauses |
| **HubSpot, Inc.**2nd Floor 30 North Wall Quay, Dublin 1, IrelandPrivacy Policy:[Privacy Policy HubSpot](https://legal.hubspot.com/terms-of-service) | Newsletter dispatch, support chat, support email, and support ticketing | First names, surnames, email addresses, telephone numbers and, where applicable, other information needed to process the Customer's or System Users query. | Order processing contract incl. EU standard contractual clauses |
| **Google Mail** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, IrelandPrivacy Policy:[Privacy Policy Google Mail](https://cloud.google.com/privacy/gdpr) | Support requests by email. | First names, surnames, email addresses, telephone numbers of the system users (incl. persons invited by the Customer to use the Skribble services) | Order processing contract incl. EU standard contractual clauses |
| **Stripe Payments Europe, Ltd**C/O A&L Goodbody, Ifsc, North Wall Quay, Dublin 1, IrelandPrivacy Policy:[Privacy Policy Stripe](https://stripe.com/de/legal/dpa) | External payment services provider for credit card payments.Stripe acts as intermediary between the customer and Skribble | Credit card information of the cardholder (administrator of the Customer) | Order processing contract incl. EU standard contractual clauses |
| **CHARGEBEE, INC.**909 Rose Avenue, Suite 610, North Bethesda, MD 20852, USAServer Location: Germany/IrelandPrivacy Policy: [Privacy Policy CHARGEBEE](https://www.chargebee.com/privacy/) | External provider for billing and revenue management. Automation of billing and invoicing processes. | Customer's billing address, names, first names, and email addresses of the person responsible for accounting, credit card details of the cardholder (customer administrator), payment method, payment information (bank account details, tax ID), IP addresses. | Order processing contract incl. EU standard contractual clauses |
| **tyntec Ltd.**8th Floor, 20 Farringdon Street, London EC4A 4AB, United Kingdom [Privacy Policy](https://www.tyntec.com/data-privacy-statement):[Privacy Policy tyntec](https://www.tyntec.com/compliance-statement) | External text message provider for sending text message codes for confirmation of the advanced electronic signature (AES) and for two-factor authentication upon log-in. | Telephone numbers of the System Users (incl. persons invited by the customer to use the Skribble services) | Order processing contract / adequacy decision of the UK |
| **Userpilot, Inc.**2035 Sunset Lake Road, Newark,Delaware 19702, USAServer location: FrancePrivacy Policy:[Privacy Policy Userpilot](https://userpilot.com/privacy-policy) | In-app interactions with users with System Users on the Skribble platform primarily to provide contextualised help to users (e.g. via a help center) | Email addresses of Customers and System users (including persons invited by the Customer to use Skribble services), IP address, device type: desktop/mobile device, operating system, browser version, country code | Order processing contract including EU standard contractual clauses |
| **Cloudflare, Inc.**101 Townsend St, San Francisco, CA 94107, USAPrivacy Policy: [Privacy Policy Cloudflare](https://www.cloudflare.com/privacypolicy/) | Network and security services to protect Skribble applications. | IP addresses and connection data of System Users (including persons invited by the Customer to use the Skribble Services). | Order processing contract including EU standard contractual clauses |
| **Clay Labs, Inc.**119 North 11th, 3C, Brooklyn, NY 11249,USAPrivacy Policy: [Privacy Policy Clay Labs](https://privacy.clay.com) | Prospecting and data enrichment services. | First names, surnames, e-mail addresses, telephone numbers of System Users  | Order processing contract including EU standard contractual clauses |

**Trust Service Providers engaged by Skribble Germany**

If you have concluded the Customer Contract with Skribble Germany, Skribble Germany may involve the following Trust Service Providers, if applicable to your specific services:

| **Trust Service Provider** | **Activity** | **Data processed** |
| --- | --- | --- |
| **Swisscom Trust Services AG**Hardturmstrasse 3,8005 Zurich, Switzerland  | Creation of electronic seals, advanced and qualified electronic signatures.Identification services of the Smart Registration Service. | First name, surname, telephone number and issuing country on the identifying document of the system users (incl. persons invited by the Customer to use the Skribble services), biometric data (e.g. selfie-video) |
| **GMO GlobalSign, Ltd.**Springfield House, Sandling Road, Maidstone, Kent, ME12 2LP, United Kingdom | Creation of electronic seals and advanced electronic signatures. | First name, surname, email address of the system users (incl. persons invited by the Customer to use the Skribble Services) |
| **A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH**1030 Vienna, Landstrasser Hauptstrasse 1b, Austria | Creation of advanced and qualified electronic signatures. | Telephone numbers of the system users (incl. persons invited by the Customer to use the Skribble Services) |

**Identification service providers engaged by Skribble Germany**

To use certain Skribble Services (such as AES or QES), System Users must first be legally identified. Skribble Germany enables identification through the independent providers listed below as required. These services are not part of the Skribble Services, and the providers are not considered subprocessors under Swiss or EU law. They are listed here for transparency.

| **Identification service providers** | **Activity** | **Data processed** |
| --- | --- | --- |
| **PXL Vision AG**Rautistrasse 338047 ZürichSwitzerlandPrivacy Policy:[Privacy Policy PXL Vision](https://pxl-vision.com/hubfs/Terms_and_Conditions/PXL_Ident_CoBranding_Privay_Policy/PrivacyPolicy_CB_EN.pdf?hsLang=en) | Identity verification services (e.g., PXL Ident), including biometric verification, required for signing with Qualified Electronic Signature (QES). | No personal data is transferred from Skribble to PXL Vision.  |
| **Intrum AG**Eschenstrasse 128603 SchwerzenbachSwitzerlandPrivacy Policy:[Privacy Policy Intrum](https://www.intrum.ch/de/business-solutions/uber-intrum/datenschutzerklarung-fur-kunden/) | Identity verification services (Intrum VideoIdent, AutoIdent and OnlineIdent), including biometric verification, required for signing with Advanced (AES) and Qualified Electronic Signatures (QES).  | No personal data is transferred from Skribble to Intrum.  |
| **Nect GmbH**Großer Burstah 2120457 Hamburg GermanyPrivacy Policy:[Privacy Policy Nect](https://nect.com/de/privacy-policy/) | Identity verification services (Nect Ident), including biometric verification, required for signing with Advanced (AES) and Qualified Electronic Signatures (QES).  | No personal data is transferred from Skribble to Nect.  |