SCRIBOFLOW DPA

Data Processing Agreement

Version 1.0 · Effective 21 August 2026

Scriboflow ApS · Denmark · privacy@scriboflow.com

This Data Processing Agreement is incorporated automatically into the Scriboflow Terms of Service and does not require a separate signature to be binding.

If your organisation has a documented requirement for a countersigned copy, you can request one by email. This public agreement applies without countersignature.

http://localhost:3001/trust/dpa View subprocessors Terms of Service Privacy Policy

1 Parties and roles

This Data Processing Agreement (DPA) is between the customer organisation identified in the Scriboflow account or applicable order (Customer) and Scriboflow ApS, Denmark, contactable at privacy@scriboflow.com (Scriboflow).

For Customer Personal Data processed to provide the Service, the Customer is the controller and Scriboflow is the processor. Where the Customer acts as a processor for another controller, Scriboflow is its subprocessor and the Customer confirms that it may appoint Scriboflow on these terms.

Capitalised terms not defined here have the meaning given in the Terms. GDPR means Regulation (EU) 2016/679, and Data Protection Law means the GDPR and other data-protection law applicable to the processing.

2 Scope and incorporation

This DPA is incorporated automatically into the Scriboflow Terms of Service at /terms-of-service and applies whenever Scriboflow processes Customer Personal Data on the Customer's behalf. It is effective for the Customer when the organisation accepts the Terms or otherwise starts using processing covered by this DPA.

If there is a conflict about processing of Customer Personal Data, this DPA prevails over the Terms. The main body prevails over an annex unless the annex expressly states otherwise. Mandatory Data Protection Law always prevails.

3 Subject matter, duration, nature, and purpose

Scriboflow processes Customer Personal Data to host and operate the contract-management and electronic-signing Service, provide support requested by the Customer, maintain security and reliability, and carry out the processing described in Annex II.

Processing continues for the term of the Customer's subscription and any limited period afterwards in which data remains available for export, deletion, legal compliance, dispute handling, or secure removal in accordance with the Terms and this DPA.

4 Documented instructions

Scriboflow will process Customer Personal Data only on documented instructions from the Customer, including the Terms, this DPA, the Customer's configuration and use of the Service, support requests, and other written instructions agreed by the parties, unless EU or Member State law requires processing.

If law requires processing beyond the Customer's instructions, Scriboflow will inform the Customer before processing unless the law prohibits that notice for important public-interest reasons. Scriboflow will promptly inform the Customer if, in its opinion, an instruction infringes Data Protection Law and may suspend the affected processing until the instruction is clarified or changed.

5 Confidentiality and authorised personnel

Scriboflow will ensure that persons authorised to process Customer Personal Data are bound by confidentiality obligations or an appropriate statutory duty of confidentiality, receive access only where needed for their work, and receive relevant data-protection and security guidance.

The Customer is responsible for managing its users, roles, sharing, recipients, signing participants, and instructions, and for ensuring that its personnel and invitees use the Service lawfully.

6 Security of processing

Taking into account the state of the art, implementation costs, and the nature, scope, context, and purposes of processing as well as risks to individuals, Scriboflow will maintain appropriate technical and organisational measures designed to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to it.

The current verified measures are described in Annex III. Scriboflow may update them as technology and risks change, provided the overall protection is not materially reduced. The Customer must use available security controls, protect credentials, configure permissions appropriately, and notify Scriboflow of suspected compromise.

7 Restricted and high-risk data

The Service is not designed for and does not broadly authorise routine processing of special categories of personal data under GDPR Article 9, personal data relating to criminal convictions and offences under Article 10, national identification numbers except where specifically required for an enabled identity service, health records, biometric templates, or similarly high-risk or regulated datasets.

The Customer must not submit such data unless the parties have expressly agreed the relevant use in writing and the Customer has established a lawful basis, safeguards, access restrictions, and any required impact assessment. Incidental appearance of information in a contract does not expand Scriboflow's authorised purposes; the Customer remains responsible for minimising and protecting it.

8 Data-subject requests

Taking into account the nature of the processing, Scriboflow will provide reasonable technical and organisational assistance for the Customer to respond to requests to exercise data-subject rights. Available product functions may be used to access, correct, export, restrict, or delete relevant data.

If Scriboflow receives a request relating to Customer Personal Data, it will, where legally permitted, direct the requester to the Customer and will not respond on the Customer's behalf without authorisation. The Customer is responsible for verifying requests and deciding how to respond.

9 Assistance with controller obligations

Taking into account the nature of processing and information available to Scriboflow, Scriboflow will provide reasonable assistance with the Customer's obligations concerning security, personal-data breaches, data-protection impact assessments, and prior consultation with supervisory authorities.

