1. PRELIMINARY PROVISIONS

1.1. Document Title and Version Control

1.1.1. This document is titled Global Privacy Policy (GDPR + Australian Privacy Act) — Digital Services App (**Policy**).

1.1.2. This Policy applies from the Effective date stated above.

1.1.3. Version control:

(a) **Major version changes** (e.g. 1.0 to 2.0) apply where there are material changes to: (a) categories of Personal Data collected; (b) Purposes of Processing; (c) Legal Bases; (d) International Transfers safeguards; or (e) Data Subject Rights handling.

(b) **Minor version changes** (e.g. 1.0 to 1.1) apply for non-material changes, including clarifications, formatting, and administrative updates.

1.1.4. We maintain an internal change log recording: (a) version number; (b) date of change; (c) summary of changes; and (d) approvals.

1.1.5. Update notification procedures:

(a) If changes are **material**, we notify Users through in-app notice and/or email (where we hold an email address) before the changes take effect, unless an urgent change is required for security or legal compliance (see section 17.4).

(b) If changes are **non-material**, we may update this Policy by publishing the revised version in-app and on our website (if applicable).

1.1.6. Where the GDPR applies, this Policy is intended to meet the transparency requirements in **Articles 12, 13 and 14** of Regulation (EU) 2016/679 (GDPR). Where Australian law applies, this Policy is intended to support compliance with the ***Privacy Act 1988*** **(Cth)** and the Australian Privacy Principles (**APPs**).

1.2. Scope and Application

1.2.1. This Policy describes how we collect, hold, use, disclose, store, secure, transfer and otherwise process Personal Data when we provide our digital services app and related services (**Services**).

1.2.2. This Policy applies to:

(a) Individuals who download, access or use the app (**Users**);

(b) prospective Users who interact with our marketing or onboarding flows;

(c) individuals who communicate with us (including customer support); and

(d) individuals whose Personal Data we receive from third parties (where permitted).

1.2.3. Territorial scope:

(a) Where the GDPR applies (including where we offer Services to individuals in the European Economic Area (EEA) and/or monitor their behaviour within the EEA), we process Personal Data in accordance with the GDPR.

(b) Where the *Privacy Act 1988* (Cth) applies, we handle Personal Information in accordance with the APPs.

1.2.4. This Policy is intended to operate as a single, cohesive global privacy policy. Where local law imposes additional requirements, section 18 applies.

1.2.5. This Policy does not cover third-party services that Users may access via links or integrations unless we expressly state otherwise. Users should review the privacy policies of those third parties.

2. DEFINITIIONS AND INTERPRETATION

2.1. GDPR-Specific Definitions

In this Policy, unless the context otherwise requires:

2.1.1. Automated decision-making has the meaning given in *Article 22 GDPR* and includes decisions based solely on automated

processing that produce legal effects concerning a Data Subject or similarly significantly affect a Data Subject.

2.1.2. **Controller** has the meaning given in *Article 4(7) GDPR* and refers to the entity that determines the purposes and means of the Processing of Personal Data

2.1.3. **Data Subject** has the meaning given in the GDPR and refers to an identified or identifiable natural person to whom Personal Data relates.

2.1.4. **EEA** means the European Economic Area.

2.1.5. **GDPR** means Regulation (EU) 2016/679 (General Data Protection Regulation).

2.1.6. **Personal Data** has the meaning given in *Article 4(1) GDPR* and means any information relating to an identified or identifiable natural person.

2.1.7. **Processing** has the meaning given in *Article 4(2) GDPR* and includes any operation performed on Personal Data, whether or not by automated means (including collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, alignment, restriction, erasure or destruction).

2.1.8. **Processor** has the meaning given in *Article 4(8) GDPR* and refers to an entity that processes Personal Data on behalf of the Controller.

2.1.9. **Profiling** has the meaning given in *Article 4(4) GDPR.*

2.1.10. **Pseudonymisation** has the meaning given in *Article 4(5) GDPR*.

2.1.11. **Special Categories of Personal Data** has the meaning given in *Article 9 GDPR*.

2.1.12. **Supervisory Authority** has the meaning given in *Article 4(21) GDPR.*

2.1.13. **UK GDPR** means the retained version of the GDPR in the United Kingdom (if applicable to our operations).

2.1.14. **Standard Contractual Clauses** or **SCCs** means standard data protection clauses adopted by the European Commission for transfers of Personal Data to third countries pursuant to *Article 46(2)(c) GDPR*, as amended, replaced or superseded from time to time.

2.1.15. **Transfer** includes a disclosure or making available of Personal Data to a recipient in a country outside the EEA.

2.2. Australian Privacy Act Definitions

2.2.1. **APPs** means the Australian Privacy Principles in Schedule 1 to the *Privacy Act 1988 (Cth)*.

2.2.2. **Australian Privacy Act** means the *Privacy Act 1988 (Cth)*.

2.2.3. **Collect** has the meaning given in the Australian Privacy Act and includes gathering, acquiring or obtaining Personal Information from any source and by any means.

2.2.4. **Consent** under Australian privacy law means express or implied consent, depending on context; where we rely on Consent for GDPR purposes, we apply the GDPR standard (freely given, specific, informed and unambiguous, and explicit where required).

2.2.5. **Disclosure** has the meaning given in the Australian Privacy Act and includes making Personal Information accessible or visible to others outside our effective control.

2.2.6. **Overseas recipient** has the meaning used in APP 8 and includes a recipient located outside Australia.

2.2.7. **Personal Information** has the meaning given in the Australian Privacy Act and means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether true or not and whether recorded in a material form or not.

2.2.8. **Sensitive Information** has the meaning given in the Australian Privacy Act and includes (among other things) health information and certain other categories requiring higher protection.

2.2.9. **Use** has the meaning given in the Australian Privacy Act and includes handling Personal Information within our organisation.

2.3. Digital Services Terminology

2.3.1. **App** means our mobile application and any associated software development kits (SDKs) and application programming interfaces (APIs) we provide or use to deliver the Services.

2.3.2. **Account** means a User account created to access the Services.

2.3.3. **Device Information** means information about a User's device and software environment, including device identifiers, operating system, app version, language, and network information.

2.3.4. **Location Data** means data indicating a User's location, including precise geolocation (where enabled) and approximate location derived from IP address or device settings.

2.3.5. **Usage Data** means data about how Users interact with the App and Services, including feature usage, session events, clicks/taps, screens viewed, and performance telemetry.

