Latest Effective Date: **27 October 2026** · Version 2026-10-27

Medi-AR – Data Management and Privacy Policy

This Data Management and Privacy Policy (hereinafter: **Policy**) regulates and explains the privacy practices of **Business Sprints Pty Ltd.** (registered: Mulgrave, VIC 3170, Australia; ABN: 78 141 341 406; hereinafter referred to as **BSPL**) in relation to the Medi-AR mobile applications for Android and iOS, the Medi-AR web viewer and web portal, and the related cloud services for the processing and visualisation of medical images (the **Service** or **Services**) provided by BSPL.

BSPL is committed to protecting your privacy. There are some ways that you might interact with BSPL, and the information you provide is often necessary for providing the Service. Please read this Policy carefully before using the Service. The terms of using the Service are set out in the Medi-AR Terms & Conditions (https://www.medi-ar.com.au/legal/terms-and-conditions/). This Policy is available at https://www.medi-ar.com.au/legal/privacy-policy/, publicly and inside the app.

This Policy is designed to address the Privacy Act 1988 (Cth) and the Australian Privacy Principles, the Health Records Act 2001 (Vic) where applicable, and the EU General Data Protection Regulation (EU) 2016/679 (**GDPR**) where its territorial scope is met, including for users in the European Economic Area.

1. Privacy contact and self-service

1.1. Most requests about your personal data can be completed by you, at any time, without contacting BSPL. Signed in to your account you may review all data BSPL keeps about you and your activity, remove single items or examinations, and delete your account:

- in the app: user menu > **My data & activity**;
- on the web, without installing or opening the app: https://backend.medi-ar.com.au/app/my-data (review), https://backend.medi-ar.com.au/app/delete-data (data deletion) and https://backend.medi-ar.com.au/app/delete-account (account deletion).

1.2. For any other request, question or complaint regarding this Policy, the privacy contact of BSPL is: **privacy@medi-ar.com.au**. BSPL responds within 30 days and verifies the identity of the requester where reasonably necessary to protect health information and account security.

2. Scope and responsibility

2.1. This Policy applies to personal data handled by BSPL in providing the Service. The allocation of privacy roles depends on how the Service is used.

2.2. **Direct use.** Where you create an account, upload an examination, or use the sharing and call features yourself, BSPL decides why and how that information is handled and is responsible for it as data controller

(GDPR) and as an APP entity (Privacy Act 1988 (Cth)).

2.3. **Provider-supplied examinations.** Where a radiology or healthcare provider sends an examination to Medi-AR under its own patient relationship, the provider remains the controller of the medical record and BSPL processes the examination on its behalf as processor under the applicable agreement (including, where the GDPR applies, a data-processing agreement under Article 28 GDPR). The provider's own privacy notice also applies, and a request about the provider's medical record shall be addressed to the provider. BSPL forwards such a request to the provider where it is received by BSPL.

3. Definitions

3.1. **Personal Data** means any information relating to an identified or reasonably identifiable living person, including online identifiers, device identifiers, IP addresses and pseudonymised data that can reasonably be re-associated with that person. "Personal data" and "personal information" have the same meaning in this Policy.

3.2. **Health Information** includes information about the physical or mental health of a person, and in particular medical imaging examinations, their DICOM metadata and the volumetric models (VLM) derived from them, while they identify or can reasonably identify a person. Health Information is Special Category Data under the GDPR and sensitive information under the Privacy Act 1988 (Cth).

3.3. **Anonymised Data** means data that has been irreversibly processed so that it no longer relates to an identified or reasonably identifiable person, and for which no key or other practical means of re-identification is kept.

3.4. **Data Subject** means the person whose personal data is being processed. All other terms, such as "data controller", "data processor", "processing" and "personal data breach", have the meaning given to them in Article 4 of the GDPR, and Australian privacy terms are interpreted consistently with the Privacy Act 1988 (Cth).

