



VITARA CAREPILOT®
More than just technology.

PRIVACY POLICY

1. INTRODUCTION

This Privacy Policy explains how Vitara Guardians, the parent company of Vitara CarePilot, collects, uses, discloses, stores, and protects personal information when you enquire about, purchase, set up, access, or use Vitara CarePilot services.

It applies to customers, care recipients, primary carers, co-carers, family members, emergency contacts, authorised representatives, and other people who interact directly with Vitara CarePilot or whose information is provided through the service.

We process your personal data to provide and improve the service, support your account and service experience, and comply with applicable legal and regulatory requirements. We are committed to protecting your privacy and handling your information with integrity, care, and transparency.

Privacy at Every Step

In addition to this Privacy Policy, we provide clear and accessible privacy information throughout the Vitara CarePilot service, including within the companion mobile app and related service interactions.

Where personal information is requested or used, we aim to provide clear and easy-to-understand notices so you can remain informed about how your information is collected, used, and managed as part of the service.

How We Provide Transparency

- **Feature-Specific Information:** Where a service function requests access to your personal information, we will provide a clear explanation of why the information is needed and how it will be used. Where available, you will be able to review and manage the relevant permissions. You can also access this information at any time through our Privacy Policy Page.
- **Accessible Details:** This information is available in your account settings or by contacting our support team.

2. PURPOSE AND 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 is designed to help individuals understand their privacy rights, how their information is managed in connection with Vitara CarePilot's physical monitoring service, companion mobile app, and related services, and the safeguards in place to protect personal and service-related information.

This policy supports transparency, customer trust, and compliance with applicable legal and regulatory obligations, including relevant NDIS Practice Standards where applicable.

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
-
- This Privacy Policy applies whether you purchase or use Vitara CarePilot for yourself, arrange or manage the service for a care recipient, or are authorised to access an account, receive alerts, or help manage care-related information.

Where one person provides information about or manages the service for another, that person must have the necessary consent or lawful authority. Information provided to us should be accurate, complete, and kept up to date, and access should be limited to people authorised to use the service.



3. COLLECTION AND USE OF PERSONAL DATA

Types of Data Collected

Personal Data: While using the Service, we may ask you to provide certain personal information that can be used to contact or identify you. Personal information may include, but is not limited to:

- Email address
- First and last name
- Phone number
- Street address, suburb or city, state or territory, and postcode

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.

Sensor, Event and Telemetry Data: The Vitara CarePilot sensors may generate technical data, event message data, telemetry data, diagnostic data, and configuration data. This may include the sensor's:

- unique identifier code,
- known as the deviceID,
- fall events,
- out of bed events,
- presence events,
- timestamps,
- event message identifiers,
- event process stage or status,
- location coordinates where applicable,
- device status,
- connectivity status,
- Wi-Fi state,
- memory usage,
- temperature,
- hardware and
- software versions,
- diagnostic logs,
- room dimensions,
- mounting type,
- mounting height,
- region dimensions,
- feature settings, and
- device control actions.

Technical telemetry may include bespoke BIN files that contain radar-based radio heatmaps of detected movement for a period before, during, and after a fall event. This telemetry is not camera footage and does not contain ordinary video or photographic images. It is technical radar data that may be visualised only through proprietary tools for purposes such as troubleshooting, fault triage, service improvement, incident review, sensor performance analysis, and analysis of historical fall events.



Radar Point Cloud Data: The Vitara CarePilot sensors use mmWave radar technology to detect and evaluate movement and activity. The radar representation of a human form is a cluster of data points based on reflected signal strength, referred to as a Point Cloud. A Point Cloud does not provide ordinary visual identification of a person and is not camera footage.

Device Configuration and Administration Data: We may collect and use device configuration and administration data, including device metadata, deviceId, hardware and software versions, serial numbers, authentication tokens, diagnostic logs, telemetry, device configuration settings, sensitivity maps, Wi-Fi state, connectivity status, memory usage, temperature, presence detection events, fall detection events, room dimensions, mounting type, mounting height, region dimensions, feature settings, and device control actions such as rebooting the device, updating configuration, uploading logs, updating Wi-Fi credentials, or adjusting sensitivity maps.

To connect a sensor to the Care Recipient's home network during installation or reconfiguration, the home Wi-Fi network name, SSID, and password may be transmitted to the sensor vendor's device-administration service, Vayyar, for the sole purpose of provisioning the device. This is household network-configuration data used only for device setup and operation.

