VITARA CAREPILOT®
More than just technology.

PRIVACY POLICY

1. INTRODUCTION

At Vitara Guardians (Parent company of Vitara CarePilot), your privacy is at the core of our mission to deliver smarter, safer, and more connected care solutions. This Privacy Policy outlines how we collect, use, and share your personal information to deliver exceptional service while upholding the highest standards of integrity and transparency.

We process your personal data to enhance service delivery, personalise user experiences, and ensure compliance with applicable regulatory requirements. Our commitment is to protect your privacy while providing value-driven solutions tailored to your needs.

Privacy at Every Step

In addition to this Privacy Policy, we provide clear and accessible data and privacy information directly within our products and services.

Features that request or use your personal information are accompanied by easy-to-understand notices so that you remain informed every step of the way.

How We Provide Transparency?

- Feature-Specific Information: Whenever a feature requests access to your data, we will provide a clear explanation of why the data is needed and how it will be used. You will always have the option to review and manage these permissions. Additionally, you can access this information anytime online at Data & Privacy Page.
- Accessible Details: This information is available in your account settings or by contacting our support team.

2. PURPOSE & SCOPE

Purpose of this policy

The purpose of this Privacy Policy is to explain how Vitara CarePilot collects, uses, discloses, stores, and protects personal information in accordance with the Privacy Act 1988 and the Australian Privacy Principles.

It ensures that individuals understand their privacy rights, how their information is managed when using Vitara CarePilot's assistive technologies and services, and the safeguards in place to protect sensitive and safety related data.

This policy supports transparency, customer trust, and compliance with NDIS Practice Standards and all applicable legal obligations.

Scope

This Privacy Policy applies to:

- All customers, families, carers, support coordinators, and authorised representatives
- All personnel, contractors, and licensed electricians engaged by Vitara CarePilot
- All services, systems, applications, and technologies operated by Vitara CarePilot

This policy covers information collected through:

- Consultations and site assessments
- Sensor installation and configuration
- The Vitara CarePilot mobile app and monitoring platform
- Customer support interactions
- Payments, subscriptions, and account management
- Alerts, reports, and automated system events

3. COLLECTING AND USE OF PERSONAL DATA

Types of Data Collected

Personal Data
While using our Service, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you. Personally identifiable information may include, but is not limited to:

- Email address
- First name and last name
- Phone number
- Address, State, Postal code, City

Care and Safety Data
This may include sensor derived activity and movement signals, room presence events, fall and unusual inactivity events, alert delivery logs, care network roles (care recipient, primary carer, co carer), and configuration data required to provide monitoring and alerts.

Medical and Emergency Information (Sensitive Information)
Medical and Emergency Information may include the care recipient's consent record, medical conditions, allergies, medications (if provided), emergency notes, and emergency contact details. This information relates to the care recipient and is collected and stored for the purpose of supporting emergency response, including enabling relevant information to be shared with emergency services or responders in the event of a medical emergency. During onboarding, the primary carer records and submits this information in the Service based on the care recipient's consent.

Usage Data
Usage Data is collected automatically when using the Service.

Usage Data may include information such as Your Device's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of our Service that You visit, the time and date of Your visit, the time spent on those pages, unique device identifiers and other diagnostic data.

When You access the Service by or through a mobile device, We may collect certain information automatically, including, but not limited to, the type of mobile device You use, Your mobile device unique ID, the IP address of Your mobile device, Your mobile operating system, the type of mobile Internet browser You use, unique device identifiers and other diagnostic data.

We may also collect information that Your browser sends whenever You visit our Service or when You access the Service by or through a mobile device.

Tracking Technologies and Cookies
We use Cookies and similar tracking technologies to track the activity on Our Service and store certain information. Tracking technologies used are beacons, tags, and scripts to collect and track information and to improve and analyse Our Service.

The technologies we use may include:

- Cookies or Browser Cookies. A cookie is a small file placed on Your Device. You can instruct Your browser to refuse all Cookies or to indicate when a Cookie is being sent. However, if You do not accept Cookies, You may not be able to use some parts of our Service.

Unless you have adjusted Your browser setting so that it will refuse Cookies, our Service may use Cookies.

Web Beacons. Certain sections of our Service and our emails may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that permit the Company, for example, to count users who have visited those pages or opened an email and for other related website statistics (for example, recording the popularity of a certain section and verifying system and server integrity).