4. Principles

BSPL, during data processing, always pays attention to the principles specified below:

4.1. BSPL processes data lawfully, fairly and with transparency – in a way that anybody would reasonably expect;

4.2. BSPL limits the data processing to its purpose and processes the data only for the specific reason it collected them;

4.3. BSPL minimises the processed data and does not collect more than it needs;

4.4. BSPL does its best to make sure that any data it holds are accurate and adequate;

4.5. BSPL will not store personal data for longer than it needs to;

4.6. BSPL always processes data securely and confidentially, and it will not share personal information without the permission of you, as the Data Subject, except as described in section 9; and

4.7. BSPL does not sell personal data or Health Information.

5. Legal basis of processing

5.1. As the Data Subject uploads an examination to the Service by a specific, express act, the processing of the examination is based on the explicit consent of the Data Subject, given separately in the app when the account is created and recorded by BSPL (Article 6(1)(a) and Article 9(2)(a) GDPR; for Australia, consent under the Australian Privacy Principles and, where Victorian health information is handled, the Health Privacy Principles of the Health Records Act 2001 (Vic)).

5.2. The Data Subject may withdraw the consent at any time by deleting the examinations concerned or the account (section 1.1). Withdrawal does not make earlier lawful processing unlawful, but the features that need the Health Information stop working.

5.3. The account and the features the Data Subject uses are provided under the Terms & Conditions (Article 6(1)(b) GDPR, contract). The security of the Service and the investigation of faults rely on BSPL's legitimate interests (Article 6(1)(f) GDPR), and records that the law requires BSPL to keep rely on its legal obligations (Article 6(1)(c) GDPR).

5.4. For provider-supplied examinations (section 2.3), the lawful basis is the one the provider relies on for its patients, for example Article 9(2)(h) GDPR where its conditions are met.

6. Scope of data processed, purpose and duration of data management

Personal data processed	Purpose of data processing	Duration of data processing
Account data: e-mail address, password (stored only as a secure hash), two-factor authentication settings, country of registration, and the record of the consents given and of the versions of this Policy and of the Terms & Conditions accepted	Identification, contact, security of the account	Until the existence of the user account; the record of consents as an audit record (section 10.2)
Health Information uploaded by the Data Subject: medical images (e.g. CT, MRI,	Conversion, storage, rendering and delivery of the examination to the Data	Until the Data Subject deletes the

Personal data processed	Purpose of data processing	Duration of data processing
ultrasound, X-ray), DICOM metadata and the derived volumetric models	Subject in 3D and in augmented or virtual reality	examination or the account
Health Information supplied by a provider	Delivery of the examination the provider shared	As set by the provider (section 2.3)
Content created by the Data Subject: annotations, saved views and presets, labels, contacts	Providing the features used	Until the Data Subject deletes it or the account
Sharing and calls: the persons an examination is shared with, the invitation e-mails sent on behalf of the Data Subject, the participants and times of calls	Delivering shares, invitations and calls; accountability and billing	7 years. Call audio and video are never recorded.
Device and technical data: app version, device model and operating system, IP address and the approximate country derived from it, sign-in sessions, security events	Operating, securing and troubleshooting the Service	Sign-in sessions until the account is deleted; security records 7 years
Payment records of paid services (section 9.2)	Billing records required by tax and accounting law	7 years
Correspondence with BSPL (support and privacy requests)	Responding to the Data Subject	As long as needed to resolve the matter

6.1. **Device permissions.** The app asks for a device permission only when a feature the Data Subject chooses to use needs it, and for the narrowest access that works: the **camera** for the augmented-reality view and for video calls, the **microphone** for calls, and the device's own file or photo picker instead of broad access to the device storage. Camera and microphone input are used live and are not stored by BSPL.

6.2. **Sources.** BSPL collects personal data from the Data Subject directly, from a radiology or healthcare provider that sends an examination for the Data Subject, from a storage service the Data Subject chooses to connect, and automatically from the app where needed for the security, reliability and operation of the Service.