Medical and Emergency Information (Sensitive Information): Medical and emergency information may include the care recipient's consent record, disclosed 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 and enabling relevant information to be shared with emergency services or responders where needed during an emergency situation.

During onboarding, the primary carer may record and submit this information in the service based on the care recipient's consent or other lawful authority to do so.

Usage Data: Usage Data is collected automatically when using the service. Usage Data may include information such as your device's Internet Protocol address, browser type, browser version, the pages or screens of the service that you access, the time and date of access, the time spent on those pages or screens, 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 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 or device sends whenever you visit or interact with the service.

Tracking Technologies and Cookies: We use cookies and similar technologies to support the operation of the Service, remember preferences, measure usage, and help us improve performance and functionality.

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 choose not to accept cookies, some parts of the service may not function as intended.
- **Cookies and Similar Technologies:** Unless you have adjusted your browser settings to refuse cookies, the Service may use cookies and similar technologies.
- **Web Beacons:** Certain parts of the Service and some emails may contain small electronic files known as web beacons, including clear GIFs, pixel tags, and single-pixel GIFs. These technologies help us understand usage patterns, measure engagement, monitor the performance of communications, and support system integrity, where permitted by law and your settings.



Cookies may be either persistent or session-based. Persistent cookies remain on your device after you close your browser until they expire or are deleted, while session cookies are generally deleted when you close your browser.

We use cookies and similar technologies on our website and related service interfaces for essential functionality, service performance, and analytics. Some emails may also include tracking technologies to help us understand engagement, where permitted by law and your settings.

We use both session and persistent cookies for the following purposes:

- **Necessary / Essential Cookies**

- **Type:** Session Cookies
- **Administered by:** Us
- **Purpose:** These cookies are necessary to provide the services available through the website and related service interfaces, including helping users log in securely, maintain account sessions, and prevent fraudulent use of accounts. Without these cookies, certain parts of the service may not function properly.

- **Cookies Policy / Notice Acceptance Cookies**

- **Type:** Persistent Cookies
- **Administered by:** Us
- **Purpose:** These cookies help us remember whether you have accepted or managed your cookie preferences on the website.

- **Functionality Cookies**

- **Type:** Persistent Cookies
- **Administered by:** Us
- **Purpose:** These cookies allow us to remember choices you make when using the website, such as login preferences or language settings, so we can provide a more consistent and convenient service experience.

Your Choices for Cookies and Analytics: Where available, you can manage non-essential cookies, analytics, marketing tags, web beacons, and similar tracking technologies through your browser, device, account, or consent settings. Essential technologies required for security, account access, and core service operation may not be disabled. We will use these technologies only as permitted by law and your settings.

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

4. USE OF YOUR PERSONAL DATA

We may use Personal Data for the following purposes:

- **To provide and maintain the service:** To operate, maintain, and improve the Vitara CarePilot physical monitoring service, including the companion mobile app, installed sensors, and related support services, and to monitor how the service is used.
- **To manage your account:** To create, manage, and support your account and access to the service. The personal information you provide helps us deliver the service functions available to you in connection with your Vitara CarePilot Plan.
- **To support emergency response:** To store and display care recipient emergency and care-related information, including disclosed medical conditions, allergies, medications if provided, emergency notes, and emergency contact details, and to enable relevant information to be shared with emergency services or responders where needed during an emergency situation, based on the care recipient's consent or other lawful authority recorded during onboarding and as otherwise permitted by law.



- **To perform our contract with you:** To process and fulfil our obligations in connection with the products and services you have purchased, including your Vitara CarePilot Plan, sensor orders, installation arrangements, billing, and related service support.
- **To contact you:** To contact you by email, telephone, SMS, push notification, or other electronic communication about your account, billing, service updates, alerts, security matters, technical issues, or other service-related information where necessary or appropriate.
- **To send marketing communications:** To send you news, updates, special offers, and information about other goods, services, or events we offer that may be relevant to you, where permitted by law and unless you have opted out of receiving those communications.
- **Marketing and Publicity:** We will not use your name, image, testimonial, care information, or identifiable service experience in case studies, public references, testimonials, or promotional material without appropriate consent. You may withdraw consent for future marketing use at any time.
- **To manage your requests:** To respond to and manage enquiries, support requests, complaints, feedback, and other communications you send to us.
- **For business transfers:** We may use your information to evaluate or carry out 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 insolvency, liquidation, or a similar process, where personal information held by us about service users is among the transferred assets.
- **For other purposes:** We may use your personal information for other legitimate business and service-related purposes, including data analysis, identifying usage trends, measuring the effectiveness of communications, and evaluating and improving the Vitara CarePilot service, companion mobile app, support services, website, and customer experience.
 - We will only send marketing communications where permitted by law and, where required, with your consent. You can opt out at any time by using the unsubscribe link in our emails or by contacting us directly.

