

Data Processing Addendum

Version 1.0

Last updated: October 5, 2026

<https://formtorch.com/legal/dpa>

1. Parties, scope and acceptance

This Data Processing Addendum ("**DPA**") forms part of the Formtorch Terms of Service (the "**Terms**"). It is between BitForward Technologies Inc., Calgary, Alberta, Canada, which operates Formtorch ("**Formtorch**"), and the customer that has accepted the Terms ("**Customer**").

1.1 Acceptance. Customer accepts this DPA by accepting the Terms. A PDF copy can be downloaded at formtorch.com/legal/dpa/formtorch-dpa-v1.0.pdf. A countersigned copy is available on request at privacy@formtorch.com, but countersignature is not required for this DPA to take effect.

1.2 Scope. This DPA applies to Customer Personal Data, meaning personal data that Formtorch processes on Customer's behalf to provide the Service, mainly form submissions. It does not apply to data that Formtorch processes as an independent controller, such as Customer account, billing and usage data and marketing website analytics. That data is governed by the Formtorch Privacy Policy.

1.3 Order of precedence. If this DPA conflicts with the Terms on any data protection matter, this DPA prevails. If this DPA conflicts with any other Formtorch legal document or page, including the Privacy Policy and the subprocessor list, this DPA prevails. If the Standard Contractual Clauses apply and conflict with this DPA, the Standard Contractual Clauses prevail.

2. Definitions

2.1 "Data Protection Laws" means all laws that apply to the processing of Customer Personal Data, including: the GDPR; the UK GDPR and the UK Data Protection Act 2018; the Swiss Federal Act on Data Protection ("**FADP**"); the Personal Information Protection and Electronic Documents Act ("**PIPEDA**") and substantially similar Canadian provincial laws; and any law that implements or supplements them.

2.2 "GDPR" means Regulation (EU) 2016/679.

2.3 "Customer Personal Data" means personal data submitted to Customer's forms or otherwise processed by Formtorch on Customer's behalf under the Terms.

2.4 "Respondent" means an individual who submits data through a form connected to Customer's Formtorch account.

2.5 "Service" means the Formtorch form backend service described in the Terms.

2.6 "Subprocessor" means a third party that Formtorch engages to process Customer Personal Data.

2.7 "Personal Data Breach" means a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Personal Data. It includes a "**breach of security safeguards**" under PIPEDA.

2.8 "Standard Contractual Clauses" or "SCCs" means the clauses approved by Commission Implementing Decision (EU) 2021/914, together with the UK Addendum and Swiss amendments where they apply.

2.9 "Canada Adequacy Decision" means Commission Decision 2002/2/EC, which recognises that Canadian organisations subject to PIPEDA provide adequate protection.

2.10 "Controller", "Processor", "Data Subject", "Personal Data", "Processing" and "Supervisory Authority" have the meanings given in the GDPR.

3. Roles of the parties

3.1 For Customer Personal Data, Customer is the Controller and Formtorch is the Processor.

3.2 Customer acting as a processor. Where Customer processes Customer Personal Data on behalf of its own client (for example, an agency that builds forms for a client's website):

- Customer confirms that its client has authorised the processing described in this DPA, including the appointment of Formtorch as a sub-processor.
- Formtorch acts as Customer's Subprocessor.
- Customer remains Formtorch's only point of contact and is responsible for passing on any information and notices to its client.

3.3 Customer's responsibilities. Customer is responsible for:

- having a lawful basis for collecting Customer Personal Data through its forms;
- giving Respondents the notices that Data Protection Laws require;
- the configuration of its forms, including retention settings, notification recipients and integrations;
- not collecting special categories of personal data, or personal data of children, unless it has a lawful basis to do so and has assessed whether the Service is suitable for that data.

4. Processing on instructions

4.1 Formtorch processes Customer Personal Data only on Customer's documented instructions, including with regard to transfers, unless the law requires otherwise. In that case, Formtorch will inform Customer of the legal requirement before processing, unless the law prohibits it.

4.2 Customer's documented instructions are the Terms, this DPA, Customer's configuration of the Service (form settings, notification recipients, webhooks, integrations and retention), and any other written instructions both parties agree to.

4.3 Integrations. When Customer enables an integration that sends data to a third party, such as Google Sheets, a webhook or an automation tool, sending data to that destination is Customer's instruction. The destination is not a Formtorch Subprocessor. Customer is responsible for its own arrangements with that provider.

