StaticForm

GDPR ARTICLE 28

Data Processing Agreement

for the form submissions StaticForm processes on your behalf

VERSION
2.2

LAST UPDATED
2026-11-11

PROCESSOR
Re: Software B.V.
Schutsboomstraat 55A
5374 CB Schaijk, the Netherlands
KvK 95753214

CONTACT
support@staticform.app
staticform.app/data-processing-agreement

Parties

1. **Re: Software B.V.**, a private limited company under Dutch law, registered with the Dutch Chamber of Commerce (KvK) under number 95753214, VAT number NL867277889B01, with its registered office at Schutsboomstraat 55A, 5374 CB Schaijk, the Netherlands, operating the service StaticForm ("we", "us", the "Processor"); and
2. the customer that has created an account for the Service and accepted the Terms of Service (the "Customer", the "Controller").

Re: Software B.V. is the contracting entity for all use of StaticForm. Invoices and contracts are issued in its name.

---

1. Introduction and Scope

This Data Processing Agreement ("DPA") forms part of the Terms of Service between the Processor and the Customer. It applies whenever personal data of the Customer's form respondents ("Customer Data") is submitted through forms the Customer operates with the Service.

This DPA implements the requirements of Article 28 of the General Data Protection Regulation (GDPR) and applies automatically to all Customers; no signature is required for it to be binding. If the Customer requires a countersigned copy for its records, it can complete the signature block at the end of this DPA and send it to support@staticform.app. We will return a countersigned copy.

The following annexes form part of this DPA:

- Annex I: Description of the processing
- Annex II: List of sub-processors
- Annex III: Technical and organisational measures

---

2. Roles of the Parties

- **The Customer is the Controller** of Customer Data: it decides which fields its forms contain, why the data is collected, where submissions are forwarded, and how long they are kept.
- **Re: Software B.V. is the Processor** of Customer Data: we store and process form submissions only to provide the Service to the Customer.
- For account data (the Customer's email address, billing details, and usage data), Re: Software B.V. acts as an independent Controller as described in our Privacy Policy. That processing is not covered by this DPA.
- **Customers acting as processors.** Where the Customer uses the Service to process personal data on behalf of its own clients (for example as an agency), those clients are the controllers, the Customer is their processor, and Re: Software B.V. acts as the Customer's sub-processor under Article 28(4) GDPR. References to the "Controller" in this DPA then mean the Customer acting on behalf of its clients. We act only on the Customer's documented instructions, which include instructions the Customer passes on from its clients, and we notify and assist the Customer rather than its clients directly. The Customer is responsible for obtaining its clients' authorisation to engage us and the sub-processors inAnnex II, and our obligations under this DPA apply to the Customer in full.

---

3. Details of Processing

The subject matter, duration, nature and purpose of the processing, the categories of data subjects, and the categories of personal data are described in Annex I.

4. Special Categories of Data and National Identification Numbers

The Service may be used to collect special categories of personal data (Article 9 GDPR) or national identification numbers **only if the Customer has a valid legal basis to do so**.

- National identification numbers are subject to additional rules under the national law of many Member States and may only be processed where that law permits it. It is the Customer's responsibility to verify the rules that apply to its processing.
- The Customer warrants that it has verified and documented its legal basis before collecting such data through the Service, and will perform a Data Protection Impact Assessment (DPIA) where required by Article 35 GDPR.
- The Customer must configure its forms and integrations appropriately for such data, for example by marking the fields as sensitive (which encrypts them separately and keeps them out of exports, search, and AI review) and by not forwarding them to third-party integrations that are not covered by the Customer's own processing agreements.
- We may suspend processing and notify the Customer if we become aware that such data is being collected in apparent violation of applicable law.

5. Processing on Documented Instructions

We process Customer Data only on the Customer's documented instructions, including with regard to transfers to third countries, unless required to do otherwise by EU or Member State law. In that case, we will inform the Customer of the legal requirement before processing, unless the law prohibits this. The Customer's instructions consist of the Terms of Service, this DPA, and the configuration choices the Customer makes in the Service (form fields, spam settings, and submit actions).

We will immediately inform the Customer if, in our opinion, an instruction infringes the GDPR or other applicable data protection provisions.

6. Confidentiality

We ensure that all persons authorised to process Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Access to Customer Data is restricted to personnel who need it to operate and support the Service.

7. Security of Processing

Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing, we implement the technical and organisational measures described in Annex III, as required by Article 32 GDPR. We may update these measures over time, provided the overall level of protection is not reduced.

The Customer is responsible for the security of its own systems and integrations, including the destinations to which it forwards submissions and the protection of its API keys and account credentials.

