

## Privacy Policy

### IMT Based Chat Application ('Application')

#### Beam Communications Pty Ltd

1. This privacy policy ('**Policy**') outlines how we handle personal information/ personal data ('**Personal Information**'). The purpose of this Policy is to ensure that during the provision of services, we manage and protect Personal Information in accordance with relevant statutory and regulatory requirements. We believe that protecting the security and privacy of your Personal Information is important. This Policy explains how we collect, hold, use, and disclose ('**process**') your Personal Information. The Personal Information that we collect about you depends on the context of your interactions with us, the products, services, and features that you use, your location, and applicable law.
2. Personal Information is information or opinion about an individual from which they can be reasonably identified. The collection of Personal Information depends on the circumstances in which we are collecting it but only if it is fair and reasonable to do so. In most situations, we will collect Personal Information directly from the individual.
3. On occasions people other than an individual may provide Personal Information about an individual. For example, a company that contracts with us may provide an individual's contact details, which would include Personal Information, from that company.
4. Depending on the circumstances, we may collect Personal Information from or about or in relation to the individual in their capacity as a user of our Application, website visitor, contractor, or in some other capacity.
5. This Policy adopts the definitions outlined in the Privacy Act 1988 (Commonwealth of Australia) and the Australian Privacy Principles.
6. Unless otherwise specified in this Policy, a reference to we, our or us is a reference to Beam Communications Pty Ltd.
7. We may, from time to time, review and update this Policy to take account of new laws and technology, changes to our operations and practices and to make sure it remains responsive to any changes in the provision of our operations.

#### What we do

8. We provide market leading products and services, to provide mobile satellite solutions to all market sectors. In particular, we operate a communication service ('**Application**') to be used on the Iridium Communications System. You provide your mobile number in order to create an account for use of the Application. As part of our services in providing the Application, we collect and hold information regarding your communications on our servers so that your data can be readily accessed as part of the Application. All data on our servers is secured.
9. In providing the Application as part of our services, we also operate a business to support provision of the Application, including administrative and technical services.

#### Processing of Personal Information

10. The purposes for which we will process Personal Information will depend on our interaction with you. We will only use your Personal Information for the purpose we collected the information or for purposes that are related to that purpose and provided it is fair and reasonable for us to do so. We will only use your Personal Information for

another purpose if you provide consent or we are required or authorised by law to use it for that purpose and provided it is fair and reasonable for us to do so.

11. In some instances where we request Personal Information and that information requested is not provided, we may not be able to provide, or continue to provide, services to an individual.

#### Processing of Personal Information related to your use of the Application and related services

12. When using our Application, or related services (each a '**Service**'), we may process the following categories of Personal Information:
  - Your contact information, such as your mobile phone number;
  - Information submitted as part of a support request;
  - Further Personal Information that you may provide to us in the course of the supply of Services to you; and
  - Information on your use and/ or interaction with the Application, or our Services, including:
    - your device and user identifier including Satellite IMEI and/or smart device phone number;
    - user smart device dataset including information on your operating system including version, locale and type of device used;
    - sites and services accessed during your visit, the date and time of each visitor request;
    - user possessed messages including text, location and images; and
    - user communication metadata.
13. We process your Personal Information for the following purposes:
  - To provide the Application and our Services and functions which includes creating and administering your account, updating, securing, and troubleshooting, providing support, as well as improving and developing the Application and our Services;
  - To verify your identity in the course of providing support;
  - To answer and fulfill your requests or instructions;
  - As reasonably necessary to enforce the Policy, the EULA, for dispute resolution, mediation, to exercise, establish or preserve a legal claim or defence, to prevent fraud or other illegal activities and any Permitted General Situations in s16A Privacy Act and Permitted Health Situations in 16B Privacy Act;
  - As reasonably necessary to maintaining security of Application and our Services, prevent and detect security threats, fraud or other criminal or malicious activities; and
  - As reasonably necessary to ensure compliance with legal or regulatory obligations, our policies or industry standards.

