EzyMaps Data Processing Agreement

Last updated 17 November 2026

This Data Processing Agreement (the "DPA") is between AViK Web LTD ("AViK Web", the "Processor") and the business, organization or individual that has accepted the EzyMaps Business Agreement or Terms of Service ("Customer", the "Controller"). It sets the terms on which AViK Web processes personal data on Customer's behalf under the Nigeria Data Protection Act 2023 (the "NDPA"). Together, the Business Agreement or Terms of Service and this DPA are the "Agreement".

This DPA forms part of the Agreement and applies automatically, without signature, to personal data that AViK Web processes for Customer. Customer can ask for a countersigned copy (section 12). Terms not defined here have the meaning given in the Agreement.

This DPA includes: Annex 1 (description of the processing), Annex 2 (security measures) and Annex 3 (sub-processors).

1. Definitions

- **"Applicable Data Protection Law"** means the NDPA, the regulations, directions and guidance of the Nigeria Data Protection Commission (the "NDPC") made under it, and any other data protection law that applies to the Customer Personal Data (for example, the GDPR where it applies).
- **"Controller", "Processor", "Data Subject", "Personal Data", "Personal Data Breach", "Sensitive Personal Data" and "Process"** have the meanings given to "data controller", "data processor", "data subject", "personal data", "personal data breach", "sensitive personal data" and "processing" in the NDPA.
- **"Customer Personal Data"** means Personal Data in Customer Data that AViK Web Processes on Customer's behalf.
- **"Instructions"** means Customer's documented instructions to AViK Web about the Processing of Customer Personal Data.
- **"Sub-processor"** means a third party that AViK Web engages to Process Customer Personal Data.
- **"Supervisory Authority"** means the NDPC or any other regulator with authority over the Processing.

2. Roles and scope

2.1 For Customer Personal Data, Customer is the Controller and AViK Web is the Processor. For Account Data and the other personal data that AViK Web handles for its own purposes, such as running and securing the Services and billing, AViK Web is a controller, as its Privacy Policy (ezymaps.com/privacy) explains. This DPA does not apply to that data.

2.2 If Customer is itself a processor for another controller, Customer confirms that it is authorized to give these Instructions and to agree to this DPA for that controller.

3. Details of the processing

The subject-matter, nature and purpose of the Processing, its duration, and the types of Personal Data and categories of Data Subjects are set out in Annex 1.

4. Customer’s responsibilities

4.1 Instructions. The Agreement, Customer's use and configuration of the features of the Services, and any written instructions Customer sends to support@ezymaps.com are Customer's complete Instructions. Anything beyond them needs the parties' agreement in writing.

4.2 Lawfulness. Customer is solely responsible for complying with Applicable Data Protection Law in its use of the Services. In particular, Customer will: (a) have a lawful basis for the Processing, such as the Data Subjects' consent; (b) give Data Subjects the notices the law requires, including that surveys record GPS position and photos; (c) get the consent of a parent or guardian before it collects Personal Data of a child under 18; and (d) keep to what is necessary, collecting only the Personal Data it needs.

4.3 Sensitive Personal Data. AViK Web does not ask Customer for Sensitive Personal Data. If Customer chooses to collect it, Customer is responsible for having a lawful basis and the safeguards the law requires, and for making sure the Instructions are lawful.

4.4 Errors and requests. Customer will tell AViK Web without undue delay about any error or irregularity in the Processing that it notices. Customer is responsible for answering Data Subjects' requests about Customer Personal Data and for any notification to a Supervisory Authority or to Data Subjects that the law requires of a Controller.

5. AViK Web’s obligations

5.1 Instructions. AViK Web will Process Customer Personal Data only on Customer's Instructions and to provide the Services, unless the law requires otherwise, in which case it will tell Customer before the Processing if the law allows. If AViK Web believes an Instruction breaks Applicable Data Protection Law, it will tell Customer without delay and may pause the Processing concerned until Customer confirms or changes the Instruction.

5.2 Confidentiality. AViK Web will make sure that everyone it authorizes to Process Customer Personal Data is bound by a duty of confidentiality, which continues after their work ends.

5.3 Security. AViK Web will keep up the technical and organizational measures in Annex 2 to protect Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access.