2.3.6. **Cookies** means small text files and similar technologies stored on a device, including SDK identifiers, mobile advertising identifiers, local storage objects, and other tracking technologies (as applicable in an app context).

2.3.7. **Tracking Technologies** means Cookies and other technologies, whether predictive or based on determinations made by artificial intelligence, used to recognise devices, store preferences, measure performance, prevent fraud, and personalise content and advertising (where applicable).

2.4. Interpretation Clauses

2.4.1. Headings are for convenience only and do not affect interpretation.

2.4.2. A reference to:

(a) a person includes an individual, body corporate, partnership, joint venture, association, government agency and any other entity;

(b) a statute or regulation includes any subordinate legislation and any amendment, consolidation, re-enactment or replacement;

(c) "including" means "including without limitation".

2.4.3. Where a term is defined both under the GDPR and the Australian Privacy Act, the meaning applicable depends on the context and the jurisdictional application described in section 1.3.

2.4.4. If there is an inconsistency between this Policy and a specific in-app notice presented at the time of collection for a particular feature, the in-app notice prevails to the extent of the inconsistency for that feature (subject to section 18.3).

3. CONTROLLER IDENTIFICATION AND CONTACT DETAILS

3.1. Data Controller Information (Article 13(1)(a) GDPR)

3.1.1. For GDPR purposes, the **Controller** of Personal Data processed under this Policy is:

(a) **Controller name:** InnerPiece Pty Ltd

(b) **ACN:** 689 982 885

(c) **Registered office:** 8 Piccadilly Crescent, Piccadilly SA, Australia.

3.1.2. **Principal place of business:** 8 Piccadilly Crescent, Piccadilly SA, Australia.

3.1.3. Where we act as a **Processor** for a business customer (for example, where the App is offered under an enterprise arrangement and we process Personal Data on the customer's instructions), we will identify that customer as Controller in the relevant contract and/or in-product notices, and this Policy applies to the extent we act as Controller.

3.2. Contact Information

3.2.1. Policy contact channels:

(a) **Email:** Contact@innerpieceapp.com

(b) **Postal address:** 8 Piccadilly Crescent, Piccadilly SA, Australia

(c) **Telephone:** +61413555148

3.2.2. Users may contact us to:

(a) ask questions about this Policy;

(b) exercise rights under section 6;

(c) make a complaint under section 16; or

(d) request further information about safeguards for International Transfers under section 7.

3.3. Data Protection Officer Details

3.3.1. **Data Protection Officer (DPO):** We have not appointed a DPO.

4. CATEGORIES OF PERSONAL DATA COLLECTED

4.1. Account Registration Data

4.1.1. We may collect the following **Account Registration Data** when a User creates or manages an Account:

(a) name (or preferred name);

(b) date of birth;

(c) email address;

(d) mobile number (if required for verification or account security);

(e) username and profile details (where provided);

(f) authentication credentials (e.g. password, password hash, or authentication tokens);

(g) account status and administrative metadata (e.g. creation date, last login).

4.1.2. Where we use third-party sign-in (e.g. “Sign in with Apple/Google”), we may receive identifiers and basic profile information from that provider, depending on the User’s settings with that provider.

4.2. Device and Technical Information

4.2.1. We may collect **Device and Technical Information**, including:

(a) device type and model;

(b) operating system and version;

(c) App version and build;

(d) device identifiers and app instance identifiers;

(e) IP address;

(f) network and connectivity information;

(g) language, time zone, and regional settings;

(h) crash logs and diagnostic data.

4.2.2. We use this information to deliver the Services, maintain security, troubleshoot issues, and improve performance.

4.3. Usage and Analytics Data

4.3.1. We may collect **Usage and Analytics Data**, including:

(a) interactions with features and screens;

(b) timestamps, session duration, and navigation paths;

(c) events such as clicks/taps, scrolls, and conversions;

(d) in-app search queries (if provided);

(e) performance telemetry (e.g. latency, load times);

(f) aggregated or pseudonymised analytics outputs.

4.3.2. Collection methods may include in-app analytics SDKs, server logs, and event tracking configured within the App.

4.4. Location Information

4.4.1. We may collect **Location Data** where it is required for a feature or where a User enables it, including:

(a) **precise geolocation** (e.g. GPS) where the User grants device permission;

(b) **approximate location** derived from IP address or device settings.

4.4.2. Location Data may be treated as sensitive in practice due to its potential to reveal patterns and behaviours. We apply enhanced controls (see sections 9 and 10).

4.4.3. Users can generally control precise location collection via device settings and in-app controls (see section 14.2).

4.5. Communications and Content Data

4.5.1. We may collect **Communications and Content Data**, including:

(a) Messages, images and other content Users submit through the App (where the Services include messaging, posting, uploads, or forms);

(b) customer support communications (including email, in-app chat, and call notes);

(c) voice recordings (which are transcript using artificial intelligence and deleted immediately after transcription);

(d) feedback, ratings, and survey responses;

(e) attachments and metadata associated with communications.

4.5.2. We do not request that Users provide Special Categories of Personal Data or Sensitive Information through general free-text fields. If Users choose to provide such information, we handle it in accordance with applicable law and this Policy.

4.6. Marketing and Preferences Data

4.6.1. We may collect **Marketing and Preferences Data**, including:

(a) marketing communication preferences (email, SMS, push notifications);

(b) consent records (including timestamp, method, and scope);

(c) campaign interaction data (opens, clicks, opt-outs);

(d) preference settings within the App.

4.6.2. Where required by law, we will obtain Consent before sending direct marketing communications, and we provide opt-out mechanisms (see section 13).

5. PURPOSES OF PROCESSING AND LEGAL BASIS

5.1. Service Provision (Article 6(1)(b) GDPR)

5.1.1. We process Personal Data as necessary to perform a contract with the User or to take steps at the User's request prior to entering into a contract, including to:

(a) create and administer Accounts;

(b) provide core App functionality and deliver requested digital services;

(c) authenticate Users and manage sessions;

(d) provide customer support and respond to enquiries;

(e) process transactions or service requests initiated by the User (where applicable); and

(f) send service-related communications (e.g. security alerts, transactional messages, changes to the Services).

5.1.2. Under Australian law, we collect Personal Information only where reasonably necessary for our functions or activities (APP 3), and we take reasonable steps to notify Users of collection matters (APP 5).