Cookies can be “Persistent” or “Session” Cookies. Persistent Cookies remain on Your personal computer or mobile device when You go offline, while Session Cookies are deleted as soon as You close Your web browser. We use cookies and similar technologies on our website for essential functionality and analytics. Some emails may include tracking pixels to measure engagement, where permitted by law and your settings.

We use both Session and Persistent Cookies for the purposes set out below:

- **Necessary / Essential Cookies**
  - Type: Session Cookies
  - Administered by: Us
  - Purpose: These Cookies are essential to provide You with services available through the Website and to enable You to use some of its features. They help to authenticate users and prevent fraudulent use of user accounts. Without these Cookies, the services that You have asked for cannot be provided, and We only use these Cookies to provide You with those services.
- **Cookies Policy / Notice Acceptance Cookies**
  - Type: Persistent Cookies
  - Administered by: Us
  - Purpose: These Cookies identify if users have accepted the use of cookies on the Website.
- **Functionality Cookies**
  - Type: Persistent Cookies
  - Administered by: Us
  - Purpose: These Cookies allow us to remember choices You make when You use the Website, such as remembering your login details or language preference.

The purpose of these Cookies is to provide You with a more personal experience and to avoid You having to re-enter your preferences every time You use the Website.

For more information about cookies and your choices, see the Cookies section of this Privacy Policy.

4. USE OF YOUR PERSONAL DATA

The Company may use Personal Data for the following purposes:

- **To provide** and maintain our Service, including to monitor the usage of our Service.
- **To manage Your Account:** to manage Your registration as a user of the Service. The Personal Data You provide can give You access to different functionalities of the Service that are available to You as a registered user.
- **To support emergency response:** To store and display care recipient medical and emergency information, including medical conditions and allergies, and to enable that information to be shared with emergency services or responders in the event of a medical emergency, based on the care recipient's consent recorded during onboarding and as otherwise permitted by law.
- **For the performance of a contract:** the development, compliance and undertaking of the purchase contract for the products, items or services You have purchased or of any other contract with Us through the Service.
- **To contact You:** To contact You by email, telephone calls, SMS, or other equivalent forms of electronic communication, such as a mobile application's push notifications regarding updates or informative communications related to the functionalities, products or contracted services, including the security updates, when necessary or reasonable for their implementation.
- **To provide You** with news, special offers and general information about other goods, services and events which we offer that are similar to those that you have already purchased or enquired about unless You have opted not to receive such information.
- **To manage Your requests:** To attend and manage Your requests to Us.
- **For business transfers:** We may use Your information to evaluate or conduct a merger, divestiture, restructuring, reorganisation, dissolution, or other sale or transfer of some or all of Our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which Personal Data held by Us about our Service users is among the assets transferred.

- **For other purposes:** We may use Your information for other purposes, such as data analysis, identifying usage trends, determining the effectiveness of our promotional campaigns and to evaluate and improve our Service, products, services, marketing and your experience.
    - We will only send marketing communications with your explicit consent, and you can opt-out at any time through the 'unsubscribe' link in our emails or by contacting us.

We may share Your personal information in the following situations:

- **With Service Providers:** We may share Your personal information with Service Providers to monitor and analyse the use of our Service, to contact You.
- **For business transfers:** We may share or transfer Your personal information in connection with, or during negotiations of, any merger, sale of Company assets, financing, or acquisition of all or a portion of Our business to another company.
- **With Affiliates:** We may share Your information with Our affiliates, in which case we will require those affiliates to honor this Privacy Policy. Affiliates include Our parent company and any other subsidiaries, joint venture partners or other companies that We control or that are under common control with Us.
- **With business partners:** We may share Your information with Our business partners to offer You certain products, services or promotions.
- **With other users:** when You share personal information or otherwise interact in the public areas with other users, such information may be viewed by all users and may be publicly distributed outside.
- **With Your consent:** We may disclose Your personal information for any other purpose with Your consent.

5. DATA PROCESSING, SHARING, AND INTERNATIONAL TRANSFERS

We process your personal data in accordance with applicable privacy laws, including the Australian Privacy Act 1988 (APA) and the General Data Protection Regulation (GDPR), depending on Your jurisdiction. Our processing activities are based on various legal grounds, including Your consent, contractual necessity, compliance with legal obligations, and Our legitimate interests.

To deliver Our services effectively, We may share Your data with trusted third-party service providers, including:

- Cloud Service Providers: For secure data storage and processing.
- Analytics Providers: To analyse usage trends and enhance Our services.
- Marketing Partners: To offer promotional communications, where You have provided consent.
- Payment Processors: To facilitate secure transactions.