4.4 Formtorch will promptly inform Customer if, in its opinion, an instruction infringes Data Protection Laws.

4.5 Spam and abuse prevention. Providing the Service includes scoring submissions for spam (TorchWarden), quarantining flagged submissions and rate limiting requests. Formtorch does not sell Customer Personal Data, does not use it for advertising, and does not use it to train generalised AI or machine-learning models.

5. Personnel

Formtorch ensures that anyone authorised to process Customer Personal Data:

- is bound by confidentiality obligations; and
- has access only as needed to provide support, investigate security or abuse, or comply with the law.

6. Security

6.1 Formtorch implements the technical and organisational measures in Annex II. These are designed to ensure a level of security appropriate to the risk, as required by Article 32 of the GDPR, and the safeguards required by PIPEDA Principle 4.7.

6.2 Formtorch may update these measures over time, provided that the overall level of security does not materially decrease.

7. Subprocessors

7.1 General authorisation. Customer authorises Formtorch to engage the Subprocessors listed in Annex III and at formtorch.com/legal/subprocessors.

7.2 Notice of changes. Formtorch will give at least 30 days' notice before adding or replacing a Subprocessor. Notice is given by email to the account owner.

7.3 Right to object. Customer may object to a new Subprocessor on reasonable data protection grounds within 30 days of the notice. The parties will discuss the objection in good faith. If they cannot resolve it, Customer may terminate the affected part of the Service and receive a pro-rata refund of any prepaid fees for it.

7.4 Urgent replacement. If a Subprocessor must be replaced urgently for security or continuity reasons, Formtorch will notify Customer as soon as possible afterwards. The objection right in 7.3 then applies.

7.5 Obligations passed on. Formtorch will put a written contract in place with each Subprocessor that imposes data protection obligations no less protective than those in this DPA.

7.6 Liability. Formtorch remains liable to Customer for its Subprocessors' performance of their obligations.

8. Data subject requests

8.1 Self-service tools. Customer's workspace administrator can view and delete Customer Personal Data, and download it in CSV format, at any time through the dashboard.

8.2 Requests received by Formtorch. If Formtorch receives a request from a Data Subject about Customer Personal Data, it will forward the request to Customer without undue delay where Customer can be identified. Formtorch will not respond to the request itself, except to direct the Data Subject to Customer, unless the law requires it to.

8.3 Further assistance. Where Customer cannot fulfil a request using the self-service tools, Formtorch will provide reasonable assistance, taking into account the nature of the processing.

9. Personal Data Breaches

9.1 Notice. Formtorch will notify Customer without undue delay, and in any event within 48 hours, after becoming aware of a Personal Data Breach.

9.2 Content of the notice. The notice will describe, as far as is then known:

- the nature of the breach;
- the categories and approximate number of Data Subjects and records affected;
- the likely consequences;
- the measures taken or proposed to address it;
- a contact point for more information.

Where not all information is available at once, Formtorch will provide it in phases without further undue delay.

9.3 Response. Formtorch will take reasonable steps to contain, investigate and mitigate the breach, and will cooperate with Customer so that it can meet its own notification obligations.

9.4 Delivery. Notices are sent to the account owner's email address. Customer is responsible for keeping that email address up to date.

9.5 Formtorch will not notify Supervisory Authorities or Data Subjects about a breach of Customer Personal Data on Customer's behalf, unless the law requires it or Customer asks it to. Notifying Customer of a breach is not an admission of fault or liability.

10. Impact assessments and prior consultation

Formtorch will provide reasonable assistance with Customer's data protection impact assessments and prior consultations with Supervisory Authorities under Articles 35 and 36 of the GDPR, and with any privacy impact assessment required by Canadian law. This assistance relates only to Formtorch's processing of Customer Personal Data and is given mainly through this DPA, the [Security page](#) and the [subprocessor list](#).

11. Deletion and return

11.1 During the term. Customer can export or delete Customer Personal Data at any time. The dashboard shows 30 days of submissions on the Free plan, 12 months on Starter, and all submissions on Pro. Older submissions are hidden, not deleted, and reappear if Customer upgrades. Formtorch deletes hidden submissions on request (privacy@formtorch.com) and at account closure (Section 11.2).

11.2 At termination. Customer may export its data before closing its account. Formtorch will delete Customer Personal Data within 30 days of account closure or termination of the Terms, unless the law requires Formtorch to keep it.

11.3 Backups. Deleted data is removed from backups as they expire, within 30 days. Until then, backups are encrypted, access to them is restricted, and they are not used for any other processing.