Scriboflow may charge reasonable fees for unusually extensive assistance that is not caused by Scriboflow's breach of this DPA, after giving the Customer advance information about the expected work and cost.

10 Personal-data breaches

Scriboflow will notify the Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data. The notice will include available information about the nature of the breach, likely consequences, affected data and individuals, measures taken or proposed, and a contact point. Information may be supplied in phases as it becomes available.

Scriboflow will take reasonable steps to contain, investigate, mitigate, and remediate the breach and will reasonably cooperate with the Customer. A notice is not an admission of fault. The Customer is responsible for notifications to supervisory authorities and individuals unless law assigns that duty to Scriboflow.

11 Impact assessments and prior consultation

On reasonable request, Scriboflow will provide information available to it that the Customer reasonably needs to conduct a data-protection impact assessment for its use of the Service or consult a supervisory authority. The Customer remains responsible for determining whether an assessment or consultation is required and for the content of its submission.

12 Return and deletion

During an active subscription, the Customer may use available export and deletion functions. On termination or a written request made in connection with termination, Scriboflow will, at the Customer's choice and subject to available functionality, return or delete Customer Personal Data and delete remaining copies after applicable operational retention periods, unless law requires continued storage.

Data retained by law will be isolated from further processing except for that legal purpose. Deletion from distributed systems and provider media may take additional time. Customer account deletion does not by itself guarantee deletion of organisation-owned data; an authorised organisation administrator must request or perform organisation-level deletion or return.

13 Information and audits

Scriboflow will make available information reasonably necessary to demonstrate compliance with GDPR Article 28 and this DPA. The Customer should first use current documentation, questionnaires, summaries, and independent reports that Scriboflow makes available.

Where that information is insufficient, the Customer may request an audit no more than once in any 12-month period, unless a breach, regulator, or credible material concern justifies another audit. Audits must be proportionate, during normal business hours, on reasonable notice, subject to confidentiality and security restrictions, and avoid access to other customers' data. The Customer bears reasonable audit costs unless the audit identifies a material breach by Scriboflow.

14 Subprocessors

The Customer gives general written authorisation for Scriboflow to use the subprocessors in Annex IV and the current public register at /trust/subprocessors. Scriboflow will impose data-protection obligations that provide substantially equivalent protection for Customer Personal Data and remains responsible for its subprocessors' performance to the extent required by Data Protection Law.

Scriboflow will give at least 30 calendar days' notice before a new customer-data subprocessor begins processing, normally by updating the register and using the Customer's registered administrative contact or an in-product notice. The Customer may object during that period on reasonable data-protection grounds.

The parties will work in good faith on a commercially reasonable solution. If none is available, Scriboflow may avoid the disputed processing or the Customer may terminate the materially affected Service before the new subprocessor begins processing. Termination is the Customer's remedy for an unresolved reasonable objection, without limiting mandatory rights.

15 International transfers

Scriboflow and its subprocessors may process Customer Personal Data outside the Customer's country and outside the EEA. Scriboflow will not make a restricted transfer unless a lawful transfer mechanism applies, such as an adequacy decision, the EU Standard Contractual Clauses, or another mechanism permitted by Data Protection Law.

Where the EU Standard Contractual Clauses are required for a transfer from the Customer to Scriboflow, Module Two applies when the Customer is a controller and Module Three applies when it is a processor. The optional docking clause applies; the supervisory authority and governing law are determined by the Customer's EEA establishment where legally possible, otherwise Denmark and Danish law; and the annexes to this DPA complete the relevant SCC annexes. If the SCCs conflict with this DPA, the SCCs prevail for that transfer.

16 Scriboflow as an independent controller

This DPA does not apply where Scriboflow independently determines purposes and essential means of processing. As described in the Privacy Policy, these limited activities may include account and business relationship administration, billing and regulated payment coordination, fraud and abuse prevention, service security, legal compliance, establishment or defence of claims, and privacy-request records.

Scriboflow will process that data under the Privacy Policy and applicable law. Scriboflow will not treat contract content as its own marketing data or sell Customer Personal Data.

17 Liability

Each party is responsible for its compliance with Data Protection Law and for damage caused by processing where the law assigns responsibility to it. Between the parties, liability arising from this DPA is subject to the exclusions, limitations, and allocation of liability in the Terms, except to the extent those terms cannot lawfully limit a data subject's rights or mandatory regulatory liability.

18 Term, termination, and changes

This DPA remains in force while Scriboflow processes Customer Personal Data on the Customer's behalf. Provisions that protect retained data or by their nature should survive will continue after termination.

Scriboflow may make editorial or non-material clarifications without renewed acceptance. Material changes are identified through a new legal acceptance revision and require organisation-level acceptance before continued use. No change reduces mandatory rights under Data Protection Law.