We may share your personal information in the following situations:

- **With service providers:** We may share your personal information with service providers who help us operate, support, maintain, monitor, analyse, or improve the Vitara CarePilot service, or who assist us in communicating with you in connection with the service.
- **For business transfers:** We may share or transfer your personal information in connection with, or during negotiations for, a merger, sale of company assets, financing, acquisition, restructuring, or similar business transaction involving all or part of our business.
- **With affiliates:** We may share your information with our affiliates, including our parent company and related entities, where reasonably necessary for service delivery, support, administration, or other purposes consistent with this Privacy Policy. We will require those affiliates to handle your information in accordance with this Privacy Policy.
- **With installation and operational contractors:** We may share limited personal information with installation, maintenance, technology, and other operational contractors where reasonably necessary to deliver or support the Vitara CarePilot service. We require them to handle information securely and only for the authorised purpose.
- **With people you authorise:** Where you ask us to connect family members, carers, emergency contacts, or authorised representatives to the service, we may share relevant account, alert, incident, care, and service information with them according to their role, your settings, your consent, or other lawful authority. You can contact us to review or change authorised access where available.
- **With other users:** If you choose to share personal information in any public or shared areas of the service, that information may be visible to other users and may be further shared by them.
- **With your consent:** We may disclose your personal information for any other purpose where you have given your consent or where disclosure is otherwise permitted or required by law.



5. DATA PROCESSING, SHARING, AND INTERNATIONAL TRANSFERS

We process your personal data in accordance with applicable privacy laws, including the Privacy Act 1988 (Cth) and, where applicable, the General Data Protection Regulation (GDPR). Depending on the circumstances, we may rely on consent, contractual necessity, legal obligations, and legitimate interests where permitted by law.

To deliver the Vitara CarePilot service, we may use trusted third-party providers for cloud hosting and processing; analytics; marketing communications; payment processing; sensor technology; push notifications and email delivery; consultation scheduling; app diagnostics; and map and address services.

Australian data location

Primary customer and care recipient data is stored and processed in Australia using Microsoft Azure Australia East in New South Wales. This includes databases, files, secrets, system telemetry, the AI daily-summary service, and Australian backup copies.

Limited overseas processing

Some service providers operate in or from the United States, including providers of push notifications, payment processing, sensor technology, email delivery, and app diagnostics. Transient message transport through EMQX Cloud in Singapore and other limited provider flows are described in Schedule 1. Only the minimum information reasonably necessary for each purpose is shared.

Where personal information is processed internationally, we take reasonable steps to ensure it is handled securely and in accordance with this Privacy Policy and applicable law. Safeguards may include contractual protections and recognised transfer mechanisms. Third-party providers handling personal information on our behalf are required, where appropriate, to meet privacy, confidentiality, and security obligations.

Australian data residency commitments

Care Recipient identity and the mapping between a Care Recipient and deviceID remain in Australia. Identifiable personal information is not processed offshore except where required by law or as described in this Privacy Policy and Schedule 1 for the limited operation of the service.

Vayyar Cloud hosting

Vitara CarePilot uses Vayyar technology and related cloud services to operate its sensors. Relevant Vayyar services operate in or from the United States. Only minimised technical sensor, event, telemetry, diagnostic, and operational data may be transmitted to or processed by Vayyar; direct identity information is not included.

Vayyar Cloud may receive technical Event Message and Telemetry Data that is minimised and pseudonymised within the Vayyar Cloud environment. This data may not, within Vayyar Cloud, be directly linked to a person's name, address, account number, or other direct identity details. However, Vitara CarePilot systems or authorised user accounts may associate a deviceID with a care recipient, room, service address, account, or care network so the service can operate, deliver alerts, support authorised care coordination, and provide service reports.