Your Personal Data may be processed at Our operating offices and in other locations where the parties involved in processing are based. This means that Your information may be transferred to and stored on computers located outside of Your state, province, country, or other governmental jurisdiction, where data protection laws may differ from those in Your jurisdiction. By submitting Your information and consenting to this Privacy Policy, You acknowledge and agree to such transfers.

We take all reasonably necessary steps to ensure that Your data is handled securely and in accordance with this Privacy Policy. When transferring data outside Australia and the European Economic Area (EEA), We implement safeguards such as Standard Contractual Clauses (SCCs) approved by regulatory authorities to ensure Your data is handled securely. Additionally, no transfer of Your Personal Data will occur to any organisation or country unless adequate safeguards are in place, including binding corporate rules (BCRs), SCCs, or other legally recognised mechanisms that uphold a high standard of data protection.

Furthermore, We ensure that all third-party vendors with whom Your data is shared comply with Our stringent data protection standards. This is achieved through legally binding Data Processing Agreements (DPAs), which outline their responsibilities and obligations under GDPR, the Australian Privacy Act 1988, and other relevant regulations, ensuring the continued security and confidentiality of Your Personal Data.

6. YOUR RIGHTS TO ACCESS, UPDATE, AND DELETE PERSONAL DATA

You have the right to request access to, correct, or delete the Personal Data We have collected about You, in compliance with the Australian Privacy Act 1988 and other applicable laws.

Our Service may provide You with the ability to update or delete certain information directly from within the Service. If You have an account, You can manage Your personal information by signing in and visiting the account settings section.

Additionally, You may contact Us to request access to, correction of, or deletion of any personal information You have provided to Us. We will respond to such requests in accordance with applicable legal requirements.

Please note that while We will make every reasonable effort to comply with Your requests, there may be instances where We are required to retain certain information due to legal obligations or other lawful bases. If You have any concerns regarding the handling of Your data, You also have the right to lodge a complaint with Us.

7. DISCLOSURE OF YOUR PERSONAL DATA

Business Transactions	If the Company is involved in a merger, acquisition or asset sale, Your Personal Data may be transferred. We will provide notice before Your Personal Data is transferred and becomes subject to a different Privacy Policy.
Emergency Disclosure	In an emergency, relevant medical and emergency information about the care recipient may be disclosed to emergency services or responders where this is necessary to protect the vital interests of the care recipient or another person, where the care recipient has consented to this sharing and that consent has been recorded in the Service, or where otherwise authorised or required by applicable law.
Law enforcement	Under certain circumstances, the Company may be required to disclose Your Personal Data if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency).
Other legal requirements	The Company may disclose Your Personal Data in the good faith belief that such action is necessary to: • Comply with a legal obligation • Protect and defend the rights or property of the Company • Prevent or investigate possible wrongdoing in connection with the Service • Protect the personal safety of Users of the Service or the public • Protect against legal liability

8. SECURITY OF YOUR PERSONAL DATA

The security of Your Personal Data is of utmost importance to Us. We implement stringent security measures to protect Your information, including:

- Encryption protocols (e.g., SSL/TLS) to safeguard data in transit and at rest.
  - We employ industry-standard encryption (AES-256 for data at rest and SSL/TLS for data in transit) and access control measures to protect your personal data.
- Access control measures and authentication processes to limit unauthorised access.
- Regular audits and vulnerability assessments to identify and address potential security risks.
- Anonymisation and pseudonymisation techniques, where possible, to enhance privacy and minimise data exposure risks.

While We strive to use commercially acceptable means to protect Your Personal Data, please note that no method of transmission over the Internet or electronic storage is entirely secure. Despite Our efforts, We cannot guarantee absolute security.

9. DATA BREACH NOTIFICATION

In the event of a data breach, Vitara Guardians will take prompt action to mitigate the impact and notify affected individuals and relevant authorities within 72 hours, in compliance with applicable laws, including the Notifiable Data Breaches (NDB) scheme under the Australian Privacy Act and the General Data Protection Regulation (GDPR).

Affected individuals will receive clear recommendations on protective actions they can take to safeguard their information. We are committed to transparency and will provide timely updates regarding the nature of the breach, the affected data, and any steps You should take to protect Yourself.

While we implement stringent security measures, Vitara Guardians is not liable for breaches resulting from factors beyond our reasonable control. Any applicable compensation will be determined on a case-by-case basis in line with relevant laws.