8. Sub-processors

The Customer grants us general authorisation to engage sub-processors for the operation of the Service. The sub-processors we currently use are listed in Annex II.

Integrations that the Customer itself enables (such as Google Sheets, Notion, Slack, Discord, webhooks, the Customer's own SMTP server, its own CAPTCHA provider keys, or its own Stripe account for form payments) are destinations chosen by the Customer, not our sub-processors; the Customer is responsible for its own agreements with those providers.

We impose data protection obligations on our sub-processors that are no less protective than those in this DPA, and we remain fully liable to the Customer for their performance. We will notify the Customer by email at least 30 days before adding or replacing a sub-processor and update Annex II accordingly. During that period, the Customer may object on reasonable data protection grounds. If no resolution is found, the Customer may terminate the affected part of the Service.

9. International Data Transfers

Customer Data is stored within the European Economic Area (EEA): the application and database in Germany, and files, backups, and outgoing email in Sweden. Some sub-processors listed in Annex II are established outside the EEA or operate a global network, which may result in access to or transit of personal data outside the EEA. For those transfers we rely on the sub-processor's certification under the EU-U.S. Data Privacy Framework where available, and otherwise on the Standard Contractual Clauses (SCCs) adopted by the European Commission, supplemented where necessary by additional measures such as encryption in transit.

10. Assistance with Data Subject Rights

Taking into account the nature of the processing, we assist the Customer with appropriate technical and organisational measures in fulfilling the Customer's obligation to respond to data subject requests under Chapter III GDPR (access, rectification, erasure, restriction, portability, and objection). In practice, the Customer can search, export, and delete individual submissions directly through the Service. If a data subject contacts us directly about data processed on the Customer's behalf, we will forward the request to the Customer without undue delay and will not respond substantively unless legally required.

11. Personal Data Breach Notification

We will notify the Customer without undue delay, and in any event within 48 hours, after becoming aware of a personal data breach affecting Customer Data. The notification will describe, to the extent known:

- The nature of the breach, including categories and approximate numbers of data subjects and records concerned
- The likely consequences of the breach
- The measures taken or proposed to address and mitigate the breach
- A contact point for further information

The Customer, as Controller, remains responsible for notifying its supervisory authority and affected data subjects where required by Articles 33 and 34 GDPR. We will reasonably assist the Customer with these obligations.

12. Data Protection Impact Assessments

Taking into account the nature of the processing and the information available to us, we will provide reasonable assistance to the Customer with data protection impact assessments and prior consultations with supervisory authorities under Articles 35 and 36 GDPR, where these relate to processing performed by the Service.

13. Deletion and Return of Data

- The Customer can delete individual submissions, forms, or its entire account at any time through the Service; deletion is permanent.
- The Customer can export submissions through the Service before deletion.
- Upon termination of the Service, we delete all Customer Data in accordance with the retention terms in our Privacy Policy, unless EU or Member State law requires further storage.
- Deleted data may remain in encrypted backups until those backups expire under the retention periods in Annex III; it is not restored from backups except to recover from an incident.

14. Audits

We will make available to the Customer all information reasonably necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR, and allow for and contribute to audits, including inspections, conducted by the Customer or an auditor mandated by the Customer. Audits require at least 30 days' written notice, may occur at most once per year (unless a supervisory authority requires otherwise or following a personal data breach), must not unreasonably disrupt our operations, and are at the Customer's expense. We may first satisfy an audit request by providing relevant documentation of our security measures.

15. Liability, Term, and Precedence

- The limitations of liability in the Terms of Service apply to this DPA.
- This DPA takes effect when the Customer first uses the Service to process personal data and remains in force as long as we process Customer Data.
- In case of conflict between this DPA and the Terms of Service regarding the processing of personal data, this DPA prevails.
- This DPA is governed by the laws of the Netherlands. Disputes are submitted to the competent court in the district where Re: Software B.V. has its registered office, unless mandatory law provides otherwise.

16. Contact

Questions about this DPA, the sub-processor list, or requests for a countersigned copy can be directed to:

- Re: Software B.V., Schutsboomstraat 55A, 5374 CB Schaijk, the Netherlands
- Email: support@staticform.app

Annex I: Description of the Processing

Subject Matter and Duration

The subject matter of the processing is the collection, storage, and delivery of form submissions on behalf of the Customer. Processing lasts for the duration of the Customer's use of the Service, until submissions or the account are deleted.