5.4 Personal Data Breach. AViK Web will tell Customer about a Personal Data Breach affecting Customer Personal Data without undue delay and, where it can, within 48 hours of becoming aware of it. The notice will say, as far as AViK Web then knows, what happened, which Customer Personal Data and roughly how many Data Subjects are affected, the likely consequences, what AViK Web has done or proposes to do, and who to contact. If AViK Web cannot give all this at once, it will give it in stages. AViK Web will help Customer to meet its duties to notify the NDPC within 72 hours and to tell affected Data Subjects where the law requires.

5.5 Data Subjects' requests. If a Data Subject asks AViK Web about Customer Personal Data, AViK Web will pass the request to Customer promptly and will not answer it itself unless Customer asks it to. Customer can use the edit and delete tools in the Services, and the survey export, to answer most requests. AViK Web will give other reasonable help, using appropriate technical and organizational measures, and may charge its reasonable costs for help that goes beyond those tools.

5.6 Impact assessments. AViK Web will give Customer reasonable help with data protection impact assessments and with consulting the NDPC, taking into account the nature of the Processing and the information AViK Web has.

5.7 Records and cooperation. AViK Web will keep a record of the Processing it does for Customer and will cooperate with the NDPC as the law requires.

6. Sub-processors

6.1 Authorization. Customer agrees that AViK Web may use the Sub-processors listed in Annex 3, and its own affiliates, to Process Customer Personal Data.

6.2 Changes. AViK Web will tell Customer at least 30 days before it adds or replaces a Sub-processor, by email to the workspace owner and by updating Annex 3. Customer may object within that time on reasonable data protection grounds. If the parties cannot resolve the objection, either may end the affected Services by written notice, and AViK Web will refund the part of any prepaid fee for the time after the end.

6.3 Flow-down. AViK Web will have a written contract with each Sub-processor that imposes data protection obligations that are, in substance, the same as those in this DPA, or will rely on the Sub-processor's standard data processing terms that give an equivalent level of protection.

6.4 Responsibility. AViK Web remains responsible to Customer for the performance of each Sub-processor's obligations.

7. Transfers outside Nigeria

7.1 Customer agrees that Customer Personal Data is Processed outside Nigeria by the Sub-processors in Annex 3, principally in the United States and the European Union.

7.2 AViK Web will make each such transfer only on a basis the NDPA allows, such as the receiving country's adequate level of protection or appropriate safeguards, including binding contractual terms, and will give Customer details of the safeguards on request.

7.3 If the GDPR or the UK GDPR applies to Customer Personal Data and a transfer needs standard contractual clauses, the parties will enter into the clauses approved for that purpose on Customer's written request, and Annexes 1 to 3 will serve as their appendices.

8. Audits

8.1 AViK Web will give Customer the information needed to show that it is complying with this DPA, such as a description of its security measures and its Sub-processors' published certifications and reports.

8.2 If that is not enough, or after a Personal Data Breach, or if a Supervisory Authority requires it, Customer may audit AViK Web's compliance, itself or through an independent auditor who is not a competitor of AViK Web. Audits will be by agreement, on at least 30 days' notice, in business hours, without interrupting AViK Web's business, subject to confidentiality, and at Customer's cost, no more than once a year unless a breach has occurred. AViK Web may decline an audit that would put the security or confidentiality of other customers' data at risk.

9. Return and deletion

9.1 If Customer deletes a workspace or account in the Services, the Customer Personal Data in it is deleted straight away and cannot be recovered. When the Agreement ends in any other way, AViK Web will keep Customer Personal Data for at least 14 days, so that Customer can export survey responses using the

Services and ask AViK Web for a copy of the rest. After that, AViK Web will delete Customer Personal Data and copies of it, normally within 30 days, and will confirm in writing if Customer asks. Backup copies are overwritten in the ordinary course.

9.2 AViK Web may keep Customer Personal Data to the extent the law requires, for example in invoices. It will then protect it and Process it only for that purpose. Where Customer asks for something beyond the export tools and normal deletion, AViK Web may charge its reasonable costs.

10. Liability

Each party's liability under this DPA is subject to the limits and exclusions in the Agreement.

11. Term, changes and precedence

11.1 This DPA lasts as long as AViK Web Processes Customer Personal Data. If Applicable Data Protection Law changes in a way that needs changes to this DPA, AViK Web may update it by notifying Customer, and the parties will work together in good faith on anything that is unclear.