Where that association makes information identifiable or reasonably identifiable, Vitara CarePilot will handle it as personal information under this Privacy Policy. Under certain circumstances, the Company may be required to disclose your personal data if required to do so by law or in response to a valid request from a court, regulator, or other public authority.



Sensor message transport - EMQX, Singapore

Event Message Data and Telemetry Data generated by the sensors is transported from the sensor cloud to the Vitara CarePilot backend in Australia using a managed message-transport service, EMQX Cloud, hosted in Singapore. This service is used for message transport between systems. The messages contain deviceIDs and technical event data, such as event type, status and coordinates, and do not contain a Care Recipient's name or direct identity.

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

You may request access to, correction of, or deletion of personal information we hold about you in accordance with the Privacy Act 1988 and other applicable laws. Where available, you can update or delete certain information through your account settings, or contact us to make a request.

When you delete your account, we will close your active account, end active sessions, and remove your profile and sign-in access from the active service.

Some information associated with your account may need to be retained after account closure. This may include incident, activity, audit and other records relating to a Care Recipient where those records are required for other carers, the Care Recipient, safety reviews, or to meet legal, regulatory, security, accounting, incident-management, dispute-resolution or other record-keeping requirements.

Where we are required or permitted to retain information, we may not be able to delete it immediately. Any retained information will be handled in accordance with the retention periods in section 17, will no longer be available through your closed account, and will only be used for the purposes for which it is retained.

Where appropriate, we will take reasonable steps to explain why information must be retained and any restrictions that apply to its use.

7. DISCLOSURE OF YOUR PERSONAL DATA

Business Transactions

If the Company is involved in a merger, acquisition, restructuring, or asset sale, your personal data may be transferred as part of that transaction. We will provide notice before your personal data becomes subject to a different privacy policy, where required by law.

Emergency Disclosure

In an emergency situation, relevant care recipient emergency and care-related information may be disclosed to emergency services or responders where reasonably necessary to help protect the care recipient or another person, where the care recipient's consent has been recorded in the Service, or where such disclosure is 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 a valid request from a court, regulator, or other public authority.

Other legal requirements

The Company may disclose your personal data where reasonably necessary to:

- comply with a legal obligation
- protect and defend the rights, property, or operations of the Company
- prevent, detect, or investigate possible wrongdoing in connection with the Service
- help protect the safety of users of the Service or other persons
- respond to or defend legal claims



8. SECURITY OF YOUR PERSONAL DATA

We protect personal data through TLS 1.2 minimum, HTTPS-only transmission, encrypted app-to-database connections, AES-256 encryption for databases, files, and all backups, and secrets held separately in an Australian vault. Access controls include a complex password of at least 12 characters, one-time email verification before first sign-in, and optional Face ID, Touch ID, or PIN on supported devices. We log care-data access, sign-in and security events, and alert acknowledgement and resolution, with security monitoring every 15 minutes.

We also use automated code and dependency scanning, internal security reviews, tested backup restores, and anonymisation or pseudonymisation where appropriate. No internet transmission or electronic storage system is completely secure, so we cannot guarantee absolute security.

9. DATA BREACH NOTIFICATION

If we become aware of an eligible data breach or any other security incident affecting personal information, Vitara Guardians will take reasonable steps to contain, assess, and respond to the incident in accordance with applicable privacy and data protection laws, including the Notifiable Data Breaches scheme under the Privacy Act 1988 (Cth) and, where applicable, the General Data Protection Regulation (GDPR).

Where required by law, we will notify affected individuals and any relevant regulator or authority as soon as practicable, and provide information about the nature of the incident, the types of information affected, and any recommended steps individuals can take to help protect themselves.

Where a data breach or security incident affects your personal information, we may contact you using the account contact details or service channels available to us. Where another person is authorised to manage the affected account or care recipient profile, we may also notify that authorised person where lawful and appropriate.

While we take reasonable steps to protect personal information and respond to security incidents, no system or method of transmission is completely secure. Nothing in this Privacy Policy limits any rights or remedies you may have under applicable law.

10. PROTECTION OF MINORS & VULNERABLE INDIVIDUALS

The Service is not intended for individuals under the age of 13, and we do not knowingly collect personal information directly from anyone under that age. If you are a parent or guardian and become aware that a child has provided us with personal information, please contact us immediately.

If we become aware that personal information has been collected from a child under 13 without any required parental or guardian consent, we will take reasonable steps to delete that information from our systems, unless we are required or permitted by law to retain it.