10. PROTECTION OF MINORS AND VULNERABLE INDIVIDUALS

Our Service is not intended for individuals under the age of 13, and We do not knowingly collect personally identifiable information from anyone under this age. If You are a parent or guardian and become aware that Your child has provided Us with Personal Data, please contact Us immediately.

In the event that We discover Personal Data has been collected from a child under 13 without verified parental consent, We will take prompt action to remove that information from Our systems. If We rely on consent as a legal basis for processing information and parental consent is required under applicable laws, We may request parental approval before collecting or using such information.

In addition to safeguarding minors, We are committed to protecting the privacy and security of vulnerable individuals, including elderly users receiving care.

11. GDPR COMPLIANCE STATEMENT

Vitara Guardians (“Vitara Guardians,” “we,” “us,” or “our”) is committed to ensuring that your personal data is handled in compliance with the General Data Protection Regulation (EU) 2016/679 (GDPR), which governs the collection, processing, and protection of personal data of individuals in the European Economic Area (EEA).

This section of our Privacy Policy outlines the principles we follow, the legal basis for processing your data, your rights as a data subject, and how you can exercise these rights.

12. PRINCIPLES OF DATA PROCESSING

We adhere to the following core principles when processing your personal data:

Lawfulness, Fairness, and Transparency: We process your data lawfully, fairly, and transparently, providing clear information about how your data is used.
Purpose Limitation: We collect and process your personal data only for specified, explicit, and legitimate purposes.
Data Minimisation: We collect only the necessary data required to achieve the intended purpose.

Accuracy: We ensure personal data is accurate and up-to-date, with mechanisms for you to correct inaccuracies.
Storage Limitation: We retain personal data only as long as necessary to fulfill our obligations or as required by law.
Integrity and Confidentiality: We apply appropriate technical and organisational measures to protect your data from unauthorised access, loss, or destruction.
Accountability: We are accountable for demonstrating compliance with GDPR principles.

13. LEGAL BASIS FOR PROCESSING PERSONAL DATA

Under the GDPR, we process your personal data based on the following lawful bases:

Consent (Article 6(1)(a)): When you provide explicit and informed consent to the processing of your data (e.g., subscribing to newsletters, receiving promotional materials).
You can withdraw your consent at any time.
Contractual Necessity (Article 6(1)(b)): Processing is necessary to fulfill our contractual obligations to you or take pre-contractual steps at your request.
Legal Obligation (Article 6(1)(c)): We are required to process personal data to comply with applicable legal and regulatory obligations.
Legitimate Interests (Article 6(1)(f)): We may process your data to pursue legitimate business interests, such as improving our services, preventing fraud, and ensuring IT security, provided it does not override your rights.

14. YOUR GDPR RIGHTS

As an individual within the EEA, you have the following rights regarding your personal data under GDPR:

- **Right to Access (Article 15 GDPR)**
  - You have the right to request access to the personal data we hold about you, including:
  - The purposes of processing.
  - The categories of personal data processed.
  - The recipients to whom the data has been disclosed.
  - The expected retention period.
- **Right to Rectification (Article 16 GDPR)**
  - If any of the information we hold about you is incorrect or incomplete, you have the right to request corrections.

- **Right to Erasure (“Right to Be Forgotten”) (Article 17 GDPR)**
  - You can request the deletion of your personal data where:
    - The data is no longer necessary for the purposes it was collected.
    - You withdraw consent and there is no other legal basis for processing.
    - The data was unlawfully processed.
- **Right to Restriction of Processing (Article 18 GDPR)**
  - You can request to limit how we use your data if:
  - You contest the accuracy of your data.
  - Processing is unlawful, but you prefer restriction over deletion.
  - We no longer need the data but require it for legal claims.
- **Right to Data Portability (Article 20 GDPR)**
  - You have the right to receive your personal data in a structured, commonly used, and machine-readable format and transmit it to another controller.
- **Right to Object (Article 21 GDPR)**
  - You have the right to object to the processing of your personal data where processing is based on:
    - Legitimate interests.
    - Direct marketing purposes.
- **Right to Withdraw Consent (Article 7 GDPR)**
  - If we process your personal data based on your consent, you have the right to withdraw it at any time.
- **Right to Lodge a Complaint (Article 77 GDPR)**
  - You have the right to lodge a complaint with a supervisory authority in your country if you believe your data is being processed unlawfully.

In the EEA, you can contact your local data protection authority or the Office of the Australian Information Commissioner (OAIC) for Australian residents.

15. DATA TRANSFERS OUTSIDE THE EEA

We may transfer your personal data outside the EEA to countries that may not provide the same level of data protection.