11.4 Confirmation. On written request, Formtorch will confirm in writing that the deletion is complete.

12. Audits and information

12.1 Information. Formtorch will make available the information needed to demonstrate compliance with this DPA, including:

- this DPA, the Security page and the subprocessor list;
- third-party audit reports of its infrastructure providers, where those providers allow Formtorch to share them;
- written answers to a reasonable security questionnaire, once every 12 months.

12.2 Audits. If that information is not enough to demonstrate compliance, or if a Supervisory Authority requires it, or after a Personal Data Breach, Customer may audit Formtorch's compliance with this DPA. The audit must:

- be requested with at least 30 days' notice;
- take place no more than once every 12 months (except after a breach or at a Supervisory Authority's request);
- be carried out during business hours, remotely where possible;
- be conducted by Customer or an independent auditor bound by confidentiality;
- be at Customer's cost.

13. International transfers

13.1 Transfers to Formtorch. Formtorch is established in Canada and is subject to PIPEDA. Transfers of Customer Personal Data from the EEA to Formtorch rely on the Canada Adequacy Decision. Transfers from the UK and Switzerland rely on the equivalent UK and Swiss adequacy recognition of Canada.

13.2 Data location. Customer Personal Data is stored in AWS us-west-2 (Oregon, United States), through Neon, and processed by serverless functions in Portland, US (Vercel region pdx1). Files uploaded through forms are stored in AWS S3 in us-west-2 (Oregon).

13.3 Onward transfers. Where a Subprocessor processes Customer Personal Data in a country without an adequacy decision, Formtorch will make sure a valid transfer mechanism is in place. Examples are the Subprocessor's certification under the EU-US Data Privacy Framework, or SCCs (Module 3, processor to processor) with a transfer impact assessment where required.

13.4 Fallback. If the Canada Adequacy Decision ceases to apply, the SCCs are incorporated into this DPA with the elections in Annex IV, and Annexes I and II serve as their annexes. Module 2 applies where Customer is a Controller and Module 3 where Customer is a Processor.

14. Canadian privacy law (PIPEDA)

14.1 Where Customer is subject to PIPEDA or substantially similar provincial laws, Formtorch processes personal information as a third party on Customer's behalf. Customer remains accountable for that information. This DPA is the contractual means of providing a comparable level of protection, as required by PIPEDA Principle 4.1.3.

14.2 Formtorch will notify Customer of any breach of security safeguards involving Customer Personal Data in accordance with Section 9. This allows Customer to assess whether the breach creates a real risk of significant harm and to report to the Office of the Privacy Commissioner of Canada and notify individuals where required. Formtorch will keep a record of each such breach for at least 24 months and provide it to Customer on request.

14.3 Where Quebec's Act respecting the protection of personal information in the private sector applies, Formtorch will provide the information Customer reasonably needs for any privacy impact assessment it must complete before personal information is communicated outside Quebec.

15. General terms

15.1 Liability. Each party's liability under this DPA is subject to the limitations in the Terms, except where Data Protection Laws or the SCCs do not permit such limitations.

15.2 Term. This DPA remains in effect for as long as Formtorch processes Customer Personal Data.

15.3 Changes. Formtorch may update this DPA to reflect changes in law or in its Subprocessors. It will give at least 30 days' notice of any change that materially affects Customer. No change will reduce the overall level of protection for Customer Personal Data.

15.4 Notices. Notices to Formtorch go to privacy@formtorch.com. Notices to Customer go to the account owner's email address.

15.5 Governing law. This DPA is governed by the law that governs the Terms, which is the law of the Province of Alberta and the federal laws of Canada that apply there, without affecting the mandatory provisions of Data Protection Laws. The SCCs, where they apply, are governed by the law chosen in Annex IV.

Signature (optional, for customers who need a countersigned copy)

	Customer	BitForward Technologies Inc. (Formtorch)
Signature		
Name		
Title		
Date		

Annex I: Description of the processing

Item	Description
Controller (data exporter)	Customer, as identified in its Formtorch account. Where Customer acts for a client, it is a Processor and the client is the Controller.
Processor (data importer)	BitForward Technologies Inc. (Formtorch), Calgary, Alberta, Canada (full registered address on request), privacy@formtorch.com , privacy lead: Long Nguyen
Categories of Data Subjects	Respondents; individuals whose details Respondents include in a submission