In addition to safeguarding minors, we are committed to protecting the privacy and security of vulnerable individuals who may use or be connected to the Vitara CarePilot service.



11. GDPR COMPLIANCE STATEMENT

Vitara Guardians is committed to handling personal data in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR), where applicable, including in relation to individuals located in the European Economic Area (EEA).

This section of our Privacy Policy outlines the principles we follow, the legal basis for processing personal data, the rights available to data subjects under the GDPR, and how those rights may be exercised.

12. PRINCIPLES OF DATA PROCESSING

We apply the following core principles when processing personal data:

Lawfulness, Fairness, and Transparency

We process personal data lawfully, fairly, and transparently, and provide clear information about how it is used.

Purpose Limitation

We collect and process personal data only for specified, explicit, and legitimate purposes.

Data Minimisation

We collect only the personal data reasonably necessary for those purposes.

Accuracy

We take reasonable steps to ensure personal data is accurate, complete, and up to date, and provide ways for you to request correction of inaccurate information.

Storage Limitation

We retain personal data only for as long as reasonably necessary to fulfil the purposes for which it was collected, to meet our legal and regulatory obligations, or to protect our legal rights.

Integrity and Confidentiality

We apply appropriate technical and organisational measures to help protect personal data against unauthorised access, disclosure, alteration, loss, misuse, or destruction.

Accountability

We are responsible for demonstrating compliance with applicable data protection requirements, including the GDPR where it applies.

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 fulfil 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 the Service, preventing fraud, and ensuring IT security, provided it does not override your rights.



14. YOUR GDPR RIGHTS

Where the GDPR applies, you may have the following rights, subject to applicable conditions and exemptions:

- **Right of Access (Article 15 GDPR):** You may request confirmation of whether we process your personal data and access a copy of that data, together with information about the processing.
- **Right to Rectification (Article 16 GDPR):** You may request correction of inaccurate personal data and completion of incomplete personal data.
- **Right to Erasure ("Right to Be Forgotten") (Article 17 GDPR):** You may request the deletion of your personal data in certain circumstances, including where:
 - the personal data is no longer necessary for the purposes for which it was collected or processed
 - you withdraw your consent, and there is no other lawful basis for the processing
 - the personal data has been processed unlawfully
 - erasure is otherwise required under applicable law
- **Right to Restriction of Processing (Article 18 GDPR):** You may request that we restrict the processing of your personal data in certain circumstances, including where:
 - you contest the accuracy of the personal data, for a period enabling us to verify its accuracy
 - the processing is unlawful and you request restriction instead of deletion
 - we no longer need the personal data for the original purpose, but you require it for the establishment, exercise, or defence of legal claims
 - you have objected to processing and verification of overriding grounds is pending
- **Right to Data Portability (Article 20 GDPR):** Where applicable, you have the right to receive the personal data you have provided to us in a structured, commonly used, and machine-readable format, and to request that it be transmitted to another controller where technically feasible.
- **Right to Object (Article 21 GDPR):** You have the right to object to the processing of your personal data in certain circumstances, including where processing is based on:
 - legitimate interests
 - direct marketing purposes
- **Right to Withdraw Consent (Article 7 GDPR):** Where we rely on your consent to process personal data, you may withdraw that consent at any time. This will not affect the lawfulness of any processing carried out before your consent was withdrawn.
- **Right to Lodge a Complaint (Article 77 GDPR):** You have the right to lodge a complaint with a relevant supervisory authority if you believe your personal data has been processed unlawfully or in breach of applicable data protection law.

If you are located in the EEA, you may contact your local data protection authority. If you are in Australia, you may contact the Office of the Australian Information Commissioner (OAIC).



15. DATA TRANSFERS OUTSIDE THE EEA

Where personal data is transferred outside the EEA, we implement appropriate safeguards as required by applicable data protection law.

Depending on the circumstances, these safeguards may include:

- Standard Contractual Clauses approved by the European Commission
- Binding Corporate Rules, where applicable
- an adequacy decision or another recognised contractual or legal transfer mechanism

You may contact us for more information about safeguards used for international data transfers.

16. AUTOMATED DECISION-MAKING AND PROFILING

We may use automated processing, including AI-assisted analysis, to help identify activity patterns, generate service-related insights, support alert functionality, and improve the Vitara CarePilot service.

Where automated processing is used, we are committed to transparency and to handling personal data in accordance with applicable privacy and data protection laws.

