



Data Processing Agreement

Version 1.0 · Effective 20 October 2026 · privacy@formbold.com

You build the forms and decide what they collect. We receive, store and deliver the submissions for you. This agreement explains how we handle the personal data inside them, in line with the GDPR and the other data protection laws listed below.

This Data Processing Agreement (the "DPA") is between Pimjo Technologies ("Pimjo", "we", "us", "our"), the company that builds and runs FormBold, and the customer that uses FormBold ("you", "your"). It forms part of the FormBold Terms of Service, or any other written agreement between us for the use of FormBold (the "Agreement").

AT A GLANCE

Our role	Processor. You are the Controller.
Security incident notice	Within 72 hours of becoming aware
Deletion after account closure	Within 72 hours from live systems
International transfers	EU Standard Contractual Clauses, UK Addendum, Swiss terms
Sub-processor changes	30 days' notice, with the right to object
Your data, your purpose	Never sold, never used for ads, never used to train AI models
Privacy contact	privacy@formbold.com

1 How this DPA applies

- 1.1 This DPA applies whenever we process Customer Personal Data on your behalf while providing the Services.
- 1.2 It takes effect when you accept it, whether by clicking to accept, ticking a box that refers to it, or signing it, or when you first use the Services after it has been made available to you, whichever happens first. A signature is not required for it to be binding.
- 1.3 The person accepting this DPA confirms they have the authority to bind you.
- 1.4 This DPA stays in force for as long as we process Customer Personal Data for you, including any period after the Agreement ends and before deletion under Section 9.

2 Definitions

Terms not defined here have the meaning given in the Agreement.

Applicable Data Protection Law

All data protection and privacy laws that apply to the processing under this DPA. Depending on where you and your form respondents are, this may include: Regulation (EU) 2016/679 (the "GDPR"); the GDPR as it forms part of UK law, together with the UK Data Protection Act 2018 (the "UK GDPR"); the Swiss Federal Act on Data Protection (the "FADP"); Bangladesh's Personal Data Protection Ordinance, 2025; and US state privacy laws, including the California Consumer Privacy Act as amended by the California Privacy Rights Act (the "CCPA").

Controller, Processor, Data Subject, Personal Data, Processing, Supervisory Authority

Have the meanings given in the GDPR. "Process" and "processed" are read in the same way.

Customer Personal Data

Personal Data that the Services receive, store or deliver on your behalf, including form submissions, uploaded files and the metadata that comes with them.

Security Incident

A breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data.

Services

FormBold, including form endpoints, the dashboard, email notifications, autoresponders, file uploads, spam protection, team workspaces and integrations.

SCCs

The standard contractual clauses approved by European Commission Implementing Decision (EU) 2021/914.

Sub-processor

Any third party we engage that processes Customer Personal Data.

UK Addendum

The International Data Transfer Addendum to the SCCs issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018.

3 Roles and instructions

- 3.1 You are the Controller of Customer Personal Data and we are your Processor. If you act as a Processor for another Controller, you confirm that your instructions to us are authorised by that Controller, and we act as your sub-processor.
- 3.2 We process Customer Personal Data only on your documented instructions. Your instructions are this DPA, the Agreement, and the settings you choose in the Services, such as notification recipients, autoresponders, retention options and the integrations you enable. Any further instructions must be agreed in writing.
- 3.3 If the law requires us to process Customer Personal Data in any other way, we will tell you before we do so, unless the law prohibits us from telling you.
- 3.4 We will tell you promptly if we believe an instruction from you breaks Applicable Data Protection Law. We may pause the affected processing until you confirm or change that instruction.

- 3.5 You are responsible for having a lawful basis to collect the data your forms ask for, for the privacy notices you show to people who fill in your forms, and for the accuracy and lawfulness of the data you ask us to process.
- 3.6 The subject matter, duration, nature and purpose of the processing, and the types of data and Data Subjects involved, are set out in Schedule 1.

4 Our people and how we use your data

- 4.1 Only staff and contractors who need access to provide, support or secure the Services can access Customer Personal Data. Each of them is bound by a duty of confidentiality that continues after their work with us ends.
- 4.2 We do not sell Customer Personal Data, use it for advertising, or use it to train artificial intelligence models.

5 Security

- 5.1 We maintain technical and organisational measures that protect Customer Personal Data to a level appropriate to the risk, taking into account the state of the art, the cost of implementation, and the nature, scope, context and purposes of the processing. These include the measures in Schedule 2.
- 5.2 We review our measures regularly and may update them as technology and threats change. Updates will not reduce the overall level of protection.
- 5.3 You are responsible for the security of your own account, including passwords, API keys, the people you invite to your workspaces, and any endpoints or integrations you send data to.