#### Unsolicited information

14. We may be provided with Personal Information without having sought it through the means of collection outlined in this Policy. This is known as 'unsolicited information' and is often collected by the following:
  - postal letters, notes, documents (either misdirected or otherwise).
  - electronic– emails, SMS, electronic messages (either misdirected or otherwise).
  - Telephone enquiries.
  - Additional information provided to us that was not requested. This may include information supplied by police, government agencies, and medical professionals, including in emergency situations.

15. Unsolicited information collected by us will only be processed if it is considered as Personal Information that could have been collected by the means outlined in this Policy. If that unsolicited information could not have been collected by normal means, then we will destroy, permanently delete or de-identify the Personal Information as appropriate unless it is otherwise lawful and reasonable for us to process that Personal Information.

#### Sensitive Information

16. We only process Sensitive Information if:
- It is fair and reasonable for one or more of our functions, activities and operations, and we have the individual's consent;
  - It is fair and reasonable to protect the welfare of a person, including by preventing a serious medical or health scenario or threat to life, health, safety and physical and mental wellbeing of that individual;
  - a Permitted General Situation exists; and
  - a Permitted Health Situation exists.

#### **Disclosure of Personal Information**

17. We may disclose your Personal Information to other entities and persons for the purposes specified in this Policy. We take reasonable steps to ensure that these entities and persons are bound by confidentiality and privacy obligations in relation to the protection of your Personal Information.
18. We will only disclose your Personal Information for the purpose we collected the information or for purposes that are related to that purpose. Otherwise, we will only disclose your Personal information for another purpose if you provide consent or we are required or authorised by law to disclose it for that purpose and if it is fair and reasonable for us to do so.
19. In providing the Application, your Personal Information:
- a. will be disclosed to and may be received from the following entities:
    - Iridium Satellite LLC: a user message sent/ received over satellite has to pass through the Iridium network in the encoded form, however, Iridium does not have access to the content of your messages; and
    - AWS by Amazon Web Services Australia Pty Ltd (ABN: 63 605 345 891) or Amazon Web Services, Inc. 206 266 7010: The Application and data relating to our Services are hosted in AWS and all Personal Information and other data collected for the purpose of providing the Application and the Services are securely stored in AWS's data center(s).
  - b. may be disclosed to and may be received from the following entities:
    - GEOS Emergency Response by Garmin Ltd: In the event of emergency raised by a user, the Satellite device phone numbers, Satellite IMEI, user location information are generated at the user's device and delivered to IERCC on the user's behalf to assist the IERCC to manage the emergency event in timely manner;
20. We may disclose Personal Information without consent or in a manner that an individual would reasonably expect if:
- Service providers. That is, we may use contractors and other companies to perform functions on our behalf, such as IT-services. These entities process Personal Information only for the purpose of such services;

- Other third parties. That is, we may disclose Personal Information to other third parties in connection with complying with legal or regulatory obligations, or establishing, exercising or defending rights or claims (e.g., for court and arbitration proceedings, to regulators, law enforcement and government authorities, to lawyers and consultants);
  - The disclosure will lessen or prevent a serious threat to the life, health, or safety of an individual or to public safety;
  - A Permitted General Situation applies; or
  - A Permitted Health Situation exists.
21. Recipients of your Personal Information may be located outside of the country in which you reside, including in Australia where we are based. Our data centers that hold Personal Information are located in the United States of America.
22. We may disclose Personal Information, held about an individual for the purposes of delivering our services, for technical and administrative purposes. This may include to disclosure to the following:
- people providing technical and administrative services to us;
  - anyone who an individual authorises us to disclose information to; and
  - anyone to whom we are required or authorised to disclose the information to by law.
23. In addition, we use services that require Personal Information to be disclosed to those service providers, including service providers located around the world. That is, Personal Information about an individual may be disclosed to an overseas organisation in the course of the provision of services, for example:
- Google and Apple push notifications services
24. We will however take all reasonable steps not to disclose an individual's Personal Information to overseas recipients unless we:
- have the individual's consent (which may be implied);
  - have satisfied our self that the overseas recipient is compliant with the Australian Privacy Principles, or a similar privacy regime, or if there is a suitable agreement in place with the overseas recipient;
  - have formed the opinion that the disclosure will lessen or prevent a serious threat to the life, health, or safety of an individual or to public safety;
  - a Permitted General Situation applies;
  - a Permitted Health Situation exists; and
  - are taking appropriate action in relation to suspected unlawful activity or serious misconduct.