Categories of personal data	Fields Customer configures in its forms, typically name, email address, phone number, company, message content and uploaded files. Technical data: IP address, user agent, referrer, submission time and spam-scoring metadata.
Special categories of data	None intended. Customer must not collect them unless it has a lawful basis and has assessed whether the Service is suitable.
Frequency	Continuous, whenever a form is submitted
Nature of processing	Receiving, spam scoring, storing, displaying in the dashboard, sending email notifications, forwarding to integrations Customer enables, exporting and deleting
Purpose	Providing the Service to Customer under the Terms
Duration	The period during which Customer uses the Service, plus the deletion period in Section 11. Individual submissions are kept until Customer deletes them or the account is closed. On Free and Starter plans, older submissions are hidden but not deleted (Section 11.1).
Competent Supervisory Authority	The authority of the EU Member State where Customer is established or, if Customer is not established in the EU, where its EU representative is located

Annex II: Technical and organisational measures

Area	Measures
Encryption	TLS 1.2 or higher for all connections. Database encrypted at rest with AES-256 (AWS storage managed by Neon). OAuth tokens encrypted at rest. Passwords hashed by the authentication provider and never stored or logged in plaintext.
Tenant isolation	Every form and submission belongs to an authenticated workspace, and every query is authorised against that workspace. There is no cross-tenant access.
Customer access control	Email and password with verification, or Google OAuth.
Internal access control	Production access limited to the founders. MFA required on hosting, database, authentication and source-code accounts (Vercel, Neon, Clerk and GitHub). Least-privilege access.
Infrastructure	Hosted on Vercel and Neon (AWS), both SOC 2 audited, with DDoS protection and automatic backups (7-day history window).
Abuse prevention	TorchWarden spam scoring with quarantine. Four-layer rate limiting (IP, form, global and burst), backed by Redis with an in-memory fallback.
Data minimisation and retention	Submissions kept until Customer deletes them; on Free and Starter plans, older submissions are hidden (Section 11.1). Deletion on demand. Deletion within 30 days of account closure.
Logging and monitoring	Error monitoring through Sentry, configured to exclude submission content.

Vulnerability management	Public responsible disclosure policy with acknowledgement within 48 hours. Regular dependency updates.
Incident response	Breaches handled as set out in Section 9: Customer notification within 48 hours and breach records kept for 24 months.
Personnel	Confidentiality obligations and need-to-know access (Section 5).

Annex III: Subprocessors

Subprocessor	Purpose	Customer Personal Data involved	Location	Transfer mechanism
Vercel Inc.	Hosting and serverless compute	All submission data in transit and in processing	Portland, US (pdx1, us-west-2)	EU-US Data Privacy Framework or SCCs, as set out in the provider's DPA
Neon, LLC	Managed Postgres database	Stored submissions	AWS us-west-2 (Oregon, US)	EU-US Data Privacy Framework or SCCs, as set out in the provider's DPA
Amazon Web Services, Inc. (S3)	File storage	Files uploaded through forms	AWS us-west-2 (Oregon, US)	EU-US Data Privacy Framework or SCCs, as set out in the provider's DPA
Upstash, Inc. (Redis)	Rate limiting	IP addresses, form IDs	AWS ca-central-1 (Canada)	None needed: data stays in Canada
Upstash, Inc. (QStash)	Background job queue for notifications, webhooks and integrations	Job and submission IDs only; no submission content	AWS us-east-1 (Virginia, US)	EU-US Data Privacy Framework or SCCs, as set out in the provider's DPA
Plus Five Five, Inc. (Resend)	Sending notification emails	Submission content, recipient email addresses	US	EU-US Data Privacy Framework or SCCs, as set out in the provider's DPA
Functional Software, Inc. (Sentry)	Error diagnostics	Request metadata; submission content excluded	US	EU-US Data Privacy Framework or SCCs, as set out in the provider's DPA

This list does not include providers that only process data Formtorch holds as an independent controller: Clerk (account authentication), Stripe (payments), Google Analytics and Microsoft Clarity. It also does not include destinations Customer enables itself, such as Google Sheets or webhooks (Section 4.3). List those providers on the public subprocessor page and in the Privacy Policy.

Annex IV: SCC elections (applies only under Section 13.4)

SCC clause	Election
Modules	Module 2 (Controller to Processor) where Customer is a Controller. Module 3 (Processor to Processor) where Customer is a Processor.
Clause 7 (docking clause)	Not used
Clause 9(a) (subprocessors)	Option 2, general written authorisation, with 30 days' notice as in Section 7
Clause 11 (redress)	The optional independent dispute resolution wording is not used
Clause 13 (supervision)	The authority named in Annex I
Clause 17 (governing law)	The law of Ireland
Clause 18 (courts)	The courts of Ireland
UK and Switzerland	The UK Addendum (version B1.0) and the Swiss FADP amendments apply to the extent required