19 Governing law and disputes

This DPA is governed by Danish law, without regard to conflict-of-law rules, and disputes are handled under the forum provision in the Terms. This does not restrict a data subject's or supervisory authority's rights under applicable Data Protection Law, and it does not alter the governing-law or forum selections required by any applicable Standard Contractual Clauses.

Annex I Parties and contacts

Party	Details
Customer / controller	The customer organisation named in the Scriboflow account or applicable order. Contact: the owner or administrator registered for that organisation. Activities: use of the Service for contract management and electronic signing. Role: controller, or processor where the Customer acts for another controller.
Scriboflow / processor	Scriboflow ApS, Denmark. Privacy contact: privacy@scriboflow.com. Legal contact: legal@scriboflow.com. Activities: provision, security, support, and maintenance of the Service. Role: processor or subprocessor for Customer Personal Data.

Scriboflow's registered address and CVR number are deliberately omitted until verified in the central legal configuration.

Annex II Description of processing

Item	Description
Data subjects	Customer users and administrators; counterparties, contacts, signers, witnesses, approvers, and other people named in contracts or uploaded materials; support correspondents.
Personal data	Names, email addresses, job and organisation details, account and authentication records, contract content and metadata, signatures and signing evidence, uploaded files, communications, audit events, device/network metadata, and support information.
Operations	Collection, recording, organisation, storage, retrieval, consultation, display, transmission to instructed recipients, signing, export, restriction, support access, security analysis, and deletion.
Nature and purpose	Providing customer-configured contract workflows, document generation, collaboration, approvals, electronic signing, evidence, notifications, storage, support, security, and reliability.
Frequency	Continuous or on demand according to the Customer's use of the Service.
Duration	For the subscription term and limited operational, legal, dispute, export, and secure-deletion periods afterwards.
Restricted data	Not broadly authorised. See clause 7. Identity data required for a selected MitID signing flow may be processed for that specific function.

Annex III Technical and organisational measures

- TLS is used for network transport between supported clients and Scriboflow services.
- Production database and object-storage providers document encryption at rest for the services Scriboflow uses.
- Authentication, organisation membership, role checks, row-level security, and restricted service credentials limit access according to role and purpose.
- Multi-factor authentication is available for Scriboflow accounts and enforced for sensitive administrative paths where configured.
- Application and signing events are recorded where required to operate contracts, investigate incidents, and produce signature evidence.
- Changes are version controlled and checked through automated linting, type checks, tests, dependency controls, and deployment checks.
- Organisation-scoped database access is protected by membership checks and row-level security policies.
- Operational errors and security events are monitored and investigated under documented incident-response procedures.
- Environment separation, secret management, and least-privilege access practices.
- Subprocessor review, contractual data-protection terms, and transfer safeguards where required.
- Customer-controlled roles, recipients, sharing, export, and deletion functions where available.

Annex IV Authorised customer-data subprocessors

Verified on 21 August 2026. The current, more detailed register is available at /trust/subprocessors.

Legal provider	Purpose	Data	Location / safeguards
Supabase, Inc.	Managed database, authentication, realtime services, and object storage.	Account, organisation, contact, contract, signing, audit, and uploaded-file data entered into the service.	Primary production region: Frankfurt, Germany. Limited provider support and ancillary processing may occur from other locations under the provider terms. EU/EEA regional hosting for the primary project; contractual transfer safeguards where required.
Google Cloud EMEA Limited and Google group processors	Cloud object storage and supporting infrastructure for files and generated contract artefacts.	Uploaded files, generated documents, contract identifiers, and related technical metadata.	Location depends on the configured resource and provider operations. Google may process where it or its subprocessors maintain facilities, as described in its DPA. Google Cloud data-processing terms, including applicable EU Standard Contractual Clauses for restricted transfers.
Vercel Inc.	Application hosting, content delivery, server-side request processing, deployment, and operational logs.	Account and request identifiers, IP and device metadata, operational logs, and data transmitted through application requests.	United States and other global locations used by Vercel and its subprocessors. Vercel DPA, EU Standard Contractual Clauses, and the EU–US Data Privacy Framework where applicable.
Resend, Inc.	Transactional email delivery for invitations, contract events, security, and service communications.	Recipient names and email addresses, organisation and contract identifiers, message content, and delivery metadata.	United States and other locations used by Resend and its infrastructure subprocessors. Resend DPA and transfer safeguards stated by the provider, including Standard Contractual Clauses where applicable.
Idura ApS	MitID authentication and identity-assisted electronic signing when that signing method is selected.	Signer identity, contact and authentication data, signing transaction identifiers, and evidence metadata.	European Union under Idura's published privacy and data-protection terms. Idura's published processor terms state that service personal data is not transferred outside EU territory and require equivalent safeguards from its processors.