### **Storage of Personal Information**

25. Depending on your interaction with us, we may hold Personal information in a combination of hard copy and electronic files. For those using the Application, we will only hold Personal Information in electronic files.
26. We store Personal Information in a variety of formats including, but not limited to:
- databases.
  - hard copy and paper-based files.
  - personal devices, including laptop computers and mobile phones.
  - third party storage providers such as cloud storage facilities.
27. We take all reasonable steps to protect the Personal Information held from misuse, loss, unauthorised access, modification, or disclosure. Our staff, contractors, and stakeholders are required to respect the confidentiality of an individual's Personal

Information that they access, and the privacy of individuals, in the provision of services by or to us.

28. These steps include, but are not limited to:

- restricting access and user privilege of information being dependent on the person's role and responsibilities;
- ensuring staff do not share personal passwords
- ensuring hard copy files are stored in lockable filing cabinets in lockable rooms. staff access is subject to user privilege;
- ensuring access to our premises are always secured;
- ensuring IT and cyber security systems, policies and procedures are implemented
- ensuring staff comply with internal policies and procedures when handling the information;
- undertaking due diligence with respect to third party service providers who may have access to the Personal Information, third party contractors who are engaged to facilitate services and cloud service providers, to ensure as far as practicable that they are compliant with the Australian Privacy Principles or a similar privacy regime;
- the destruction, deletion, or de-identification of the Personal Information held that is no longer required for the purpose that it was collected unless required to be retained by any other laws.

### **Responding to data breaches**

29. We will take appropriate, prompt action if it has reasonable grounds to believe that a data breach may have or is suspected to have occurred. Depending on the type of data breach, this may include a review of our internal security procedures, taking remedial internal action, notifying affected individuals and regulators. If we are unable to notify individuals, we will publish a statement on our website and take reasonable steps to publicise the contents of this statement.

### **Cookies**

30. We may collect information in the form of 'cookies' about your visit to our website via 'cookies'. Cookies include information about the device you used to browse our website (such as browser type, version and language, and operating system), information about the pages viewed while browsing the website (pages visited, day and time of your visit, whether you used a search engine to find us, and referring website address), and some geographical information about what country and state you are in. This collected information is used solely for our internal purposes of gauging visitor traffic, trends and delivering personalised content to you while you are at our website.

31. If you wish, you can set your browser to reject cookies, or to notify you when you receive one in order to accept or reject such receipt in each instance.

### **Retention and Destruction periods**

32. Unless indicated otherwise at the time of the collection of your Personal Information, we destroy or otherwise de-identify your Personal Information if the retention of that Personal Information is no longer necessary for the purposes for which they were collected or otherwise processed, or to comply with legal obligations (such as retention obligations under tax or telecommunications laws, or court order).

- We retain your registered phone number and any association with satellite IMEI, as long as the Application is active. If the Application is not in use for 3 months, it will be deleted but retained in backups. The backups will then be deleted 90 days

following that period. At that time the registered phone number shall be deleted from backups along associations to satellite IMEI's;

- We retain your User possessed messages (texts, images) as soon as a message is successfully delivered to the message receiver with 30 days from the time the system received the message. If a message is not successfully delivered to the message receiver within 30 days, it will be deleted. We keep an image message for 30 days regardless the message is successfully delivered or not. After 30 days from the time the system receives the message, the image message will be deleted. Messages/ images and conversations are User possessed data and kept locally in the user's Application on a user's possessed smart device and outside of the Application; and
- We retain user conversation metadata (that is, data without message content) for 2 years from the time it is created. The user conversation metadata only shows message length, sender number, receiver number, timestamp, message status such as received/ delivered.