In such cases, we ensure the following safeguards:

- Standard Contractual Clauses (SCCs) approved by the European Commission.
- Binding Corporate Rules (BCRs).
- Certification under frameworks such as the EU-U.S. Data Privacy Framework.

You can request further details about international data transfers by contacting us.

16. AUTOMATED DECISION-MAKING AND PROFILING

We utilise AI-powered insights to enhance Our services and provide a more personalised experience. Our service leverages AI-driven insights to offer proactive care recommendations, helping to improve user wellbeing and support individual needs. In cases where automated decision-making, including profiling, is used, We are committed to transparency and ensuring Your rights are protected. Users have the right to request human review in situations where decisions significantly impact their care and wellbeing.

You will be informed about the use of such technologies and their potential impact on You.

Specifically, We will:

- Provide meaningful information about the logic involved in automated decisions.
- Explain the significance and potential consequences of these decisions for You.
- Offer the right to request human intervention where applicable, ensuring that important decisions are reviewed by a qualified individual.

Our goal is to balance automation with fairness and accountability, ensuring that Your interests and rights are respected in accordance with applicable data protection regulations.

17. RETENTION OF YOUR PERSONAL DATA

We will retain your personal data only for as long as necessary to fulfill the purposes for which it was collected, including:

Data Type	Retention Period	Legal Basis
Account Data	Retained for the duration of the account and up to 7 years post-termination	Performance of contract (account administration)
Billing Data	Retained for at least 7 years for compliance with financial regulations.	Legal obligation (tax and accounting record keeping)
Care recipient consent records	Duration of the care recipient profile plus 7 years after profile closure	Performance of contract, Legal obligation where applicable, Legitimate interests (audit trail, dispute handling, safety governance)
Marketing Data	Retained until you withdraw consent or opt out.	Consent (direct marketing where required)

Data Type	Retention Period	Legal Basis
Medical and emergency information (conditions, allergies)	Duration of the care recipient profile or until updated or deleted, plus up to 30 days in backups	Explicit consent of the care recipient (sensitive information), Vital interests (emergency situations), Performance of contract (feature delivery)
Usage Analytics	Retained for a period of 24 months for service improvement.	Legitimate interests (service improvement, product analytics)
Sensor telemetry and activity events	12 months rolling from event date (default)	Performance of contract (provide monitoring and app functionality)
Incident and alert logs	12 months from incident close date (or event date if not closed)	Performance of contract (deliver safety alerts and history)
Support interactions	24 months from ticket closure	Legitimate interests (resolve issues, quality assurance, training)
Audit and security logs	24 months from log creation	Legitimate interests (security, fraud prevention, abuse detection)

We will retain and use Your Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.

The Company will also retain Usage Data for internal analysis purposes. Usage Data is generally retained for a shorter period of time, except when this data is used to strengthen the security or to improve the functionality of Our Service, or We are legally obligated to retain this data for longer time periods.

To request access, correction, or deletion of your data, please visit your account settings or contact us at privacy@vitaraguardians.com. We will respond within 30 days as required by law.

18. LINKS TO THIRD-PARTY WEBSITES AND DATA SHARING DISCLOSURE

Our Service may contain links to third-party websites that are not operated by Us. If You click on a third-party link, You will be directed to that third party's site. We strongly advise You to review the Privacy Policy of every site You visit, as We have no control over and assume no responsibility for the content, privacy policies, or practices of any third-party sites or services.

Additionally, We may share Your personal data with selected third parties, including but not limited to cloud service providers, analytics services, and business partners, strictly for purposes such as improving our Service, providing customer support, and enhancing user experience.

These third parties are contractually obligated to protect Your information in compliance with applicable data protection regulations.

For the current version of this Privacy Policy, refer to https://vitaracarepilot.com/privacy-policy/

19. CHANGES TO OUR PRIVACY POLICY AND ONGOING ASSESSMENTS

We may update Our Privacy Policy from time to time to reflect changes in regulatory requirements, business practices, or service offerings. We review our Privacy Policy annually and whenever significant regulatory or operational changes occur to ensure it reflects our latest practices. Any significant updates will be communicated to You via email and through a prominent notice on Our website, where the revised Privacy Policy will be posted. We will inform You in advance of any changes taking effect and update the “Last updated” date at the top of this Privacy Policy.

We encourage You to review this Privacy Policy periodically to stay informed about how We are protecting Your information. Changes to this Privacy Policy become effective once they are posted on this page.