6 Sub-processors

- 6.1 You give us general authorisation to engage Sub-processors. The Sub-processors we use on the effective date are listed in Schedule 3.
- 6.2 Before a Sub-processor processes Customer Personal Data, we put a written agreement in place that requires data protection obligations no less protective than those in this DPA. We remain responsible to you for how each Sub-processor meets those obligations.
- 6.3 We will give you at least 30 days' notice before adding or replacing a Sub-processor, by email to your account owner and by updating our Sub-processor list.
- 6.4 You may object to a change on reasonable data protection grounds by emailing privacy@formbold.com within the notice period. We will work with you in good faith to resolve the objection. If we cannot, you may end the affected Services, and we will refund any prepaid fees for the period after termination.

7 Helping you meet your obligations

- 7.1 Where the Services let you view, export or delete submissions yourself, those features are the first way to respond to requests from Data Subjects. Where you need more help, we will assist you with appropriate technical and organisational measures, as far as reasonably possible.

- 7.2 If a Data Subject contacts us directly about Customer Personal Data, we will forward the request to you without undue delay. We will not respond to it ourselves, other than to direct the person to you, unless you instruct us to or the law requires it.
- 7.3 We will give you reasonable help with data protection impact assessments, prior consultations with Supervisory Authorities, and your obligations under Articles 32 to 36 of the GDPR, based on the nature of the processing and the information available to us.

8 Security incidents

- 8.1 We will notify you without undue delay, and in any case within 72 hours, after we become aware of a Security Incident affecting Customer Personal Data.
- 8.2 Our notice will describe, as far as we know at the time:
- what happened and when;
 - the categories and approximate number of Data Subjects and records involved;
 - the likely consequences;
 - the steps we have taken or plan to take to address it and limit its effects; and
 - a contact person for further information.
- If some details are not yet available, we will share them in stages, without further undue delay.
- 8.3 We will take reasonable steps to contain the incident and find its cause, and we will cooperate with you on any notices you need to give to Supervisory Authorities or affected individuals.
- 8.4 We send notices to the email address of your account owner. Keeping that address current is your responsibility.
- 8.5 Unsuccessful attempts that do not compromise Customer Personal Data, such as blocked login attempts, port scans or denial of service attempts, are not Security Incidents.
- 8.6 Notifying you of, or responding to, a Security Incident is not an admission of fault or liability.

9 Retention, return and deletion

- 9.1 Submissions are kept for the retention period that applies to your FormBold plan, or until you delete them, whichever comes first.
- 9.2 You can delete submissions and forms from your dashboard at any time.
- 9.3 Before you close your account or the Agreement ends, you can export your data. After account closure, we delete Customer Personal Data from our live systems within 72 hours, unless the law requires us to keep it.
- 9.4 Any copies held in backups are removed through our routine backup cycle. Until then, they stay protected under this DPA and are not used for any other purpose.
- 9.5 On request, we will confirm deletion in writing.

10 Audits and compliance information

- 10.1 On request, we will make available the information reasonably needed to show that we meet this DPA and Article 28 of the GDPR. This may include this DPA, a description of our security measures, answers to a reasonable security questionnaire, and the certifications or audit reports of our main infrastructure providers.
- 10.2 If that information is not enough to meet a requirement of Applicable Data Protection Law or a request from a Supervisory Authority, you may audit our processing of Customer Personal Data. Audits are limited to once in any 12 month period, except after a Security Incident or where a Supervisory Authority requires otherwise. They need at least 30 days' written notice, take place during normal business hours, are carried out by you or an independent auditor bound by confidentiality, are at your cost, and must not disrupt our operations or expose other customers' data.
- 10.3 Our Sub-processors are assessed through their own certifications and audit reports, not by direct audit under this Section.