### **Quality of Personal Information**

33. We take all reasonable steps to ensure Personal Information processed is accurate, complete, and up to date, including at the time of using or disclosing the information.
34. If we become aware that Personal Information is incorrect or out of date, we will take reasonable steps to rectify the incorrect or out of date information.

### **Accessing and correction of Personal Information**

35. You have a right to access and correct your Personal Information, subject to exceptions allowed by law. If you would like to do so, please contact us using the contact details listed below in the 'Contact us' section.
36. We reserve the right to charge a fee for searching for, and providing you with access to, your Personal Information on a per request basis.
37. Upon receiving such a request, we may take steps to verify the individual's identity before granting access or correcting any perceived inaccuracy. If the rejection relates to a request/ application to change Personal Information, an individual may make a statement about the requested change, and we will include this statement with the relevant record.
38. To make a request/ application to access or to update any Personal Information, please contact our Privacy Officer in writing via email below. An applicant for access will be required to specify what information is sought to be accessed, corrected, or updated. We may charge a fee to cover the cost of verifying an application and locating, retrieving, reviewing, and copying any material requested. If the information sought is extensive, we will advise the likely cost in advance.
39. There may be occasions when access is denied. Such occasions would include where release of the information would have an unreasonable impact on the privacy of others, or where the release may result in a breach of a duty of care or competing obligation. If we cannot provide an applicant access to that information, we will provide the applicant with written notice explaining the reasons for refusal.
40. There are some exceptions to these rights regarding access and correction, as set out in applicable legislation.
41. The privacy and data protection laws in the jurisdiction in which you reside may entitle you to specific rights in relation to your Personal Information. In particular, and subject to the legal requirements, you may be entitled to the following

- Obtain from us confirmation as to whether or not your Personal Information is being processed;
- Access to your Personal Information;
- Correction of inaccurate Personal Information concerning you;
- Erasure of your Personal Information;
- Restriction of processing regarding your Personal Information;
- Data portability concerning Personal Information, which you actively provided;
- Object, on grounds relating to your particular situation, to further processing of Personal Information concerning you; and
- Withdraw your consent to our processing of your Personal Information.

## **Contact Us**

42. If you have a concern about your privacy, our compliance with applicable privacy laws, or a query on how we process your Personal Information, our Privacy Officer provides support with any privacy related issues and may be contacted at: [info@beamcommunications.com](mailto:info@beamcommunications.com).
43. We will respond to your query as soon as reasonably practicable. We may seek further information in order to provide a full and complete response.
44. We do not charge a fee for the handling of complaints.
45. If you are not satisfied with our response, you may also contact the Office of the Australian Information Commissioner. A complaint can be made using the OAIC online Privacy Complaint form or by mail or email. A referral to OAIC should be a last resort once all other avenues of resolution have been exhausted. Otherwise, you always have the right to approach the competent privacy or data protection authority based on your location with your request or complaint.

## **Processing under the EU's General Data Protection Regulation, and under the United Kingdom's Data Protection Act 2018 and the UK GDPR**

46. This section applies and provides you with further information if your personal data is processed and you are located in the European Economic Area.
47. This section also applies and provides you with further information if your personal data is processed, and you are located in the United Kingdom, under the Data Protection Act 2018 and/or the UK GDPR (meaning Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018).
48. A reference in this section to the General Data Protection Regulation also includes a reference to the UK GDPR.

### Data Controller - Application

49. We, as the provider of the Application are the operator of the Application and the data controller in the meaning of the General Data Protection Regulation for the processing activities described in this Policy.

### Legal basis of the processing

50. The General Data Protection Regulation requires us to provide you with information on the legal basis of the processing of your personal data.

