Authi - Connect
Data Protection Addendum

This Data Protection Addendum ("DPA") describes how Authi and the User handle Personal Information in connection with the Services.

This document forms part of the Authi Connect contractual framework and is an Incorporated Document under the Authi Connect Master Terms and Conditions (the "Master Terms"). This DPA forms part of the Authi Connect Agreement between Authi Limited ("Authi") and the User, and applies in addition to the other documents that form part of the Authi Connect Agreement. Matters including termination, suspension, liability, indemnities, assignment, dispute resolution, and governing law are governed exclusively by the Master Terms.

Version 1 – Effective 8 January 2026

1. Purpose and Precedence

1.1. Purpose: This DPA describes how Authi and the User handle Personal Information in connection with the Services (including access to reporting in the Authi Portal).

1.2. Precedence: If there is any conflict between this DPA and the Master Terms, this DPA prevails to the extent of the conflict on matters of privacy and data protection (and otherwise the order of precedence in the Master Terms applies)

1.3. Governing law: This DPA is governed by the laws of New Zealand.

2. Roles and Relationship

2.1. Independent controllers: The Parties acknowledge that, for the Services, Authi and the User act as independent controllers of the Personal Information each processes. Authi does not process consumer Personal Information on behalf of the User as a processor.

2.2. No consumer Personal Information: As at the Effective Date, the Parties acknowledge that Authi does not collect or store Personal Information that identifies individual consumers who interact with Campaigns. Authi's interaction and performance data is collected and stored in an aggregated and/or de-identified form (and/or as non-personal operational records).

2.3. User Portal accounts: Authi processes account and access data for Users of the Authi Portal (for example, names, business contact details, login credentials, role permissions, and audit logs) to operate, secure and support the Services.

2.4. Campaign configuration: The User configures Campaigns in the Authi Portal. Authi determines the technical and operational means by which the Services are delivered, including systems for security, fraud prevention, reconciliation and reporting.

3. Definitions

3.1. In this DPA, unless the context requires otherwise:

- Personal Information has the meaning given in the Privacy Act 2020 (New Zealand).
- Privacy Act means the Privacy Act 2020 (New Zealand), as amended from time to time.
- Services means the services provided by Authi under the Agreement, including the Authi Portal, Campaign configuration and delivery (where applicable), content display and interaction capture on supported terminals, and reporting and analytics features.
- Subprocessor means a third party engaged by Authi to process Personal Information for or on behalf of Authi in connection with the Services.
- User means the entity that enters into the Agreement with Authi and accesses and uses the Services via the Authi Portal.

4. Compliance with Privacy Laws

4.1. Each Party will comply with applicable privacy and data protection laws in connection with the Personal Information it controls and processes, including the Privacy Act.

4.2. Each Party is responsible for providing its own privacy notices and obtaining any consents or authorisations it requires for its own processing activities.

5. Use, Sharing, and Aggregation

5.1. Authi will use Personal Information it controls (including User Portal account information) only as reasonably necessary to provide, secure, support, maintain and improve the Services, to prevent fraud and abuse, and to reconcile and administer operational obligations.

5.2. Aggregated benchmarking: Authi may create and use aggregated and/or de-identified data derived from the Services (including Campaign performance data and reporting outputs) for benchmarking, analytics, product improvement, and industry reporting. Any such aggregation will be performed in a manner that does not identify any individual or any User. Authi may share aggregated and/or de-identified data with third parties (including partners) for analytics, benchmarking and reporting, including on a commercial basis, provided that such data does not identify any individual or any User. Authi will not disclose non-aggregated Personal Information of the User's Portal users to third parties except as permitted under the Subprocessors section or as required by law.

5.3. No onward disclosure of non-aggregated data: Authi will not provide to other Users any non-aggregated data provided by the User or derived from the User's Campaigns. Any sharing for benchmarking or comparative reporting will be in aggregated and/or de-identified form.

6. Security Measures

6.1. Authi will implement and maintain appropriate technical and organisational security measures designed to protect Personal Information against accidental or unlawful loss, access, disclosure, alteration or destruction.

6.2. At a minimum, Authi's measures include: encryption in transit and at rest, role-based access controls, multi-factor authentication for privileged access, and logging and monitoring of access to production systems.

6.3. SOC 2 alignment: Authi maintains an information security programme aligned to the SOC 2 Trust Services Criteria and may provide security summaries and/or independent assurance reports when available, subject to confidentiality and reasonable limitations.

7. Reporting Features

7.1. Reporting access: Users have the ability to access reporting within the Authi Portal. Reporting forms part of the Services and is treated as operationally important functionality for the purposes of Authi's service operation and incident response, but does not constitute a guarantee as to the accuracy, completeness, or fitness for purpose of any reporting outputs.