As part of our commitment to privacy and data protection, We conduct regular Privacy Impact Assessments (PIAs) to evaluate how new projects, technologies, or services may impact user privacy. These assessments enable Us to identify potential risks and implement proactive measures to ensure compliance with privacy laws and industry best practices.

20. PERSONALISED PRIVACY CONTROLS

We believe privacy should be empowering. That’s why we provide tools and controls to help you manage how your information is collected and used:

- Employee Access: Employee access to personal data is restricted based on role necessity, and all employees undergo regular data protection training.

- Privacy Dashboard: Access a summary of the data collected and how it's used.
- Customisable Permissions: Adjust privacy settings to suit your needs.
- Real-Time Notifications: Receive alerts when your data is accessed by specific features.

21. HOW TO LEARN MORE

We've designed our Privacy Policy to be transparent and easy to navigate. Below are key areas to help you familiarise yourself with our practices:

- **What We Collect and Why:** Learn about the types of personal information we collect and how we use it to improve your experience.
- **How We Share Your Information:** Understand the limited circumstances in which your information may be shared, such as with trusted service providers.
- **Your Rights and Choices:** Discover how to access, correct, or delete your personal data.
- **Data Security:** Learn about the measures we take to protect your information.

22. YOUR RIGHTS AND CHOICES

You can manage your consent preferences via your account settings or by contacting us. In cases where consent is the legal basis for processing, you have the right to withdraw it at any time without affecting the lawfulness of processing based on consent before withdrawal.

For all products and services:

- You have the right to access, correct, or delete your personal data.
- You can customise data collection preferences through your account settings or by contacting us.
- If you have questions about how your data is used, please contact us directly.

Care recipient consent and primary carer role:

Where the primary carer enters or manages medical and emergency information about a care recipient, the primary carer confirms they have obtained the care recipient's consent (or are otherwise authorised by law to act on the care recipient's behalf) for the collection, use, and emergency disclosure of that information through the Service. The Service records the consent status captured during onboarding.

The primary carer can update or delete the care recipient's medical and emergency information through the Service, subject to any legal or technical limitations. Where we rely on the care recipient's explicit consent to process sensitive information, that consent may be withdrawn by updating or deleting the information or by contacting us, noting this may limit emergency related functionality.

We are committed to ensuring your data is used responsibly and transparently. Thank you for trusting Vitara Guardians to support your care needs.

If you have any questions, concerns, or feedback regarding your privacy, our dedicated team is here to assist you.

Additionally, to exercise your data rights, submit a request by contacting us at privacy@vitaraguardians.com. We will respond within 30 days.

23. INTERPRETATIONS AND DEFINITIONS

Interpretation

The words of which the initial letter is capitalised have meanings defined under the following conditions. The following definitions shall have the same meaning regardless of whether they appear in singular or in plural.

Definitions

For the purposes of this Privacy Policy:

- **'Account'** means a unique account created for you to access our Service or parts of our Service.
- **'Affiliate'** means an entity that controls, is controlled by, or is under common control with a party, where "control" means ownership of 50% or more of the shares, equity interest, or other securities entitled to vote for election of directors or other managing authority.
- **Care recipient** means the individual receiving care or monitoring support through the Service, whose personal data may be entered and managed in the Service by a primary carer or other authorised person.
- **'Company'** (referred to as either "the Company", "We", "Us" or "Our" in this Agreement) refers to Vitara Guardians.
- **'Cookies'** are small files that are placed on your computer, mobile device, or any other device by a website, containing details of your browsing history on that website among its many uses.
- **'Country'** refers to Australia.

- **‘Device’** means any device that can access the Service such as a computer, a cellphone, or a digital tablet.
- **‘Personal Data’** is any information that relates to an identified or identifiable individual.
- **‘Service’** refers to the Vitara CarePilot website, mobile app, monitoring platform, and related services described in this Privacy Policy
- **‘Service Provider’** means any natural or legal person who processes the data on behalf of the Company. It refers to third-party companies or individuals employed by the Company to facilitate the Service, provide the Service on behalf of the Company, perform services related to the Service, or assist the Company in analysing how the Service is used.
- **‘State’** refers to New South Wales
- ‘**Usage Data’** refers to data collected automatically, either generated by the use of the Service or from the Service infrastructure itself (for example, the duration of a page visit).
- ‘**Website’** refers to Vitara CarePilot, accessible from https://vitaracarepilot.com.
- **‘You’** means the individual accessing or using the Service, or the company, or other legal entity on behalf of which such individual is accessing or using the Service, as applicable.