11 International data transfers

- 11.1 Pimjo is based in Bangladesh. Customer Personal Data may be processed in Bangladesh and in the countries where our Sub-processors operate, as listed in Schedule 3.
- 11.2 **Transfers from the EEA.** Where Customer Personal Data is transferred from the European Economic Area to a country that does not have an adequacy decision, the SCCs are incorporated into this DPA by reference and apply as follows:
- Module Two (Controller to Processor) applies where you are a Controller, and Module Three (Processor to Processor) applies where you are a Processor;
 - you are the data exporter and we are the data importer;
 - the optional docking clause in Clause 7 applies;
 - in Clause 9, Option 2 (general written authorisation) applies, with the notice period in Section 6.3;
 - the optional wording in Clause 11 does not apply;
 - in Clauses 17 and 18, the SCCs are governed by the laws of Ireland and disputes are resolved by the courts of Ireland; and
 - Annexes I, II and III of the SCCs are completed by Schedules 1, 2 and 3 of this DPA.
- 11.3 **Transfers from the UK.** Where the UK GDPR applies, the UK Addendum is incorporated into this DPA. Tables 1 to 3 of the UK Addendum are completed with the information in this DPA and the SCC selections in Section 11.2, and in Table 4 either party may end the UK Addendum as set out in its Section 19.
- 11.4 **Transfers from Switzerland.** Where the FADP applies, the SCCs apply with these changes: references to the GDPR are read as references to the FADP; the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner; and the term "Member State" does not prevent Data Subjects in Switzerland from bringing claims where they habitually live.
- 11.5 **Onward transfers.** Where a Sub-processor receives Customer Personal Data in another country, we make sure the transfer is covered by a valid transfer mechanism, such as an adequacy decision, the EU-US Data Privacy Framework where the Sub-processor is certified, or the SCCs.
- 11.6 If a transfer mechanism we rely on is no longer valid, we will work with you to put a suitable alternative in place.

12 US state privacy laws

- 12.1 Where the CCPA or a similar US state privacy law applies, we act as your "service provider" or "processor" as those terms are defined in that law.
- 12.2 We will not sell or share Customer Personal Data, as those terms are defined in the CCPA. We will not retain, use or disclose it for any purpose other than providing the Services to you, or outside our direct business relationship with you. We will not combine it with personal data we receive from other sources, except as the law allows.
- 12.3 We will tell you if we can no longer meet these obligations, and you may take reasonable steps to stop and correct any unauthorised use. We certify that we understand these restrictions and will comply with them.

13 Liability and order of precedence

- 13.1 Each party's liability under this DPA is subject to the limits and exclusions of liability in the Agreement, and counts towards the same overall cap, except where Applicable Data Protection Law or the SCCs do not allow it.
- 13.2 If there is a conflict, the SCCs (where they apply) take priority over this DPA, and this DPA takes priority over the Agreement in relation to the processing of Customer Personal Data.

14 General

- 14.1 We may update this DPA to reflect changes in the law, our Sub-processors or our security measures. Updates will not materially reduce the protection you receive. The current version is published on the FormBold website, and we will notify you of material changes.
- 14.2 Except where the SCCs or Applicable Data Protection Law require otherwise, this DPA is governed by the laws of Bangladesh, and the courts of Dhaka have exclusive jurisdiction.
- 14.3 If any part of this DPA is found invalid or unenforceable, the rest remains in full effect.
- 14.4 Questions about this DPA or about how we handle Customer Personal Data can be sent to privacy@formbold.com.

SCHEDULE 1 · SCCS ANNEX I

Details of processing

A. The parties

Data exporter	The customer named in the FormBold account. Contact: the account owner's email address. Role: Controller, or Processor acting for a third party Controller.
Data importer	Pimjo Technologies, Dhaka, Bangladesh, operator of FormBold. Contact: privacy@formbold.com . Role: Processor.
Activities	Providing the FormBold form backend service under the Agreement.

B. Description of the processing

Data Subjects	People who fill in your forms, such as website visitors, leads, customers, job applicants and event registrants, and any other people whose details are included in a submission.
Types of Personal Data	Set by you through the fields your forms collect. Typically this includes name, email address, phone number, company, postal address, message content and uploaded files, plus technical data such as IP address, browser and device details, the page the form was sent from, timestamps and spam screening signals.
Special categories	Not required to provide the Services. If you choose to collect special category data, such as health information, you are responsible for having a lawful basis and for any extra safeguards it needs.
Frequency	Continuous, each time a form is submitted.
Nature of processing	Receiving submissions at form endpoints, screening them for spam and abuse, storing them, showing them in your dashboard, sending email notifications and autoresponders, storing uploaded files, passing data to the integrations you enable, and deleting data.
Purpose	To provide the Services to you under the Agreement.
Retention	As described in Section 9: for your plan's retention period or until you delete it, and deleted from live systems within 72 hours of account closure.
Transfers to Sub-processors	Same subject matter and nature as above, limited to each Sub-processor's role in Schedule 3, for the duration of the Agreement.

C. Competent supervisory authority

Determined in line with Clause 13 of the SCCs, based on the data exporter's establishment or, where relevant, its representative in the European Union.

Account data is separate. Information about you and your team as FormBold users, such as login details and billing contacts, is processed by Pimjo as a Controller under the FormBold Privacy Policy, not under this DPA.

SCHEDULE 2 · SCCS ANNEX II

Technical and organisational measures

We protect Customer Personal Data with the following measures, which we review and improve over time.