6.3. If the Data Subject uploads or shares another person's medical information, the conditions of the Terms & Conditions apply (the Data Subject must be authorised to do so).

7. Health Information

7.1. BSPL does not sell Health Information and does not use examinations, volumetric models or any other Health Information for advertising, marketing, data-broker purposes, cross-app or cross-site tracking, or for decisions about insurance, employment or creditworthiness.

7.2. The segmentation, rendering and annotation tools of Medi-AR are visualisation tools. BSPL does not use them to make solely automated decisions with legal or similarly significant effects on the Data Subject, and does not use identifiable or pseudonymised Health Information to train artificial intelligence or machine-learning models.

7.3. **Anonymised records.** BSPL may retain and use examination data for quality assurance and the improvement of the Service only after it has been fully anonymised (section 3.3), in line with recognised de-identification standards (such as DICOM PS3.15 Annex E) and, for provider-supplied examinations, only where the agreement with the provider permits it. Anonymised Data is no longer Personal Data and is not used to identify, contact or make decisions about any person; BSPL does not attempt to re-identify it. Any use of Health Information that is not anonymised for such purposes requires a valid legal basis, the separate and optional consent of the Data Subject and, where required, ethics approval.

8. Storage and Security of Personal Data and recourse to data processors

8.1. BSPL stores Health Information electronically in cloud infrastructure, in a territorial server related to the (home) country of registration of the user. Data is encrypted in transit over public networks (TLS/HTTPS) and at rest.

8.2. BSPL, as data controller (and as processor where section 2.3 applies), shall involve the following data processors and service providers in the data management process as part of the Services:

Data processor	Role	Location
Amazon Web Services, Inc., 440 Terry Ave N, Seattle, WA 98109	Storage and processing of examinations and accounts	Frankfurt (EU) or Sydney (Australia), by the country of registration
Local server hosting	Application servers, database and e-mail delivery of the Service	Hungary and Australia
Cloudflare, Inc.	Relay of a call only when a direct connection between the devices is not possible; the media remains encrypted and is not recorded	Global network

Data processor	Role	Location
Stripe, Inc.	Processing of payments for paid services (section 9.2); BSPL does not receive or store full payment card details	Stripe's global infrastructure

8.3. Each data processor is bound to protect personal data to the same or an equal standard as this Policy, to keep it confidential, and to use it only to provide its service to BSPL. Where personal data of a Data Subject in the European Economic Area is transferred outside it, BSPL relies on the safeguards recognised by the GDPR, such as the standard contractual clauses of the European Commission.

8.4. BSPL reserves the right to add further data processing entities in the data management process, which will be communicated to you as Data Subject by amending this Policy.

8.5. **Platform services.** On Android, the augmented-reality view runs on **Google Play Services for AR (ARCore), which is provided by Google LLC and governed by the Google Privacy Policy** (https://policies.google.com/privacy). On iOS, the augmented-reality view uses Apple ARKit, and the camera image is processed on the device. A storage service the Data Subject chooses to connect (for example Dropbox) is governed by its own privacy policy.

8.6. **Security.** BSPL uses technical and organisational safeguards appropriate to the sensitivity of Health Information: encryption at rest and in transit, least-privilege access, strong authentication of administrators, logging and monitoring. Authorised staff may access data only where needed to operate, secure or support the Service, under confidentiality obligations. No system is perfectly secure.

8.7. **Data incidents.** BSPL has procedures to assess and respond to suspected data breaches and notifies the affected Data Subjects and the regulators where required, including under the Australian Notifiable Data Breaches scheme and, where applicable, the GDPR.