5.2. Legitimate Interests Processing (Article 6(1)(f) GDPR)

5.2.1. We may process Personal Data where it is necessary for our legitimate interests (or those of a third party), except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject.

5.2.2. Our legitimate interests include:

(a) **security and fraud prevention**, including detecting suspicious activity, preventing unauthorised access, and maintaining the integrity of the App;

(b) **service improvement**, including debugging, performance monitoring, and developing new features;

(c) **analytics and measurement**, including understanding how Users engage with the Services to improve user experience;

(d) **business operations**, including internal reporting, forecasting, and corporate governance;

(e) **legal risk management**, including establishing, exercising or defending legal claims.

5.2.3. Where we rely on legitimate interests, we implement safeguards such as data minimisation, access controls, and (where appropriate) pseudonymisation (see section 10).

5.2.4. Users have the right to object to Processing based on legitimate interests (section 6.6).

5.3. Consent-Based Processing (Article 6(1)(a) GDPR)

5.3.1. We rely on Consent where required by law or where we choose to do so, including for:

(a) optional features that require additional permissions (e.g. precise location, contacts, photos/media);

(b) direct marketing in jurisdictions requiring opt-in;

(c) certain Cookies/Tracking Technologies (see section 9); and

(d) personalised advertising and profiling (where applicable and where required).

5.3.2. Where we rely on Consent:

(a) Users may withdraw Consent at any time (section 6.8);

(b) withdrawal does not affect the lawfulness of Processing before withdrawal; and

(c) we provide in-app controls and/or device-level controls to manage permissions.

5.4. Legal Compliance Processing (Article 6(1)(c) GDPR)

5.4.1. We may process Personal Data where necessary to comply with a legal obligation, including to:

(a) comply with lawful requests and legal processes;

(b) meet record-keeping obligations;

(c) comply with regulatory requirements applicable to our operations.

5.4.2. Under Australian law, we may use or disclose Personal Information where required or authorised by law (including under APP 6).

5.5. Vital Interests and Public Tasks

5.5.1. We may process Personal Data where necessary to protect the vital interests of a Data Subject or another person (*Article 6(1)(d) GDPR*), for example in urgent situations involving safety.

5.5.2. We do not generally process Personal Data to perform a task carried out in the public interest or in the exercise of official authority (*Article 6(1)(e) GDPR*), unless explicitly stated for a particular feature or regulatory context.

5.6. Business Purposes for Collection and Use (California)

5.6.1. Where we collect and use Personal Information of California consumers, we do so for the following business purposes:

(a) providing the Services, including creating and administering Accounts, authenticating Users, managing sessions, and delivering core App functionality;

(b) maintaining and servicing accounts, including processing transactions or service requests and providing customer support;

(c) providing analytic services, including understanding how Users engage with the Services to improve user experience, debugging, and performance monitoring;

(d) undertaking internal research for technological development and demonstration;

(e) undertaking activities to verify or maintain the quality and safety of the Services, and to improve, upgrade, or enhance the Services;

(f) detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that;

(g) short-term, transient use, where the Personal Information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction;

(h) performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, and providing similar services; and

(i) sending service-related communications, including security alerts, transactional messages, and changes to the Services.

5.7. Commercial Purposes (California)

5.7.1. We may also use Personal Information for the following commercial purposes:

(a) marketing and advertising, including delivering and measuring campaigns

(b) personalised advertising and profiling, where applicable and where the consumer has not opted out;

(c) campaign interaction measurement, including opens, clicks, and opt-outs.

5.8. Recharacterization of Legitimate Interests Processing for California Consumers:

5.8.1. The processing activities described in section 5.7 are, for California consumers, undertaken for the following purposes:

(a) Security and fraud prevention: This constitutes a business purpose of detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible.

(b) Service improvement and debugging: This constitutes a business purpose of undertaking activities to verify or maintain the quality and safety of the Services, and to improve, upgrade, or enhance the Services.

(c) Analytics and measurement: This constitutes a business purpose of providing analytic services. However, to the extent that analytics data is used for cross-context behavioural advertising or is shared with third parties for advertising purposes, this may constitute "sharing" under California law, and the consumer's right to opt out applies (see section [new opt-out section]).

(d) Business operations: This constitutes a business purpose of performing services on behalf of the business, including internal reporting, forecasting, and corporate governance.

(e) Legal risk management: This constitutes processing that is reasonably necessary and proportionate to establish, exercise, or defend legal claims, or to comply with legal obligations.

5.9. Consent and Opt-Out Framework for California Consumers

5.9.1. Opt-out model for sale and sharing: Where we sell or share (as those terms are understood under California privacy law) the Personal Information of California consumers, consumers have the right to opt out. We do not require consumers to opt in to the sale or sharing of their Personal Information, except as described in paragraph (c) below.

5.9.2. Sensitive personal information: Where we collect or use sensitive personal information of California consumers (including precise geolocation data as described in section 4.4, and account log-in credentials as described in section 4.1.1(e)), consumers have the right to limit our use and disclosure of such information to purposes that are reasonably necessary and proportionate to provide the Services. We provide a

mechanism for consumers to exercise this right [see new section reference].

5.9.3. Minors: We do not knowingly sell or share the Personal Information of consumers under the age of 16 without affirmative authorisation. For consumers aged 13 to 15, we obtain opt-in consent before selling or sharing their Personal Information. For consumers under 13, we obtain verifiable parental consent.

5.9.4. Financial incentives: If we offer financial incentive programmes (such as loyalty programmes, discounts, or other benefits in exchange for the collection, retention, sale, or sharing of Personal Information), we will provide a notice explaining the material terms of the programme, obtain opt-in consent, and allow consumers to opt out at any time.

5.10. Sale and Sharing of Personal Information (California)

5.10.1. We disclose Personal Information to the categories of third parties described in section 11 of this Policy. Some of these disclosures may constitute a "sale" or "sharing" of Personal Information under California privacy law.

5.10.2. The following disclosures may constitute "sharing" for cross-context behavioural advertising:

(a) disclosure of device identifiers and usage data (to advertising technology partners for the purpose of personalised advertising;

(b) disclosure of campaign interaction data to marketing partners for campaign measurement and optimisation.

(c) California Users have the right to opt out of the sale and sharing of their Personal Information pursuant to the terms and processes set out in this Policy;

(d) we do not sell or share the Personal Information of consumers we know to be under the age of 16 without affirmative authorisation as described in section 5.9.3;

(e) we do not use or disclose sensitive personal information for purposes other than those reasonably necessary to provide the Services, unless the consumer has not exercised their right to limit such use.