11.2 If this DPA conflicts with the rest of the Agreement about the protection of personal data, this DPA prevails. If a part of it is invalid or unenforceable, the rest is not affected.

11.3 This DPA is governed by the laws of the Federal Republic of Nigeria. Disputes are resolved as the Agreement provides.

12. Contact and countersignature

Questions about this DPA, requests under section 5.5 and requests for a countersigned copy go to support@ezymaps.com, with the name of the organization and the account email. Signing is not needed for this DPA to apply. A countersigned copy is for Customers who need one for their own records.

AViK Web LTD

By: _____

Name: _____

Title: _____

Date: _____

Customer: _____

By: _____

Name: _____

Title: _____

Date: _____

Annex 1: Description of the processing

Subject-matter	Hosting and processing Customer Data so that Customer can build maps and surveys, publish and embed maps, and use datasets in EzyMaps.
Nature and purpose	Storing, organizing, displaying, publishing, exporting, backing up, transmitting and deleting Customer Data; delivering emails Customer asks the Services to send; giving support when Customer asks; and, where Customer uses Ask AI, sending summaries and scrubbed text answers to an AI provider to produce an answer.
Duration	The term of the Agreement, plus the export and deletion period in section 9.
Categories of Data Subjects	Customer's team members, staff and contractors; people whose details Customer puts on maps or in spreadsheets (for example, contacts at locations); people Customer's field teams survey; and visitors to Customer's published maps and embeds.
Types of Personal Data	Names, phone numbers, email addresses and other contact details; locations (coordinates and addresses); GPS readings with their accuracy and time; photos; free-text and other survey answers, as Customer designs its surveys; account and team data (names, emails, roles); and technical data of map viewers (IP address, browser and the page showing the map).
Sensitive Personal Data	Not requested by AViK Web. If Customer collects any, it does so at its own choice and responsibility (section 4.3).
Frequency	Continuous, while Customer uses the Services.

Annex 2: Security measures

AViK Web currently uses the measures below. It may change them, as long as it does not materially reduce the overall level of protection. Physical security of data centres is provided by AViK Web's hosting providers.

- **Sign-in and access.** Sign-in is handled by Auth0, so AViK Web does not store passwords. Access inside a workspace depends on a person's role (owner, admin or member). Access to production systems is limited to authorized staff who need it.
- **Encryption.** All traffic between browsers and AViK Web's servers is encrypted in transit. Files are stored privately and served through short-lived links. Storage providers encrypt files at rest by default.
- **Separation.** Each workspace's files are stored under their own folders, and access to a workspace's data is checked on every request.
- **Abuse protection.** Public and sign-in-related endpoints are rate limited. Embedded maps use short-lived signed sessions and an allowed-domain check.
- **Logging and monitoring.** Security events, such as sign-ins and failed attempts, are logged with the IP address and kept for a limited time. Errors are monitored without personal details attached by default.
- **Data minimization and retention.** Spreadsheets uploaded for import are deleted automatically about a day after upload. Ask AI sends only summaries and text answers with names, emails and phone numbers removed, and its conversations are deleted after 30 days. Customer Data is deleted on request and after the Agreement ends (section 9).
- **People.** Staff and contractors who can access Customer Personal Data are bound by confidentiality.

- **Incidents.** AViK Web investigates suspected incidents and notifies Customer as section 5.4 provides.

Annex 3: Sub-processors

Each Sub-processor below Processes data outside Nigeria, principally in the United States and the European Union. Mailgun sends through its EU region. AViK Web can give the specific regions on request.

Sub-processor	What it does	Customer Personal Data involved
Railway	Application servers, database and task queue	All Customer Data
Amazon Web Services (S3)	Private file storage	Photos and temporary spreadsheet uploads
Cloudflare	Delivery, security, storage of published maps and datasets, and custom domains	Published map content; visitors' IP addresses
Auth0 (Okta)	Sign-in and identity	Team members' names, emails and sign-in activity
Mailgun (Sinch), EU region	Service emails such as invitations	Recipients' names and email addresses
Sentry	Error monitoring	Technical error reports, without personal details by default
Mapbox	Basemaps and address search	The map area viewed, search text and viewers' IP addresses
Anthropic	The AI model behind Ask AI, only when used	Summaries and text answers with names, emails and phone numbers removed