9. Sharing of data

9.1. Access to the data is restricted to natural persons who are the data controller itself or those who are employed or otherwise in legal relationship with the data controller with the aim of providing the Services. Data is disclosed outside BSPL only:

- (a) at the direction of the Data Subject, for example when an examination is shared or a call participant is invited;
- (b) to the radiology or healthcare provider that supplied the examination and its authorised users;
- (c) to the data processors listed in section 8.2;
- (d) to a third-party service the Data Subject orders (section 9.2), to the extent that service needs it;
- (e) to a storage service the Data Subject chooses to connect;

- (f) where the law requires or authorises it, in particular to public bodies in exceptional, legally binding cases; and
- (g) in a merger, acquisition or sale of the business, with continued protection of the information under this Policy.

9.2. **Paid and third-party services.** Paid services (such as call service plans, service subscriptions, or third-party services such as a second-opinion radiology report or an AI/CAD analysis) are ordered through the central payment system of BSPL, outside the mobile apps, and the payments are processed by Stripe. When the Data Subject orders a third-party service, BSPL provides the third-party provider only with the examination and the data that service needs, under confidentiality and data-protection terms.

10. Retention and account deletion

10.1. If you created a Medi-AR account, you can delete the account and its associated data from within the app (user menu > My data & activity > Delete account) and, without installing or opening the app, at https://backend.medi-ar.com.au/app/delete-account. Before confirming, the page shows exactly what will be removed. Deletion takes place immediately once the Data Subject confirms it with the code sent to the e-mail address of the account, and removes the account, the sign-in data, the uploaded examinations and the content created by the Data Subject from the systems of BSPL and its storage providers.

10.2. Where BSPL must keep some data for security, accountability, or legal, financial or regulatory reasons, it separates that data from the deleted account and keeps only what is required:

- (a) security and audit records, including the record of the consents given: 7 years;
- (b) billing records, including the records of calls: 7 years;
- (c) examinations supplied by a provider, which remain with the provider under its own retention obligations; and
- (d) encrypted, access-restricted backups, which are overwritten within 30 days; deletion is reapplied if a backup is ever restored.

11. Data Rights

11.1. The Data Subject may request what Personal Data and Health Information is processed, and inquire about the legal basis, purpose, source and duration of the data processing, and to whom, when and under what authority BSPL has given access to the data. Most of this information is available to the Data Subject directly in **My data & activity** (section 1.1).

11.2. You as the Data Subject shall have the right to access the data, to request the correction or erasure of your Personal Data or Health Information, and to object to the processing. Where the GDPR applies, you also have the rights of restriction of processing, data portability and withdrawal of consent, subject to the limits of the law.

11.3. If you want to exercise any rights described above, please use the self-service options of section 1.1 or contact **privacy@medi-ar.com.au**. Where BSPL acts only as a provider's processor, a request about the provider's medical record is referred to the provider (section 2.3).

11.4. You may complain to BSPL. If you are not satisfied with the answer, you may complain to the Office of the Australian Information Commissioner (OAIC, https://www.oaic.gov.au) or, where the GDPR applies, to the competent data-protection supervisory authority.

12. Children

The Service is intended for users aged 18 and over. The examination of a child may be used only through the child's parent or guardian or a healthcare provider. The privacy rights remain with the person the information is about, subject to the rules for parents, guardians and authorised representatives.

13. Miscellaneous

13.1. This Policy may change from time to time when necessary to reflect customer feedback, changes in BSPL's projects and the Services, or legal changes. The latest effective date is highlighted at the top of this Policy, and the earlier versions remain available at https://www.medi-ar.com.au/legal/archive/. If there are material changes in this Policy, BSPL asks you in the app to review and accept the updated Policy before you next sign in. If a new use of Health Information requires your consent, BSPL obtains that consent before starting the new use.

13.2. For matters not regulated by this Policy, the GDPR shall govern for EU jurisdiction and the Privacy Act 1988 (Cth) for Australia, together with the Health Records Act 2001 (Vic) and other Australian state or territory health-privacy laws where applicable. Your rights to complain to regulators or courts are not limited by this Policy.

13.3. Medi-AR is not intended to be used as a medical device and is not approved for medical use; see the Terms & Conditions.