5.11. Purpose Limitation (California)

5.11.1. We do not collect additional categories of Personal Information or use Personal Information collected for additional purposes

that are materially different from, or incompatible with, the purposes described in this Policy without providing California consumers with notice.

5.11.2. Where we intend to use previously collected Personal Information for a purpose materially different from the purpose for which it was collected, we will provide direct notice to the consumer and, where required, obtain consent before such use.

5.12. Service Provider, Contractor, and Third-Party Distinctions (California)

5.12.1. Where we disclose Personal Information to a service provider (as that term is understood under California privacy law), we enter into a written contract that:

(a) specifies the business purpose for which the Personal Information is disclosed;

(b) requires the service provider not to sell or share the Personal Information;

(c) requires the service provider not to retain, use, or disclose the Personal Information for any purpose other than the specified business purpose or as otherwise permitted;

(d) requires the service provider to comply with applicable California privacy obligations and to grant the business rights to take reasonable and appropriate steps to help ensure compliance; and

(e) requires the service provider to notify us if it can no longer meet its obligations.

5.12.2. Where we disclose Personal Information to a contractor, we enter into a written contract with substantially similar restrictions as described in section 5.12.1.

5.12.3. Where we disclose Personal Information to a third party (including marketing and advertising partners described in section 11.5), such disclosure may constitute a "sale" or "sharing" under California privacy law, and the consumer's right to opt out applies as described in section 5.10.

6. DATA SUBJECT RIGHTS

6.1. Right of Access (Article 15 GDPR)

6.1.1. Data Subjects may request confirmation as to whether we process their Personal Data and, where we do, request access to that Personal Data and information required by Article 15 GDPR.

6.1.2. Access requests may be made using the contact details in section 3.2 or via in-app tools where available.

6.1.3. We may request information to verify identity before providing access, particularly where disclosure could expose Personal Data to unauthorised parties.

6.1.4. Where feasible, we provide access in a secure electronic format.

6.2. Right to Rectification (Article 16 GDPR)

6.2.1. Data Subjects may request correction of inaccurate Personal Data and completion of incomplete Personal Data.

6.2.2. Users can rectify certain information directly in the App via account settings (section 14.2).

6.2.3. Where we have disclosed Personal Data to third parties, we take reasonable steps to notify those third parties of rectification where required by the GDPR and where practicable.

6.3. Right to Erasure (Article 17 GDPR)

6.3.1. Data Subjects may request erasure of Personal Data in the circumstances set out in *Article 17 GDPR*, including where:

(a) the Personal Data is no longer necessary for the purposes for which it was collected;

(b) the Data Subject withdraws Consent and there is no other legal basis;

(c) the Data Subject objects under *Article 21 GDPR* and there are no overriding legitimate grounds;

(d) the Personal Data has been unlawfully processed; or

(e) erasure is required to comply with a legal obligation.

6.3.2. Erasure is not absolute. We may retain Personal Data where an exception applies, including where Processing is necessary for:

(a) exercising the right of freedom of expression and information;

(b) compliance with a legal obligation;

(c) reasons of public interest in the area of public health (where applicable);

(d) archiving in the public interest, scientific or historical research, or statistical purposes (where applicable); or

(e) establishment, exercise or defence of legal claims.

6.3.3. Where erasure is granted, we apply secure deletion and de-identification practices consistent with section 8.4.

6.4. Right to Restrict Processing (Article 18 GDPR)

6.4.1. Data Subjects may request restriction of Processing in the circumstances set out in *Article 18 GDPR*, including where:

(a) accuracy is contested (restriction applies for a period enabling verification);

(b) Processing is unlawful and the Data Subject opposes erasure;

(c) we no longer need the Personal Data but it is required for legal claims; or

(d) the Data Subject has objected under *Article 21 GDPR* pending verification of overriding grounds.

6.4.2. Where Processing is restricted, we store the Personal Data and only process it with Consent or for limited purposes permitted by the GDPR.

6.5. Right to Data Portability (Article 20 GDPR)

6.5.1. Where *Article 20 GDPR* applies, Data Subjects may request to receive their Personal Data in a structured, commonly used and machine-readable format, and to transmit that data to another controller, where:

(a) Processing is based on Consent or contract; and

(b) Processing is carried out by automated means.

6.5.2. Portability applies to Personal Data provided by the Data Subject and does not adversely affect the rights and freedoms of others.

6.5.3. Where technically feasible, we may transmit the data directly to another controller at the Data Subject's request.

6.5.4. Our Services have functionality which allows a Data Subject to action an export of all their Personal Data.

6.6. Right to Object (Article 21 GDPR)

6.6.1. Data Subjects may object to Processing based on legitimate interests (*Article 6(1)(f) GDPR*) on grounds relating to their particular situation.

6.6.2. Where a valid objection is made, we stop Processing unless we demonstrate compelling legitimate grounds overriding the interests, rights and freedoms of the Data Subject, or the Processing is necessary for legal claims.

6.6.3. Data Subjects have an absolute right to object to Processing for direct marketing purposes. If a Data Subject objects, we stop Processing for direct marketing.

6.7. Rights Related to Automated Decision-Making (Article 22 GDPR)

6.7.1. Where applicable, Data Subjects have rights in relation to decisions based solely on automated processing, including profiling, that produce legal effects or similarly significantly affect them.

6.7.2. If we conduct such processing for a feature, we will provide:

(a) meaningful information about the logic involved;

(b) the significance and envisaged consequences; and

(c) the right to obtain human intervention, express a point of view, and contest the decision, where required by the GDPR.

6.7.3. We use automated decision making for Data security and these systems may apply restrictions and other limitations to Users accounts without input from a human decision maker. If a User's account is subject to an permanent ban that ban is not an automated decision and is the product of a human decision within our organisation.

6.8. Request Procedures and Response Timeframes

6.8.1. Requests may be submitted via:

(a) the contact details in section 3.2; and/or

(b) in-app privacy tools (where available).

6.8.2. We respond to GDPR rights requests within **one month** of receipt, subject to extensions permitted by the GDPR for complex or numerous requests.

6.8.3. We may refuse to act on a request where permitted by the GDPR (for example, where requests are manifestly unfounded or excessive), and in that case we will provide reasons and information about complaint rights.

6.8.4. Under the Australian Privacy Act, individuals may request access to and correction of Personal Information, and we respond within a reasonable period and in accordance with applicable requirements.

6.8.5. Identity verification: we may request additional information to verify identity and/or authority to act (e.g. where an agent submits a request).

6.8.6. Consent withdrawal mechanisms:

(a) Users can withdraw marketing consent via unsubscribe links, in-app settings, or by contacting us.

(b) Users can withdraw device permission-based consents (e.g. location) via device settings and in-app controls.

7. INTERNATIONAL DATA TRANSFERS

7.1. Transfers from EU to Australia

7.1.1. We are an Australian organisation and may store and process Personal Data in Australia and other locations where we or our service providers operate.

(a) Our service provides currently operate within the following regions:

7.1.1.a.1. Australia;

7.1.1.a.2. United States; and

7.1.1.a.3. Europe.

7.1.2. Where the GDPR applies and we transfer Personal Data from the EEA to Australia (a “third country”), we implement appropriate safeguards under *Chapter V GDPR* unless an exception applies.

7.1.3. We inform Data Subjects that Australia may not be the subject of an adequacy decision for all Processing contexts, and therefore we rely on safeguards described in section 7.2 and supplementary measures in section 7.3.

7.2. Standard Contractual Clauses Implementation

7.2.1. For relevant transfers, we use **Standard Contractual Clauses (SCCs)** approved by the European Commission as an appropriate safeguard under *Article 46 GDPR*.

7.2.2. SCCs are implemented:

(a) between us and relevant EEA-based exporters (where we receive Personal Data from an EEA entity); and/or

(b) between us and our Processors/Sub-processors where they receive or access EEA Personal Data.

7.2.3. We maintain contractual governance to ensure SCCs are:

(a) incorporated into relevant data processing agreements;

(b) flowed down to sub-processors where required; and

(c) supported by technical and organisational measures.

7.3. Additional Safeguards and Security Measures

7.3.1. In addition to SCCs, we apply supplementary measures appropriate to the risk profile of the transfer, which may include:

(a) encryption in transit and at rest;

(b) access controls, least privilege, and strong authentication;

(c) logging and monitoring of access to systems processing EEA Personal Data;

(d) data minimisation and pseudonymisation where feasible; and

(e) contractual commitments regarding government access requests, transparency, and challenge procedures to the extent legally permissible.

7.4. Transfer Impact Assessments

7.4.1. Where required, we conduct and maintain a **Transfer Impact Assessment** (**TIA**) process to evaluate:

(a) the nature of the Personal Data;

(b) the purposes of Processing;

(c) the likelihood and severity of risks to Data Subjects;

(d) the laws and practices of the destination country relevant to access by public authorities; and

(e) the effectiveness of SCCs and supplementary measures.

7.4.2. We review TIAs periodically and upon material changes to transfer arrangements.

7.5. Cross-Border Disclosure Under Australian Privacy Act

7.5.1. Where we disclose Personal Information to an overseas recipient, we take reasonable steps to ensure the overseas recipient does not breach the APPs in relation to the information (APP 8), unless an exception applies.

7.5.2. We may disclose overseas where:

(a) it is necessary to provide the Services (e.g. cloud hosting, support tooling);

(b) Users have consented (where required); or

(c) the disclosure is required or authorised by law.

7.5.3. We remain accountable for overseas disclosures to the extent required by the Australian Privacy Act.

7.5.4. We remain accountable for overseas disclosures to the extent required by the Australian Privacy Act.

8. DATA RETENTION POLICIES

8.1. General Retention Principles

8.1.1. We retain Personal Data only for as long as necessary to fulfil the purposes described in this Policy, unless a longer retention period is required or permitted by law.

8.1.2. Retention decisions consider:

(a) the nature and sensitivity of the data;

(b) the purposes of Processing;

(c) legal and regulatory requirements;

(d) limitation periods for legal claims;

(e) security and fraud prevention needs; and

(f) whether the data can be de-identified.

8.1.3. Where feasible, we de-identify or aggregate data rather than retain identifiable Personal Data.

8.1.4. If a User requests deletion of their Personal Data that request will be actioned such that any Personal Data we hold will be destroyed with in 30 calendar days.

8.2. Category-Specific Retention Periods

8.2.1. **Account Registration Data:** retained for the life of the Account and for a reasonable period after account closure to: (a) enable reactivation where requested; (b) address disputes; (c) comply with legal obligations; and (d) prevent fraud.

8.2.2. **Device and Technical Information:** retained for as long as needed for security, diagnostics, and service improvement, subject to periodic review and minimisation.

8.2.3. **Usage and Analytics Data:** retained for analytics and service improvement for a period proportionate to those purposes, with preference for aggregation and pseudonymisation.

8.2.4. **Location Data:** retained only as long as needed for the feature requiring it, with minimisation and user controls applied.

8.2.5. **Communications and Content Data:** retained for as long as needed to provide the Services, manage support, and maintain records of interactions, subject to deletion requests and legal holds.

8.2.6. **Marketing and Preferences Data:** retained until the User opts out or withdraws consent and thereafter retained only as necessary to maintain suppression lists and demonstrate compliance.

8.2.7. Where a User requests erasure, we apply section 6.3 and delete or de-identify data unless an exception applies.

8.3. Legal and Regulatory Retention Requirements

8.3.1. We may retain Personal Data to comply with legal obligations, including record-keeping obligations and responding to lawful requests.

8.3.2. Where we are subject to a legal hold (e.g. litigation or regulatory investigation), we preserve relevant data until the hold is lifted.

8.4. Secure Deletion Procedures

8.4.1. We implement secure deletion procedures appropriate to the storage medium and system architecture, which may include:

(a) logical deletion and secure wiping;

(b) cryptographic erasure where encryption is used;

(c) deletion from active systems and, within a reasonable cycle, from backups (or rendering backups inaccessible through key destruction);

(d) access restriction during backup retention cycles.

8.4.2 We maintain records of deletion activities where appropriate for accountability.

8.5. Retention Policy Reviews and Updates

8.5.1. We review retention settings and practices periodically and when:

(a) we introduce new features;

(b) we change service providers;

(c) applicable law changes; or

(d) we identify new risks through DPIAs/TIAs.

8.5.2. We update this Policy where retention practices change materially (section 17).

9. COOKIES AND TRACKING TECHNOLOGIES

9.1. Cookie Categories and Classification

9.1.1. In an app context, “cookies” may include mobile identifiers and SDK-based tracking. We classify Tracking Technologies as:

(a) **Strictly necessary**: required to provide core functionality, security, and session management.

(b) **Performance/analytics**: used to measure performance and understand usage.

(c) **Functionality**: used to remember preferences and enhance features.

(d) **Targeting/advertising**: used to personalise advertising and measure campaigns (where applicable).

9.1.2. Some Tracking Technologies may be first-party (set by us) or third-party (set by service providers integrated into the App).

9.2. Consent Management and Cookie Banners

9.2.1. Where required by applicable European law, we present Users with clear choices for non-essential Tracking Technologies, including:

(a) an initial notice identifying categories and purposes;

(b) the ability to accept or reject non-essential categories; and

(c) the ability to change preferences at any time via in-app settings.

9.2.2. We maintain consent records, including the scope of consent, timestamp, and method. We currently record the date and time consent and Data is provided in respect of the following:

(a) Terms of Service acceptance timestamp;

(b) Privacy Policy acceptance timestamp;

(c) Version of Terms of Service acceptance;

(d) Version of Privacy Policy accepted;

(e) Date of birth / age verification;

(f) Account creation timestamp;

(g) Account deletion request timestamp; and

(h) Push notification permission consent.

9.2.3. Where consent is withdrawn, we stop the relevant Tracking Technologies and/or cease related Processing to the extent required and technically feasible.

9.3. Third-Party Cookies and Tracking

9.3.1. We may use third-party service providers for analytics, crash reporting, performance monitoring, customer support, and (where applicable) advertising measurement.

9.3.2. Where third-party Tracking Technologies are used, we:

(a) identify the category and purpose in our cookie/tracking disclosures;

(b) ensure appropriate contractual protections; and

(c) configure settings to minimise data collection where feasible.

9.4. Alternative Tracking Technologies

9.4.1. We may use technologies including:

(a) SDK identifiers and app instance IDs;

(b) mobile advertising identifiers (where available and permitted);

(c) local storage and secure storage;

(d) pixels and similar technologies in emails (subject to marketing preferences); and

(e) device fingerprinting only where necessary for security and fraud prevention, and subject to applicable law.

9.5. User Control and Opt-Out Mechanisms

9.5.1. Users can control Tracking Technologies through:

(a) in-app privacy settings;

(b) device operating system privacy controls (including advertising identifier settings); and

(c) cookie/tracking consent tools (where presented).

9.5.2. Users can opt out of direct marketing at any time (section 13).

9.5.3. We use Tracking Technologies to maintain a safe and functional service, as a result users cannot disable certain Tracking Technologies as these are essential to maintaining the security and functionality of our App.

10. SECURITY MEASURES AND DATA PROTECTION

10.1. Technical Security Measures

10.1.1. We implement technical measures appropriate to risk, which may include:

(a) encryption in transit (e.g. TLS) and encryption at rest where appropriate;

(b) encryption which is aligned the requirements of our Service Providers (including the Apple App Store);

(c) secure key management;

(d) access controls and role-based access;

(e) secure authentication and session management;

(f) logging, monitoring, and alerting;

(g) secure software development practices, including code review and dependency management; and

(h) segregation of environments (development/test/production) and data minimisation in non-production environments.

10.2. Artificial Intelligence

10.2.1. We use artificial intelligence as described in this Policy to deliver the Services.

10.2.2. Our artificial intelligence Service Providers are commercially engaged such that Personal Data you provide in receiving the Services:

(a) is subject to the data processing terms of our artificial intelligence Service Providers; and

(b) is not permitted to be used by our artificial intelligence Service Providers for their internal training purposes.

10.3. Organisational Security Measures

10.3.1. We implement organisational measures including:

(a) staff training and confidentiality obligations;

(b) access provisioning and deprovisioning processes;

(c) vendor security due diligence (section 15.4);

(d) incident response planning (section 10.4);

(e) governance oversight (section 15.1).

10.4. Data Protection by Design and Default

10.4.1. We apply privacy-by-design and privacy-by-default principles, including:

(a) collecting only data necessary for stated purposes;

(b) using privacy-protective default settings;

(c) embedding security controls into feature design;

(d) conducting DPIAs where required (section 15.3).

10.5. Security Incident Response

10.5.1. We maintain processes to detect, investigate, contain, remediate, and document suspected or confirmed security incidents involving Personal Data.

10.5.2. Where the GDPR applies, we assess whether an incident constitutes a Personal Data breach and whether notification is required under *Articles 33 and 34 GDPR*.

10.5.3. Where the Australian Privacy Act applies, we assess whether an incident constitutes an eligible data breach and whether notification is required under the Notifiable Data Breaches scheme.

10.5.4. We maintain internal records of incidents and remediation actions.

10.6. Regular Security Assessments

10.6.1. We conduct periodic security assessments appropriate to our risk profile, which may include:

(a) vulnerability scanning and remediation;

(b) penetration testing;

(c) access reviews;

(d) audits of key controls;

(e) supplier assurance reviews.

11. DATA SHARING AND THIRD-PARTY DISCLOSURES

11.1. Service Provider Relationships

11.1.1. We may share Personal Data with service providers who assist us to provide the Services, including providers of:

(a) cloud hosting and infrastructure;

(b) analytics and performance monitoring;

(c) crash reporting and diagnostics;

(d) customer support tooling;

(e) communications delivery (email/SMS/push);

(f) payment processing (where applicable);

(g) authentication providers (including Apple and Google);

(h) artificial intelligence services.

11.1.2. Where service providers act as Processors, we implement contractual protections consistent with *Article 28 GDPR* where the GDPR applies and take reasonable steps to ensure appropriate handling under the APPs where Australian law applies.

11.1.3. We authorise sub-processors where necessary and maintain oversight through contractual and governance measures.

11.2. Business Partner Integrations

11.2.1. Where the App integrates with third-party services at the User's request (e.g. via APIs), we may disclose Personal Data to those third parties to enable the integration.

11.2.2. We provide information in-app about the integration and, where required, obtain Consent.

11.2.3. Third parties receiving data through integrations may act as independent controllers. Their privacy practices are governed by their own policies.

11.3. Legal Disclosure Requirements

11.3.1. We may disclose Personal Data to courts, law enforcement, regulators, or government agencies where required or authorised by law, including in response to lawful requests.

11.3.2. We review requests for validity and scope and respond in accordance with applicable law.

11.3.3. Where permitted, we may notify affected Users of such requests.

11.4. Corporate Transactions

11.4.1. If we undergo a merger, acquisition, restructuring, or sale of assets, Personal Data may be disclosed to advisers and prospective counterparties as part of due diligence and transferred as part of the transaction.

11.4.2. We apply confidentiality and security protections and, where required, provide notice to Users.

11.5. Marketing and Advertising Partners

11.5.1. Where applicable, we may share limited data with marketing and advertising partners to:

(a) deliver and measure campaigns;

(b) suppress marketing to Users who have opted out; and

(c) (where permitted) personalise advertising.

11.5.2. Where required by law, we obtain Consent before enabling targeting/advertising Tracking Technologies (section 9).

11.5.3. Users can object to direct marketing and manage preferences (section 13).

12. CHILDREN'S PRIVACY PROTECTION

12.1. Age Verification and Parental Consent

12.1.1. The Services are not intended for children under 18, unless expressly stated for a specific product offering.

12.1.2. Where *Article 8 GDPR* applies and we rely on Consent for Processing in relation to information society services offered directly to a child, we implement age-gating and parental consent mechanisms where required by applicable Member State law.

12.1.3. If we become aware that we have collected Personal Data from a child in a manner not permitted by applicable law, we will take steps to delete or de-identify it.

12.2. Enhanced Protection for Children's Data

12.2.1. Where we process children’s data, we apply enhanced safeguards, including:

(a) data minimisation;

(b) restricted profiling and marketing;

(c) heightened access controls;

(d) shorter retention where appropriate.

12.3. Educational and Safety Considerations

12.3.1. We may provide age-appropriate privacy information and safety resources within the App where relevant.

12.3.2. We may provide reporting channels for safety concerns and inappropriate content.

13. MARKETING AND COMMUNICATIONS

13.1. Email Marketing Consent and Management

13.1.1. We may send marketing communications by email (and other channels) where permitted by law and in accordance with User preferences.

13.1.2. Users can opt out at any time by:

(a) using the unsubscribe link in marketing emails;

(b) changing in-app communication preferences; or

(c) contacting us (section 3.2).

13.1.3. We maintain suppression lists to ensure we respect opt-out requests.

13.2. Push Notification Controls

13.2.1. We may send push notifications for:

(a) service and security messages; and

(b) marketing messages (where enabled).

13.2.2. Users can control push notifications through device settings and in-app preferences.

13.2.3. Where required, we obtain Consent for marketing push notifications.

13.3. Personalised Advertising and Profiling

13.3.1. Where applicable, we may use data to personalise content and advertising, including through Profiling.

13.3.2. Where required by applicable law, we obtain Consent for advertising Tracking Technologies and provide opt-out controls (section 9).

13.3.3. Users may object to Processing for direct marketing at any time (section 6.6).

13.4. Direct Marketing Under Australian Privacy Act

13.4.1. We comply with APP 7 in relation to direct marketing.

13.4.2. We do not use Sensitive Information for direct marketing unless the individual has consented (where required).

13.4.3. We provide a simple means to opt out of direct marketing communications.

14. USER ACCOUNT MANAGEMENT

14.1. Account Creation and Verification

14.1.1. Users must provide certain information to create an Account (section 4.1).

14.1.2. We may use verification measures (e.g. email verification, SMS verification) to protect Accounts and prevent fraud.

14.1.3. We may log account creation and verification events for security and audit purposes.

14.2. Account Settings and Privacy Controls

14.2.1. We provide in-app settings to enable Users to:

(a) update profile information;

(b) manage marketing preferences;

(c) manage certain permissions (where supported);

(d) access privacy information and submit rights requests (where available).

14.2.2. Device permissions (e.g. location, camera, contacts) can generally be controlled via device operating system settings.

14.2.3. Where feasible, we provide granular controls so Users can enable optional features without enabling unrelated data collection.

14.3. Account Suspension and Termination

14.3.1. We may suspend or terminate Accounts in accordance with our terms of service (if applicable), including for security reasons or misuse.

14.3.2. Upon termination or closure, we handle Personal Data in accordance with section 8 (retention) and section 6.3 (erasure), subject to legal holds and other lawful retention needs.

14.3.3. We may retain limited data to prevent fraud, enforce terms, and comply with legal obligations.

14.4. Account Security Features

14.4.1. We may offer security features such as:

(a) multi-factor authentication;

(b) session management and device management;

(c) account recovery processes;

(d) suspicious login detection.

14.4.2. Users should keep credentials confidential and notify us of suspected unauthorised access.

15. COMPLIANCE MONITORING AND GOVERNANCE

15.1. Privacy Governance Framework

15.1.1. We maintain a privacy governance framework appropriate to our size and risk profile, including:

(a) assignment of privacy responsibilities;

(b) policies and procedures supporting this Policy;

(c) oversight of high-risk processing activities;

(d) periodic reporting to senior management.

15.2. Staff Training and Awareness

15.2.1. We provide privacy and security training to staff and contractors with access to Personal Data, including training on:

(a) GDPR principles and obligations (where applicable);

(b) APP requirements;

(c) incident reporting and response;

(d) secure handling of Personal Data.

15.3. Privacy Impact Assessments

15.3.1. Where required by *Article 35 GDPR*, we conduct Data Protection Impact Assessments (**DPIAs**) for processing likely to result in a high risk to the rights and freedoms of individuals, including where we introduce new technologies or large-scale profiling.

15.3.2. DPIAs consider:

(a) necessity and proportionality;

(b) risks to individuals;

(c) measures to address risks and demonstrate compliance.

15.3.3. We maintain DPIA records and review DPIAs when processing changes.

15.4. Vendor Management and Due Diligence

15.4.1. We assess vendors that process Personal Data on our behalf, including their:

(a) security posture;

(b) privacy compliance measures;

(c) sub-processing arrangements;

(d) location of processing and transfer safeguards.

15.4.2. We contractually require vendors to implement appropriate technical and organisational measures and to notify us of incidents.

15.5. Regulatory Engagement and Reporting

15.5.1. We maintain processes to engage with regulators and Supervisory Authorities where required.

15.5.2. We maintain records of processing activities where required by the GDPR and appropriate internal records to support APP compliance.