Nature and Purpose

- Receiving form submissions via the Service's endpoints
- Storing submissions and uploaded files
- Spam and abuse filtering, including an AI review of borderline submissions, which is on by default and which the Customer can switch off per form
- Delivering submissions to destinations configured by the Customer (email, webhooks, Slack, Discord, Google Sheets, Notion, and similar integrations)

Categories of Data Subjects

Individuals who submit data through the Customer's forms (for example website visitors, customers, applicants, or employees of the Customer).

Categories of Personal Data

The Customer determines the categories of personal data through the design of its forms. This may include contact details, identification data, uploaded files, and any other information the Customer chooses to collect, as well as IP addresses and request metadata processed for spam prevention.

Frequency

Continuous, for as long as the Customer's forms accept submissions.

Annex II: List of Sub-processors

Sub-processor	Purpose	Processing location	Data concerned
Hetzner Online GmbH Gunzenhausen, Germany	Hosting of the application servers, database, message queue, and logs	Data centre in Nuremberg, Germany (EEA)	All Customer Data
Amazon Web Services EMEA SARL Luxembourg	Storage of uploaded files (Amazon S3), encrypted backups of the database and files (Amazon S3), and delivery of notification emails (Amazon SES)	AWS region eu-north-1, Stockholm, Sweden (EEA)	All Customer Data (backups); uploaded files; content of email notifications
Cloudflare, Inc. San Francisco, United States	DNS, TLS termination, content delivery, and DDoS protection for the API and web app; Turnstile bot verification	Global edge network (nearest data centre to the visitor)	Submissions in transit, IP addresses, and request metadata
TypeSafe AI, Inc. San Francisco, United States	AI review of borderline submissions for spam detection; on by default, the Customer can switch it off per form	United States	Field values of borderline submissions on forms with AI review on; uploaded files, fields marked sensitive, and fields the Customer excludes are never sent

Payments for the Customer's own StaticForm subscription are processed by Stripe Payments Europe, Ltd. (Ireland). That concerns account data, not Customer Data, and is described in our Privacy Policy.

Annex III: Technical and Organisational Measures

Encryption

- All traffic to the API and web app is encrypted with HTTPS (TLS). Traffic between Cloudflare and our servers is encrypted and authenticated with client certificates, so the origin only accepts requests through Cloudflare.
- Uploaded files and backups are stored encrypted at rest in Amazon S3.
- Fields the Customer marks as sensitive are encrypted separately in the database and replaced by a placeholder in listings, exports, search, and AI review.
- Personal data in account records is encrypted at column level with keys managed by the application.

Access Control

- Customer accounts support two-factor authentication (TOTP) and passkeys; passwords are hashed and checked against known breached passwords.
- Sensitive account actions require re-authentication.
- Role-based permissions for form collaboration; collaborators see only the forms they were invited to.
- API keys are scoped to the account and can be revoked at any time.
- Administrative access to production systems is limited to authorised personnel with individual credentials. Secrets are kept in a dedicated secrets manager, not in source code.

Infrastructure and Network Security

- Production runs on a Kubernetes cluster in an ISO 27001 certified data centre in Germany.
- The database, cache, and message queue are not reachable from the internet; only the API is exposed, behind Cloudflare's DDoS protection.
- Rate limiting on public endpoints and authentication.
- Spam and abuse filtering rejects malicious traffic before it is stored.

Logging and Monitoring

- Security-relevant events (sign-ins, permission changes, data exports, deletions) are recorded in a tamper-evident audit log.
- Application logs, traces, and metrics are processed on our own infrastructure in the EEA.
- Automated alerts on service health, errors, and failed backups.

Availability and Backups

- Continuous archiving of the database (point-in-time recovery) with a retention of 30 days.
- Daily full backups of the database and uploaded files, stored encrypted in a separate storage bucket in the EEA.

Data Minimisation and Retention

- Submissions and their files are kept until the Customer deletes them, the form, or its account; the Customer can delete individual submissions at any time.
- Inactive accounts are deleted after a notice period, with warning emails 30, 7, and 1 day in advance.
- Copies of notification emails are kept in the email log for 90 days, for delivery troubleshooting.

Secure Development

- Changes are made through pull requests that run an automated test suite, including architecture tests that enforce the handling of personal data.

- Dependencies are monitored and updated automatically for known vulnerabilities.
- Production is deployed from version control only; infrastructure is defined as code.

Organisational Measures

- Personnel with access to Customer Data are bound by confidentiality.
- An incident response procedure covers detection, containment, and notification within the period in section 11.
- Sub-processors are selected for their security and data protection guarantees and bound by written agreements.

Signatures

Controller (Customer)

Company:

Name and title:

Date:

Signature:

Processor

Company: Re: Software B.V.

Name and title:

Date:

Signature: