

CompliGUARD Pty. Ltd.

DATA PROCESSING ADDENDUM

Effective Date: 29 October 2026 | Version 1.1

This Data Processing Addendum ("**DPA**") forms part of, and is subject to, the CompliGUARD Terms and Conditions (or Master Services Agreement in the case of an Enterprise plan) between CompliGUARD Pty Ltd t/a CompliGUARD ("**CompliGUARD**") and Customer that references this DPA (the "**Agreement**"). This DPA is effective on the Effective Date of the Agreement.

This DPA applies where, and to the extent that, CompliGUARD processes Customer Personal Data as Processor, on behalf of Customer acting as Controller, when providing Services under the Agreement. All capitalised terms not defined in this DPA shall have the meanings set forth in the Agreement.

Without prejudice to the foregoing, CompliGUARD and the Customer may have access to personal data of natural persons acting as contact points, provided by the other party including employees, representatives or agents, which it may process as Controller in the context of the proper performance of this Agreement. Each party is responsible for informing data subjects whose personal data it has disclosed of the processing carried out by the other party and of the provisions of this DPA.

1. Definitions

Term	Definition
Australian Privacy Laws	The Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs) contained therein, together with any applicable state or territory privacy legislation.
Data Breach	Any unauthorised or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data.
Data Controller or Controller	An entity that determines the purposes and means of the processing of Personal Data.
Data Processor or Processor	An entity that processes Personal Data under the instructions and on behalf of a Data Controller.
Notifiable Data Breach	A Data Breach that is likely to result in serious harm to one or more individuals, as defined under Part IIIC of the Privacy Act 1988 (Cth).
Personal Data	Information or an opinion about an identified individual, or an individual who is reasonably identifiable, as defined under Australian Privacy Laws.

Term	Definition
Processing	Any operation or set of operations performed on Personal Data, including collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, alignment, restriction, erasure, or destruction.
Services	The AI-powered compliance infrastructure services provided by CompliGUARD, including health marketing content assessment against TGA, AHPRA, FSANZ, and ACCC regulatory frameworks, as described in the Agreement.
Sub-Processor	Any Data Processor engaged by CompliGUARD or its affiliates to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA.

2. Relationship with the Agreement

2.1 This DPA shall replace any existing DPA or other data protection provisions the parties may have previously entered into in connection with the Services.

3. Scope of this DPA

3.1 This DPA applies where and only to the extent that CompliGUARD processes Personal Data on behalf of Customer in the course of providing Services pursuant to the Agreement, and where such processing is subject to Australian Privacy Laws or any other applicable data protection legislation.

4. Parties' Qualification

4.1 As part of the provision of Services under this Agreement, CompliGUARD processes Customer Personal Data under the instructions and on behalf of the Customer.

4.2 Customer is the Data Controller of Customer Personal Data. CompliGUARD is the Data Processor acting on behalf of Customer.

5. Customer's Obligations

5.1 Customer agrees that (i) it will comply with its obligations as a Data Controller under Australian Privacy Laws in respect of its processing of Customer Personal Data and any processing instructions it issues to CompliGUARD; and (ii) it ensures that the processing is lawful so that CompliGUARD can

process Customer Personal Data pursuant to the Agreement and this DPA and in compliance with applicable privacy laws.

5.2 It is the Customer's responsibility to provide appropriate privacy notices to data subjects at the time of collection of their Personal Data, as required by the APPs.

5.3 Customer agrees not to provide CompliGUARD with sensitive information (as defined under the Privacy Act 1988) unless strictly necessary for the provision of Services, and in any event only where doing so is lawfully permitted. The Customer warrants that any Personal Data (including any sensitive information) provided to CompliGUARD will be collected, used and disclosed in accordance with Australian Privacy Laws.

6. CompliGUARD's Obligations

6.1 CompliGUARD will process Customer Personal Data in accordance with Customer's documented instructions. Customer agrees that this DPA, the Agreement, any subsequent statements of work or service orders agreed in writing between the parties, and any Services configurations made by Customer or its authorised users comprise Customer's complete instructions to CompliGUARD regarding the Processing of Customer Personal Data. Any additional or alternate instructions must be agreed between the parties in writing.

6.2 CompliGUARD is not responsible for determining if Customer's instructions are compliant with applicable law. However, if CompliGUARD reasonably believes a Customer instruction infringes applicable Privacy Laws, CompliGUARD shall notify Customer as soon as reasonably practicable and shall not be required to comply with such infringing instruction.

6.3 Details of Data Processing

Details of Data Processing — which refer to Customer Personal Data submitted to the Services by the Customer — are set forth in Exhibit B.

Customer will provide CompliGUARD in writing with reasonable prior notice if it intends to make any changes to the aforementioned Data Processing, including but not limited to Customer Personal Data processed. If needed, Exhibit B will be amended accordingly.

6.4 Register of Categories of Personal Data Processing Activities

CompliGUARD undertakes to maintain appropriate records of all categories of Customer Personal Data Processing activities carried out on behalf of Customer, in accordance with applicable privacy law obligations. CompliGUARD shall provide Customer with related information as contained in the relevant register upon reasonable written request.

7. Sub-Processing

7.1 Authorised Sub-Processors. Customer agrees that in order to provide the Services, CompliGUARD may engage Sub-Processors to process Customer Personal Data. CompliGUARD maintains a list of its authorised Sub-Processors, accessible at compliguard.com.au/sub-processors, and Customer authorises CompliGUARD to rely on these Sub-Processors. The list of Sub-Processors applicable as of the Effective Date of the Agreement is attached hereto as Exhibit D.

7.2 Sub-Processor Obligations. Where CompliGUARD is authorised to rely on Sub-Processors:

- (a) CompliGUARD will enter into a written agreement with the Sub-Processor imposing data protection terms substantially similar to those contained in this DPA and that require the Sub-Processor to protect Customer Personal Data to the standard required by applicable Privacy Laws; and
- (b) CompliGUARD will remain responsible for the compliance of the Sub-Processor with the obligations of this DPA.

7.3 New Sub-Processors. CompliGUARD will provide Customer with ten (10) days prior notice if it intends to make any changes to its Sub-Processors list. Customer may object in writing during this period to CompliGUARD's appointment of a new Sub-Processor, provided that such objection is based on reasonable grounds relating to data protection. Objections may be sent to privacy@compliguard.com.au. In such event, the parties will discuss such concerns in good faith with a view to achieving resolution. If this is not possible, Customer may suspend or terminate the Agreement (without prejudice to any fees incurred prior to suspension or termination).

8. Security Measures and Data Breach Response

8.1 Security Measures. CompliGUARD has implemented and will maintain appropriate technical and organisational security measures to protect Customer Personal Data from Security Incidents and to preserve the security and confidentiality of Customer Personal Data ("Security Measures"). The latest Security Measures applicable to the Services are described in Exhibit C and are available at compliguard.com.au/security.

8.2 Updates to Security Measures. Customer is responsible for reviewing the information made available by CompliGUARD relating to data security and for making an independent determination as to whether the Services meet Customer's requirements and legal obligations under applicable Privacy Laws. CompliGUARD may update or modify the Security Measures from time to time provided that such updates maintain a similar or higher level of protection.

8.3 Personnel. CompliGUARD restricts its personnel from processing Customer Personal Data without authorisation, and shall ensure that any person authorised to process Customer Personal Data is under an appropriate obligation of confidentiality.

8.4 Customer Responsibilities. Notwithstanding the above, Customer is responsible for its secure use of the Services, including: (i) protecting account authentication credentials; (ii) protecting the security of Customer Data when in transit to and from the Services; (iii) implementing appropriate backup measures; and (iv) taking appropriate steps to encrypt, anonymise or pseudonymise any Customer Personal Data uploaded to CompliGUARD's Services.

8.5 Data Breach Response. Upon becoming aware of a Notifiable Data Breach affecting Customer Personal Data, CompliGUARD will notify Customer without undue delay, and in any event as required under the Privacy Act 1988. CompliGUARD will provide information to Customer relating to the Data Breach and will take reasonable steps to mitigate and, where possible, remedy the effects of any Data Breach.

9. Cross-Border Data Transfers

9.1 CompliGUARD may transfer and process Customer Personal Data to its Sub-Processors that maintain data processing operations outside Australia. CompliGUARD will at all times ensure that such transfers comply with the requirements of Australian Privacy Principle 8 (APP 8) and any applicable cross-border data transfer obligations under the Privacy Act 1988, including by ensuring that overseas recipients are subject to binding privacy obligations at least equivalent to the APPs.

9.2 Customer hereby consents to processing of Customer Personal Data in the countries set out in Exhibit D (List of Sub-Processors), as necessary to provide the Services. Countries where Sub-Processors may process data include the United States and the European Union.

10. Return or Deletion of Data

10.1 Upon termination or expiration of the Agreement, CompliGUARD shall (at Customer's election):

- (a) delete or return to Customer all Customer Personal Data in its possession or control in accordance with the terms of the Agreement; or
- (b) make available to the Customer the ability to export or retrieve Customer Personal Data.

This requirement shall not apply to the extent CompliGUARD is required by applicable law to retain some or all of the Customer Personal Data, or to Customer Personal Data that CompliGUARD has archived on back-up systems, provided that CompliGUARD shall securely isolate and protect such Customer Personal Data from any further processing except to the extent required by law.

11. Cooperation

11.1 To the extent that Customer is unable to independently access the relevant Customer Personal Data within the Services, CompliGUARD shall (at Customer's expense) provide reasonable cooperation to assist Customer to respond to any requests from individuals or applicable privacy authorities relating to the processing of Customer Personal Data under the Agreement. In the event that any such request is

made directly to CompliGUARD, CompliGUARD will forward the request to Customer and will not respond to such communication directly, unless legally required to do so.

11.2 If a law enforcement agency sends CompliGUARD a demand for Customer Personal Data, CompliGUARD will attempt to redirect the law enforcement agency to request that data directly from Customer. CompliGUARD will notify Customer of such demands where legally permitted. If compelled to disclose Customer Personal Data to a law enforcement agency, CompliGUARD will give Customer reasonable notice to allow Customer to seek a protective order or other appropriate remedy, unless legally prohibited from doing so.

11.3 To the extent reasonably required, CompliGUARD will provide information regarding the Services to enable Customer to carry out privacy impact assessments or prior consultations with privacy authorities as required by applicable law.

12. Liability

12.1 Any claims or remedies the Customer may have against CompliGUARD arising under or in connection with this DPA, including (i) breach of this DPA; (ii) regulatory penalties imposed upon Customer; and (iii) claims under applicable Privacy Laws including claims relating to damages paid to a data subject, will be subject to the limitation of liability provisions (including any agreed aggregate financial cap) that apply under the Agreement. Customer shall defend, indemnify and hold harmless CompliGUARD and its directors, officers, employees, representatives, and agents from and against any claims, liabilities, damages, fines, penalties and expenses including reasonable legal fees arising out of or in connection with violation by the Customer of any applicable Privacy Laws.

12.2 Any claims against CompliGUARD under this DPA shall be brought solely against the entity that is a party to the Agreement.

13. Governing Law

13.1 This DPA will be governed by and construed in accordance with the laws of South Australia, and the parties submit to the non-exclusive jurisdiction of the courts of South Australia. This is without prejudice to any mandatory obligations arising under Australian Privacy Laws.

14. Severability

14.1 The provisions of this DPA are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability shall affect only such phrase, clause or provision, and the rest of this DPA shall remain in full force and effect.

15. Miscellaneous

15.1 No one other than a party to this DPA, their successors and permitted assignees shall have any right to enforce any of its terms.

15.2 Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict.

EXHIBIT A: Privacy Contact Details

Customers may contact CompliGUARD regarding privacy and data protection matters as follows:

- By email: privacy@compliguard.com.au
- By post: CompliGUARD Pty Ltd t/a CompliGUARD, Attn: Chris Sarandis, 9 Wycombe Drive, Mount Barker South Australia
- Through the privacy portal: compliguard.com.au/privacy

EXHIBIT B: Data Processing Details

This exhibit details the data processing where CompliGUARD (“Data Processor”) processes Customer Personal Data on behalf of Customer (“Controller”) to provide Services under the Agreement.

A. List of Parties

- Data Importer: Customer (as identified in the Agreement)
- Data Exporter: CompliGUARD Pty Ltd t/a CompliGUARD (Data Processor)

B. Data Processing Details

Data subjects	Customer’s marketing team members, compliance personnel, authorised users, and other personnel whose data is included in health marketing content submitted for review.
Customer Personal Data Categories	User account information (name, email, role); health marketing content and promotional materials submitted for compliance assessment; product and SKU information; query data and assessment records; IP addresses and usage logs.
Special categories	None. Customers must not submit sensitive health information about identifiable individuals. Assessment content relates to health product marketing, not individual health records.
Transfer frequency	Customer Personal Data is transferred on a continuous basis whenever

	Customer submits content for assessment or accesses the Services.
Nature and purpose	AI-powered assessment of health marketing content against TGA · AHPRA · FSANZ · ACCC regulatory frameworks; delivery of compliance reports; proactive regulatory monitoring (Tier 2+); account management and service delivery.
Duration	The duration of processing corresponds to the term of the Agreement, subject to Section 11 (Return or Deletion of Data).
Processing operations	Collection, storage, transmission to AI sub-processors for assessment, analysis, report generation, archiving, deletion.

EXHIBIT C: Security Measures

Security Measures maintained by CompliGUARD to protect Customer Personal Data include:

- Encryption in transit (TLS 1.2+) and at rest (AES-256) for all Customer Personal Data
- Supabase authentication with role-based access controls and MFA
- Anthropic (Claude API) under its standard commercial terms — no training use of submitted content; automatic deletion by Anthropic within 30 days
- Airtable: SOC 2 Type 2 and ISO/IEC 27001-certified provider; access restricted to authorised CompliGUARD personnel
- n8n workflow automation with environment variable secrets management
- Annual security reviews of critical third-party vendors
- Weekly application security scans, with findings reviewed and remediated
- Incident response and Notifiable Data Breach procedures per Part IIIC Privacy Act 1988

Current and updated Security Measures are available at compliguard.com.au/security.

EXHIBIT D: List of Sub-Processors

The Sub-Processors authorised to process Customer Personal Data in connection with CompliGUARD’s Services as of the Effective Date are described in the CompliGUARD Sub-Processors Notice, available at compliguard.com.au/sub-processors and attached as a separate document to this DPA.