You will be informed about the use of these technologies where required, including how they may affect the information presented through the service.

Where applicable, we will:

- provide information about the use of automated processing in connection with the service
- explain the significance and potential effects of such processing where required by law
- offer the ability to request human review or intervention where applicable under relevant privacy or data protection laws

Our aim is to use automation in a fair, reasonable, and accountable way while supporting the operation and improvement of the Vitara CarePilot service.

17. RETENTION OF YOUR PERSONAL DATA

We will retain your personal data only for as long as necessary to fulfil 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)
Medical & emergency information (conditions, allergies)	Profile duration or until updated/deleted; backups: daily 35 days, monthly recovery up to 13 months. Encrypted, access restricted/logged, restoration-only, and automatically destroyed at expiry.	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)
Authorised user and care-network access records	Retained only for as long as reasonably necessary for account administration, security, safety, audit, and applicable legal obligations.	Performance of contract, legal obligation, and legitimate interests (account administration, security, safety, and audit).
Installation, maintenance, and service records	Retained only for as long as reasonably necessary to provide support, manage warranties and disputes, and comply with applicable legal obligations.	Performance of contract, legal obligation, and legitimate interests (service support, quality assurance, and dispute handling).



Longer Retention Where Required: We may retain personal information, sensitive information, sensor telemetry, activity events, incident records, alert logs, event histories, escalation records, service reports, audit records, support records, and compliance records for longer than the standard retention periods set out in this table where required by law, incident-reporting obligations, audit or insurance requirements, dispute resolution, or other legal obligations.

Where a longer period is required or permitted, we will retain only the information reasonably necessary and limit its use to the relevant legal, safety, audit, dispute, or compliance purpose.

We retain and use personal data to the extent reasonably necessary to comply with our legal and regulatory obligations, resolve disputes, and enforce our agreements and policies.

We may also retain Usage Data for internal analysis, service improvement, security, and operational purposes. Usage Data is generally kept for a shorter period, unless it is needed to help strengthen the security or functionality of the service, or where a longer retention period is required or permitted by law.

To request access to, correction of, or deletion of your personal data, please use your account settings where available or contact us at privacy@vitaracarepilot.com. We will respond within the timeframe required under applicable law.

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

The Service may contain links to third-party websites or services that are not operated by us. If you follow a third-party link, review that provider's privacy policy because we are not responsible for its content, privacy practices, or policies.

We may share personal information with selected third-party providers where reasonably necessary to operate, deliver, maintain, or improve Vitara CarePilot. These may include cloud service providers; analytics providers; payment processors; installation and sensor technology partners; push-notification and email-delivery providers; consultation-scheduling providers; app-diagnostics providers; map and address services; and providers supporting customer service and related functions.

Where personal information is shared, we take reasonable steps to ensure the recipient is subject to appropriate privacy, confidentiality, and security obligations under applicable law.

Integrated Third-Party Systems: Vitara CarePilot may integrate with external alerting, reporting, dashboard, payment, or other service-management systems operated by us or our service providers. Sensor outputs, event messages, alerts, technical data, service records, and related information may be shared with those systems only where reasonably necessary to deliver alerts, support authorised reporting, provide service functions, or maintain the Service.

For more information about how we handle personal information, please refer to this Privacy Policy or contact us directly.



19. CHANGES TO OUR PRIVACY POLICY AND ONGOING ASSESSMENTS

We may update this Privacy Policy from time to time to reflect changes in legal or regulatory requirements, business practices, technologies, or the Vitara CarePilot service. We review this Privacy Policy periodically, including whenever significant operational or regulatory changes occur, to help ensure it remains accurate and up to date.

Where required by law, or where changes are material, we will notify you by email, through the service, or by a prominent notice on our website before or when those changes take effect. We will also update the effective date shown in this Privacy Policy.

We encourage you to review this Privacy Policy from time to time so you remain informed about how we collect, use, and protect personal information.

As part of our ongoing privacy and data protection practices, we may carry out Privacy Impact Assessments or similar internal reviews to assess how new projects, technologies, or service changes may affect personal information. These reviews help us identify potential privacy risks and support compliance with applicable privacy laws and good privacy practices.

20. PERSONALISED PRIVACY CONTROLS

We aim to give you clear and practical ways to understand and manage how personal information is collected, used, and handled in connection with the Vitara CarePilot service.