51. The legal basis for our processing data about you is that such processing is necessary for the purposes of the following:
- exercising our rights and performing our obligations under any contract we make with you (Article 6(1)(b) General Data Protection Regulation) (**'Contract Performance'**);
  - Compliance with our legal obligations (Article 6(1)(c) General Data Protection Regulation) (**'Compliance with Legal Obligations'**); and/or
  - Legitimate interests pursued by us (Article 6(1)(f) General Data Protection Regulation) (**'Legitimate Interest'**). Generally, the legitimate interest pursued by us in relation to our use of your personal data is the efficient performance or management of
    - your use of the Application, and/or
    - our relationship with you.
52. Where the below table states that we rely on our legitimate interests for a given purpose, we are of the opinion that our legitimate interest is not overridden by your interests and rights or freedoms, given the following:
- the regular reviews and related documentation of the processing activities described in this Policy;
  - the protection of your personal data by our data privacy processes;
  - the transparency we provide on the processing activity; and
  - the rights you have in relation to the processing activity. \
53. If you wish to obtain further information on this balancing test approach, please contact us at: [info@beamcommunications.com](mailto:info@beamcommunications.com).
54. In some cases, we may ask if you consent to the relevant use of your personal data. In such cases, the legal basis for us processing that data about you may (in addition or instead) be that you have consented (Article 6(1)(a) General Data Protection Regulation) (**"Consent"**).

Purpose	Basis
<b>Processing of personal data in the context of the Application services</b>	
To provide the Application and related Services and functions which includes creating and administering your account, updating, securing, and troubleshooting, providing support, as well as improving and developing our Application and related Services	<b>Contract Performance</b> (Article 6(1)(b) General Data Protection Regulation)  <b>Legitimate Interest</b> (Article 6(1)(f) GDPR)
To answer and fulfill your requests or instructions	<b>Contract Performance</b> (Article 6(1)(b) General Data Protection Regulation)  <b>Legitimate Interest</b> (Article 6(1)(f) GDPR)
As reasonably necessary to enforce the Policy, the EULA, to establish or preserve a legal claim or defence, to prevent fraud or other illegal activities, including attacks on our information technology systems	<b>Compliance with Legal Obligations</b> (Article 6 (1) (c) GDPR)  <b>Legitimate Interest</b> (Article 6(1)(f) GDPR)

Communicating about our Application or Services e.g. by responding to inquiries	<b>Contract Performance</b> (Article 6(1)(b) GDPR)  <b>Legitimate Interest</b> (Article 6(1)(f) GDPR)
Performing and managing the relationship	<b>Contract Performance</b> (Article 6(1)(b) GDPR)  <b>Compliance with Legal Obligations</b> (Article 6(1)(c) GDPR)
Day-to-day operations including training our staff;  Systems development; developing new programs and services; undertaking planning, research, and statistical analysis;  The engagement of contractors.	<b>Contract Performance</b> (Article 6(1)(b) GDPR)  <b>Compliance with Legal Obligations</b> (Article 6(1)(c) GDPR)  <b>Legitimate Interest</b> (Article 6(1)(f) GDPR)
Maintaining security of our services, preventing and detecting security threats, fraud or other criminal or malicious activities	<b>Compliance with Legal Obligations</b> (Article 6(1)(c) GDPR)  <b>Legitimate Interest</b> (Article 6(1)(f) GDPR)
Ensuring compliance with legal or regulatory obligations, our policies or industry standards	<b>Compliance with Legal Obligations</b> (Article 6(1)(c) GDPR)  <b>Legitimate Interest</b> (Article 6(1)(f) GDPR)
Dispute resolution, enforce our legal rights and to establish, exercise or defend legal claims.	<b>Compliance with Legal Obligations</b>  (Article 6(1)(c) GDPR) <b>Legitimate Interest</b> (Article 6(1)(f) GDPR)

#### International data transfers

55. As we transfer your personal data outside the European Economic Area, in particular to Australia, we ensure that your data is protected in a manner that complies with the General Data Protection Regulation and relevant data protection laws, including, if applicable, EU Standard Contractual Clauses, or a European Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC or Article 45 of the GDPR. In other words, your rights and protections remain with your data and we use approved contractual clauses and other measures designed to ensure that the recipients of your personal data protect it.

#### Your competent data protection authority

56. In case of data privacy related concerns and requests, we encourage you to contact our Privacy Officer at: [info@beamcommunications.com](mailto:info@beamcommunications.com).

57. Besides contacting the Privacy Officer, you always have the right to approach the competent data protection authority with your request or complaint.