16. COMPLAINT PROCEDURES AND DISPUTE RESOLUTION

16.1. Internal Complaint Procedures

16.1.1. Individuals may lodge a privacy complaint by contacting us via section 3.2.

16.1.2. Complaints should include sufficient details for us to investigate (e.g. account identifier, description of concern, relevant dates).

16.1.3. We will:

(a) acknowledge receipt within a reasonable time;

(b) investigate and respond within a reasonable time; and

(c) take steps to address substantiated issues.

16.2. Regulatory Complaint Rights

16.2.1. Where the GDPR applies, Data Subjects may lodge a complaint with a Supervisory Authority, in particular in the Member State of their habitual residence, place of work, or place of the alleged infringement.

16.2.2. Where the Australian Privacy Act applies, individuals may lodge a complaint with the Office of the Australian Information Commissioner (**OAIC**).

16.3. Alternative Dispute Resolution

16.3.1. Where appropriate, we may offer or participate in alternative dispute resolution processes to resolve privacy complaints efficiently.

16.4. Legal Remedies and Compensation

16.4.1. Where the GDPR applies, Data Subjects may have rights to judicial remedies and compensation in accordance with the GDPR, including *Article 82 GDPR*.

16.4.2. Under Australian law, enforcement mechanisms may apply under the Australian Privacy Act and associated regulatory processes.

17. POLICY UPDATES AND NOTIFICATION PROCEDURES

17.1. Policy Review and Update Procedures

17.1.1. We review this Policy at least annually and when:

(a) we introduce new features or materially change data practices;

(b) we change vendors or hosting arrangements in a way that affects Processing;

(c) laws or regulatory guidance change;

(d) we identify new risks through DPIAs/TIAs or incidents.

17.2. User Notification of Changes

17.2.1. We notify Users of material changes via in-app notice and/or email where appropriate.

17.2.2. Where required, we obtain Consent for changes that expand Processing activities requiring Consent.

17.3. Version Control and Historical Records

17.3.1. We maintain historical versions of this Policy and make prior versions available upon request where reasonably required for accountability.

17.4. Emergency Update Procedures

17.4.1. We may implement urgent updates without advance notice where necessary to:

(a) address a security risk;

(b) comply with a legal requirement; or

(c) prevent misuse or harm.

17.4.2. Where practicable, we will notify Users as soon as reasonably possible after an emergency update.

18. JURISDICTION-SPECIFIC PROVISIONS

18.1. European Union Member State Variations

18.1.1. Some GDPR requirements may vary by Member State (for example, in relation to children’s consent age thresholds and certain employment or health contexts).

18.1.2. Where such variations apply to our Processing, we implement feature-level notices and controls to meet local requirements.

18.2. Australian State and Territory Considerations

18.2.1. Additional privacy and surveillance obligations may apply in Australian states and territories in specific contexts (e.g. health information handling, workplace surveillance).

18.2.2. Where such obligations apply to our operations, we implement supplementary procedures and notices.

18.3. Conflict of Laws Provisions

18.3.1. This Policy is intended to be read to give effect to both GDPR and Australian privacy requirements.

18.3.2. Where there is a direct conflict between mandatory requirements:

(a) for EEA Data Subjects and GDPR-scoped Processing, we apply the GDPR standard to the extent required;

(b) for Australian-scoped Processing, we apply the Australian Privacy Act and APPs to the extent required; and

(c) we apply the higher standard where feasible to maintain a single global approach.

19. APPENDICES AND REFERENCE MATERIALS

19.1. Standard Contractual Clauses

19.1.1. We use SCCs as described in section 7.2.

19.1.2. A copy of the SCCs (as executed for relevant transfers) may be requested via section 3.2, subject to redaction of confidential commercial information where permitted.

19.2. Cookie Policy Detail

19.2.1. We maintain a current list of Tracking Technologies used in the App, including:

(a) category;

(b) purpose;

(c) provider (first/third party);

(d) duration/expiry (where applicable);

(e) data elements collected;

(f) consent status (required/not required depending on jurisdiction and category).

19.2.2. Users can request the current list via section 3.2 and/or access it in-app where provided.

19.3. Contact Forms and Request Templates

19.3.1. We may provide templates for:

(a) access requests;

(b) rectification requests;

(c) erasure requests;

(d) restriction requests;

(e) portability requests;

(f) objection requests;

(g) complaints.

19.3.2. Requests may be submitted without using a template provided they contain sufficient information for us to verify identity and locate relevant data.

19.4. Legal References and Citations

19.4.1. Key GDPR provisions referenced in this Policy include: *Articles 12–22, 27, 28, 33–35, 37, 44–49, 82 GDPR*.

19.4.2. Key Australian privacy instruments referenced include: *Privacy Act 1988 (Cth)* and the *Australian Privacy Principles (APPs)*.

19.5. Glossary of Technical Terms

19.5.1. **API**: Application Programming Interface enabling software components to communicate.

19.5.2. **Encryption**: A security method that encodes data to prevent unauthorised access.

19.5.3. **SDK**: Software Development Kit, often used for analytics, crash reporting, or feature enablement.

19.5.4. **Pseudonymisation**: Processing that reduces identifiability by separating identifiers from data.

19.5.5. **Telemetry**: Automated collection of performance and usage signals for reliability and improvement.

20. EXECUTION AND EFFECTIVE DATE

20.1. Policy Authorisation

20.1.1. This Policy is approved for use by the organisation and is authorised by:

(a) the Board (or delegated committee) where applicable; and/or

(b) an authorised executive responsible for risk and compliance.

20.1.2. Internal approvals and sign-off records are maintained as part of our governance framework (section 15.1).

20.2. Effective Date and Implementation

20.2.1. This Policy takes effect on the Effective date stated at the beginning of this document.

20.2.2. We implement this Policy by:

(a) publishing it in-app and making it accessible during onboarding;

(b) training relevant staff (section 15.2);

(c) configuring consent and privacy controls (sections 9 and 14);

(d) implementing vendor contractual safeguards (section 11 and 15.4).

20.3. Supersession of Previous Policies

20.3.1. This Policy supersedes all prior privacy policies and privacy notices issued by us in relation to the App and Services to the extent of any inconsistency, from the Effective date.

EXECUTION

Dated

Executed for and on behalf of INNERPIECE PTY LTD (ACN 689 982 885) in accordance with section 127 of the Corporations Act by:		
Full Name	**Capacity (circle)**	**Signature**
Lily Ella Cummins	**Sole director Director Secretary**	
Susan Lynch	**Director Secretary Witness**