Depending on the part of the service you are using, available privacy controls and information may include:

- **Role-Based Access Controls** - Access to personal information is limited to authorised personnel and service providers who need that access for service delivery, support, security, or compliance purposes.
- **Privacy Information and Notices** - Clear information about how personal information is collected, used, and shared is provided throughout the service and related interactions.
- **Permission Management** - Where available, you can review and manage relevant permissions connected to your account, device, or service interactions.
- **Account and Communication Preferences** - You may be able to manage certain account settings, communication preferences, or consent choices through your account or by contacting us directly.

21. HOW TO LEARN MORE

We have designed this Privacy Policy to be clear and easy to navigate. Below are key areas to help you better understand how personal information is handled in connection with the Vitara CarePilot service:

- **What We Collect and Why:** Learn about the types of personal information we collect and the purposes for which it is used.
- **How We Share Your Information:** Understand the circumstances in which personal information may be shared, including with trusted service providers and where required by law.
- **Your Rights and Choices:** Learn how to request access to, correction of, or deletion of personal information, and how to exercise other applicable privacy rights.
- **Data Security:** Learn about the steps we take to help protect personal information.



22. YOUR RIGHTS, CHOICES, AND COMPLAINTS

You may manage certain consent preferences through your account settings, where available, or by contacting us directly. Where consent is the legal basis for processing, you may withdraw that consent at any time. This will not affect the lawfulness of any processing carried out before consent was withdrawn.

For the Vitara CarePilot service:

- You may request access to, correction of, or deletion of your personal data, subject to applicable law
- You may manage certain account, communication, or consent preferences through your account settings, where available, or by contacting us directly
- You may contact us directly if you have questions about how your personal data is used

Care Recipient Consent and Primary Carer Role

Where the primary carer enters or manages care recipient emergency and care-related information through the service, the primary carer confirms that 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.

The service records the consent status captured during onboarding. The primary carer may update or delete the care recipient's emergency and care-related information through the service, subject to any legal, operational, or technical limitations. Where we rely on explicit consent to process sensitive information, that consent may be withdrawn by updating or deleting the information through the service, where available, or by contacting us directly. Please note that withdrawing or removing this information may limit certain emergency-related functions of the service.

Where a primary carer or authorised representative sets up or manages the service for a care recipient, that person must confirm that the care recipient has provided consent, or that another lawful authority exists, for Vitara CarePilot to collect, use, store, and disclose the personal information, sensitive information, emergency information, sensor event information, telemetry data, alerts, incident records, service records, and care-related information reasonably necessary to provide the service. The person managing the account must provide only information they are authorised to provide and keep account permissions and consent details current.

Privacy Complaints

If you believe we have not handled your personal information in accordance with this Privacy Policy or applicable privacy law, please submit a written complaint to privacy@vitaracarepilot.com with details of your concern. We will acknowledge and investigate your complaint and aim to provide a substantive response within 30 days. If you are not satisfied with our response, you may contact the Office of the Australian Information Commissioner at oaic.gov.au.

We are committed to handling personal data responsibly and transparently. If you have any questions, concerns, feedback, or would like to exercise your privacy rights, please contact us at privacy@vitaracarepilot.com. We will respond within the timeframe required by applicable law.



23. INTERPRETATIONS AND DEFINITIONS

Interpretation

Defined terms have the meanings set out below. These definitions have the same meaning whether they appear in singular or plural form, unless the context requires otherwise.

Definitions

For the purposes of this Privacy Policy:

- **Account** means a unique account created for you to access and use the Vitara CarePilot service or related account functions.
- **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 interests, or other securities entitled to vote for election of directors or other managing authority.
- **Authorised User means a person who has permission from the account holder or Care Recipient, or is otherwise legally authorised, to access or manage specified parts of the Vitara CarePilot service.**
- **Care Recipient** means the individual connected to the Vitara CarePilot monitoring service whose personal information may be entered, managed, or used in connection with the service by a primary carer or other authorised person.
- **Co-carer** means an authorised user linked to the service who may access and use the Vitara CarePilot service in connection with the care recipient and the primary carer’s account.
- **Company** means Vitara Guardians and refers to “the Company”, “we”, “us”, or “our” in this Privacy Policy.
- **Companion App** means the Vitara CarePilot mobile application used in connection with the physical monitoring service, including alerts, account access, billing management, and other related service functions.
- **Cookies** means small files placed on your computer, mobile device, or other device by a website, containing details of your browsing activity on that website among their various uses.
- **Country** means Australia.
- **Device means** any device capable of accessing the service, including a computer, mobile phone, or tablet.
- **deviceID** means the unique identifier code associated with a Vitara CarePilot sensor.
- **Emergency and Care Related Information** means information recorded in connection with the service for emergency response or support purposes, including emergency contacts, emergency notes, and any disclosed medical conditions, allergies, medications, or other sensitive information provided by or on behalf of the care recipient.
- **Event Message Data** means technical sensor event data generated by the Vitara CarePilot sensors, which may include deviceID, event type, timestamp, event message identifier, event status, location coordinates where applicable, and device status where applicable.
- **Customer means an individual who purchases, subscribes to, or manages the Vitara CarePilot service for themselves or a Care Recipient.**
- **Customer Account means the account through which the Customer and any Authorised Users access and manage the Vitara CarePilot service.**
- **Personal Data** means any information relating to an identified or identifiable individual.
- **Primary Carer** means the authorised person responsible for the main account and for entering, managing, or updating information connected to the care recipient and the service.
- **Service Agreement means the terms, plan, order, subscription, or other direct agreement between Vitara CarePilot and a Customer for the service.**
- **Sensitive Information** means personal information that is treated as sensitive under applicable privacy law, including health information and other information requiring a higher level of protection.



- **Service** means the Vitara CarePilot physical monitoring service provided in connection with installed sensors, together with the companion mobile app, website, monitoring platform, and related support services described in this Privacy Policy.
- **Service Provider** means any third-party provider engaged by us to support the operation, delivery, maintenance, analysis, improvement, billing, installation, or support of the Vitara CarePilot service.
- **Telemetry Data** means technical sensor data generated by the Vitara CarePilot sensors, including diagnostic data, connectivity data, technical status data, and radar-based telemetry files used for troubleshooting, fault triage, service improvement, and incident review.
- **Usage Data** means information collected automatically when the service is accessed or used, including technical, device, diagnostic, and interaction information.
- **Website** means the Vitara CarePilot website and any related online pages or portals operated by or on behalf of Vitara Guardians in connection with the service.
- **You or Your** means the individual accessing or using the service, or a person authorised to act for a Care Recipient, as applicable.



SCHEDULE 1 — OFFSHORE PROCESSING SCHEDULE

This Offshore Processing Schedule describes the limited third-party data flows that may occur outside Australia.

Primary customer and care recipient data is stored in Microsoft Azure Australia East in New South Wales. Databases, files, secrets, system telemetry, the AI daily-summary service, and Australian backup copies remain in Australia.

Limited flows include United States-based or operated providers for push notifications, payments, sensor technology, email, app diagnostics, consultation scheduling, and map or address services, plus transient EMQX message transport through Singapore. We minimise and pseudonymise data; Care Recipient identity and deviceID mapping remain only in Australia. Details are set out below.

Service provider	Location	Data processed or transmitted	Purpose	Identifiability status
Microsoft Azure	Australia East	Care Recipient identity records, care records, alert records, incident records, escalation records, audit records, PHI access logs and account records	Primary hosting, storage and processing	In Australia. Not offshore.
Vayyar Cloud	United States	deviceIDs, radar Event Message Data, Telemetry Data, device configuration commands, and home Wi-Fi SSID and password for device setup only	Radar sensor operation and device administration	Pseudonymised telemetry using deviceID only. Wi-Fi credentials are household network-configuration data.
EMQX Cloud	Singapore	deviceIDs, Event Message Data and Telemetry Data for message transport only	MQTT transport hop from sensor cloud to Australian backend	Pseudonymised and transient. No storage. No Care Recipient name.
Resend	United States / Tokyo	Alert email content limited to alert type, room and time. No Care Recipient name.	Transactional alert and account email delivery	Minimised. No Care Recipient name.
Apple / Google services (push, diagnostics, maps)	Global / United States	Push tokens, alert metadata, crash/app diagnostics, map/address queries	Push delivery, app diagnostics and address lookup	Minimised or pseudonymised; no Care Recipient name
Stripe	Global / United States	Email, payment instrument and subscription metadata	Billing and payment processing	Standard payment processor data.

Identity-separation safeguard: A Care Recipient's name and a deviceID do not leave Australia together. The device-to-person mapping exists only in Vitara CarePilot's Australian database.