Encryption	• All connections to form endpoints, the dashboard and our APIs are encrypted in transit with TLS. • Stored submissions and uploaded files are encrypted at rest.
Access control	• Access to production systems is limited to authorised personnel on a need-to-know, least-privilege basis. • Strong authentication, including multi-factor authentication where supported, on accounts with access to production infrastructure. • Access is removed promptly when it is no longer needed.
Customer controls	• Team workspaces let you decide who in your organisation can see submissions. • You can delete submissions and forms, and export your data, from the dashboard.
Application and abuse protection	• Spam and abuse screening on submissions, using our own filtering rules and Google reCAPTCHA on forms where it is enabled. • Error monitoring to detect and fix faults quickly.
Infrastructure and resilience	• Hosting on established cloud providers that maintain recognised security certifications for their data centres. • Regular backups, so availability and access to data can be restored after an incident.
Organisational measures	• Confidentiality obligations for everyone with access to Customer Personal Data. • A documented process for detecting, handling and reporting Security Incidents within the 72 hour window in Section 8. • Data protection review of new Sub-processors before they are engaged. • Data minimisation and deletion controls, including retention limits by plan and deletion after account closure.

SCHEDULE 3 · SCCS ANNEX III

Sub-processors

We use the following Sub-processors to provide the Services as of the effective date of this DPA. Changes are notified as described in Section 6.

Sub-processor	What they do for FormBold	Data involved	Location
DigitalOcean, LLC	Application hosting, compute and databases	All Customer Personal Data stored in the Services	Data centre region selected for the Services
Cloudflare, Inc.	File storage for form uploads (Cloudflare R2)	Uploaded files and file metadata	Storage location configured for the Services
Amazon Web Services, Inc.	Email delivery for notifications and autoresponders (Amazon SES)	Submission content included in emails, recipient and sender addresses	AWS region configured for the Services
Zoho Corporation (ZeptoMail)	Transactional email delivery for notifications and autoresponders	Submission content included in emails, recipient and sender addresses	Data centre linked to our ZeptoMail account
Google LLC (reCAPTCHA)	Bot and spam detection on forms where reCAPTCHA is enabled	IP address, browser and device details, interaction signals	United States and global
Functional Software, Inc. (Sentry)	Error monitoring and diagnostics	Technical data in error reports, which may include IP address and limited request data	Region of our Sentry organisation
Microsoft Corporation (Clarity)	Product analytics and session replay on the FormBold website and dashboard, used to improve usability	On-screen interaction data, device details, IP address	United States and global

Services that are not Sub-processors

Website analytics	We run Umami analytics on our own infrastructure. No submission or analytics data is shared with a third party analytics provider through it.
Customer support	Support is handled by email and through Nivon, a support platform built and run in-house by Pimjo.
Payments	Paddle.com Market Limited is our merchant of record. Paddle handles billing, tax and fraud prevention as an independent Controller under its own terms and privacy policy, and does not receive form submission data.
Integrations and webhooks	When you connect a third party tool or send submissions to a webhook, data goes to your own account or endpoint with that provider. That provider works for you, not for us, and is not our Sub-processor. Your agreement with them governs that data.

SCHEDULE 4**GDPR Article 28 reference**

For your records and vendor reviews, this table shows where each requirement of Article 28 of the GDPR, and the transfer rules in Chapter V, is covered in this DPA.

GDPR requirement	Where it is covered
Art. 28(1) Sufficient guarantees of appropriate measures	Section 5, Schedule 2
Art. 28(2) and 28(4) Engaging other processors	Section 6, Schedule 3
Art. 28(3) Subject matter, duration, nature, purpose, data and Data Subjects	Section 3.6, Schedule 1
Art. 28(3)(a) Processing only on documented instructions, including for transfers	Sections 3.2, 3.3 and 11
Art. 28(3)(b) Confidentiality of authorised persons	Section 4.1
Art. 28(3)(c) Security measures under Art. 32	Section 5, Schedule 2
Art. 28(3)(d) Conditions for using Sub-processors	Section 6
Art. 28(3)(e) Helping with Data Subject requests	Sections 7.1 and 7.2
Art. 28(3)(f) Helping with Arts. 32 to 36 (security, breaches, DPIAs)	Sections 7.3 and 8
Art. 28(3)(g) Deletion or return at the end of the Services	Section 9
Art. 28(3)(h) Information and audits	Section 10
Art. 28(3) Telling the Controller about infringing instructions	Section 3.4
Arts. 44 to 49 International transfers	Section 11

Signatures

This DPA is binding once accepted as described in Section 1.2. A signature is not needed. If your procurement process requires a signed copy, both parties may sign below. Signing adds no obligations beyond those in this DPA. This DPA may be signed electronically and in counterparts.

PROCESSOR	CUSTOMER
Pimjo Technologies	
Signature	Company name
Name	Signature
Title	Name and title
Date	Date