8. Subprocessors

8.1. Authorisation: The User authorises Authi to engage Subprocessors to support delivery of the Services.

8.2. Current Subprocessors: As at the Effective Date, Authi uses the following Subprocessors:

- Google Cloud Platform (GCP) for hosting and storage (primary region: Australia).
- Email service provider(s) for service communications and support email (provider: Google).

8.3. Changes: Authi may add or replace Subprocessors. Where reasonably practicable, Authi will provide prior notice of material changes (including via the Authi Portal or email).

8.4. Flow-down: Authi will impose data protection obligations on Subprocessors that are materially consistent with this DPA, to the extent applicable.

9. Data Retention and Deletion

9.1. Operational records retention: Authi may retain operational records (including system, security and audit logs, and other records necessary to operate, secure and support the Services) for the minimum period reasonably required for security, fraud prevention, reconciliation, auditability, dispute management and legal/compliance obligations. Unless a longer period is required by law or reasonably required to establish, exercise or defend legal claims, Authi will apply the following retention periods:

9.1.1. security and audit logs: up to 24 months;

9.1.2. backups: up to 35 days; and

9.1.3. billing, tax and financial records: 7 years.

Authi may retain aggregated and/or de-identified data that does not identify any individual indefinitely.

9.2. Portal user Personal Information: On written request by the User, or upon termination of the User's account, Authi will delete or anonymise Portal user Personal Information controlled by Authi within 30 days, unless retention is required by law or reasonably required for security, fraud prevention, auditability, dispute management, or to establish, exercise or defend legal claims. Where Authi retains Portal user Personal Information under this paragraph, Authi will restrict access to it and delete or anonymise it when it is no longer required for those purposes.

9.3. Limit on deletion (immutable records): The Parties acknowledge that certain operational records may need to remain immutable to preserve system integrity and auditability. In those cases, Authi will delete or anonymise direct identifiers where reasonably practicable while preserving the underlying record integrity.

10. Privacy Breach Notification

10.1. Notification: If Authi becomes aware of a Privacy Breach involving Personal Information it controls (including User Portal account information), Authi will notify the User without undue delay and will provide reasonable information about the breach as it becomes available

10.2. Content: Notifications will include (to the extent known): the nature of the breach, the categories of Personal Information affected, the likely consequences, and the measures taken or proposed to address the breach and mitigate adverse effects.

10.3. Cooperation: Authi will reasonably cooperate with the User in relation to the breach, including to support the User's assessment of any notification obligations the User may have under applicable law.

11. Requests and Data Subject Rights

11.1. Requests to Authi: Requests relating to Authi-controlled Personal Information (including Portal user account information) may be submitted to: system@authi.com.

11.2. Assistance: Authi will respond to access and correction requests it receives in accordance with the Privacy Act, and will reasonably assist the User with requests where the request relates to information Authi holds about the User's account or Campaign records, subject to the Data Retention and Deletion section.

12. Audit and Information

12.1. Information: On reasonable request, Authi will provide information reasonably necessary to demonstrate compliance with this DPA (for example, security summaries, policies, or independent assurance materials when available).

12.2. Limitations: Any audit or review must be conducted on reasonable notice, during business hours, and in a manner that does not unreasonably interfere with Authi's operations. Authi may require that audits be limited to documentation review unless there is a reasonable basis to believe a material non-compliance exists.

13. Liability

This section is governed by the Master Terms.

Schedule 1 - Processing Overview

This Schedule provides a high-level overview of Personal Information processed by Authi in connection with the Services.

Categories of Personal Information

1. **User Portal account data**: names, email addresses, business contact details, roles and permissions, authentication data (excluding password contents), and audit logs relating to access and use of the Authi Portal.

2. **Support communications**: emails and other communications sent to or from Authi support, and any attachments or information provided by the User in connection with support requests.

3. **Business and operational records**: Campaign configuration details, content settings, terminal or deployment identifiers, billing and contact details, and Campaign performance and interaction records, processed in aggregated and/or de-identified form and/or as non-personal operational records.

Purposes of Processing

1. Provision, operation, and maintenance of the Services, including the Authi Portal and reporting features.

2. Account provisioning, authentication, access control, and audit logging.

3. User support and service communications.

4. Security, fraud prevention, abuse monitoring, and incident detection and response.

5. Reconciliation, administration, and operational record-keeping relating to the Services.

6. Aggregated and/or de-identified analytics, benchmarking, and product improvement, as described in the Use, Sharing, and Aggregation section of this DPA.

Locations of Processing

Primary hosting and processing locations are Google Cloud Platform regions in Australia, with Authi operational access and support from Auckland, New Zealand.

Retention

Personal Information is retained in accordance with the Data Retention and Deletion section of this DPA, including:

1. Retention of operational and security records for minimum periods reasonably required for security, auditability, dispute management, and legal or compliance obligations.

2. Deletion or anonymisation of User Portal Personal Information upon request or account termination, where reasonably practicable and subject to applicable exceptions.

3. Indefinite retention of aggregated and/or de-identified data that does not identify any individual.