AIZATRON

# THE PROTECTION OF PERSONAL INFORMATION ACT

# SMART BELL MOBILE APPLICATION

# CUSTOMER PRIVACY NOTICE

## 1) General

a) Aizatron recognises the importance of protecting your personal information and your right to having your personal information kept private. Aizatron ensures that it adheres to all data protection laws and has the implemented safeguards to ensure that your personal information is kept safe from unauthorised access.

b) This Privacy policy relates to the collection, use and retention of personal information you supply to us through your use of any of our Channels including but not limited to this mobile application, associated websites, mobile sites and other channels etc. This policy governs the manner in which your personal information will be dealt with.

c) This policy applies to all users of the Smart Bell Mobile Application (the "App") and forms part of the App's terms and conditions. By installing and registering for the App, you are agreeing to the terms of this policy.

## 2) Personal Information

a) Aizatron aligns its definition of "personal information" with that as set out in the Protection of Personal Information Act, 2013 (POPIA). All information specific to yourself and / or any of your approved contacts and / or associates that is provided to us via the App or any other channel will be classified as personal information. This includes but is not limited to personal information that is provided to us in the course of installation, registration and use of the App.

b) We do not collect personal information of minors i.e. persons under 18 or individuals that do not have legal capacity to act). Only users over the age of 18 and those with legal capacity may register for the App.

c) Where this App is obtained for a minor, their personal information will be collected through a competent person as defined in POPIA, their legal guardian or parent only and they may only use the App with the assistance of a parent or guardian who has provided consent.

d) You are responsible for any data you enter for completeness and correctness and it is entirely your responsibility to obtain consent of any individual, contact and / or associate whose personal information is uploaded to any of our Channels including but not limited to this mobile application, associated websites, mobile sites, and other channels etc. as applicable.

**3) Collection**

a) We collect and process the following categories and types of personal information, including:

- personal details :- your name and biometric information, specifically facial features / face data as well as similar information that relates to your authorised and listed contacts and / or associates. Only persons who have consented and agreed to their contact details, biometric information being shared with us may be added. It is your sole responsibility to obtain the necessary consent and we will presume that any person whose personal information that has been uploaded to this mobile application, associated websites, mobile sites, and other channels etc. has consented to his/her personal information being shared with us;

- contact details :- your email address;

- other related details:- your IMEI i.e. International Mobile Equipment Identity which is the unique 15-digit code that precisely identifies the associated device with the SIM card input, audio, alert history.

b) Our primary goals in collecting personal information from you are to:

- verify your identity;

- verify the identity of your approved contacts and / or associates;

- provide the services as described in the App;

- access your mobile device to send and/or receive invitations, notifications and / or alerts related to use of the App and to remotely allow access to premises of approved contacts and/ or associates;

- maintain our internal administrative or management systems, including the use of third party outsourced providers;

- data analytics i.e analyzing your information in order to optimize processes to increase the overall efficiency of the App;

- assist with internal record keeping;

- comply with any applicable law, court order, other judicial process, or the requirements of a regulator;

- use as otherwise required or permitted by law.

b) You undertake to keep the personal information up to date by keeping us informed of any changes that need to be made to the personal information.

**4) Disclosure of personal information**

a) We will only disclose your personal information:

- strictly for the purpose of providing the services described in the App;
- to verify your and / or your approved contacts and /or associates' identity;
- to courts, tribunals, regulatory authorities, and law enforcement officers as required by law, in connection with any actual or prospective legal proceedings;
- To third parties, including agents, sub-contractors or service providers such as Amazon Web Services (AWS), who may assist us in storing and safeguarding your personal information and providing services to you. This may include parties located outside of South Africa.

b) Where we disclose your personal information to third parties for these purposes, the third party will be obligated to take all reasonable and necessary measures to safeguard against unauthorised disclosures and may only use personal information in accordance with this Privacy Policy.

c) Aizatron has the highest regard for the privacy of its users and will only use the personal information obtained through the use of the App, for the purpose for which it was collected subject to the terms and conditions relating to the App.

**5) The use of Cookies**

a) Although we do not make use Cookies, we do use JWT Tokens. A JSON web token, or JWT for short, is a standardized, optionally validated and/or encrypted container format that is used to securely transfer information between two parties. The tokens are an authentication and authorization method used to validate the interaction/session between you, the user, and the App. Tokens are stored on your device when you log in. This allows the App to attach the tokens to backend requests to allow you to pass the security requirements needed to use the App.

b) The tokens by themselves cannot be used to discover your identity and will not damage your device. Use of the tokens are essential to effectively use the App.

**6) Your Rights:**

a) **Access to information**

i) You have the right to request a copy of the personal information we hold about you and / or your approved contacts and / or associates. To do this, simply contact us as provided below and specify what information you require. We will need to verify your identity before providing details of such personal information.

ii) Please note that any such access request may be subject to a payment of a legally allowable fee.

b) **Correction of your information**

i) You have the right to ask us to update, correct or delete your personal information. We will need to verify your identity before making changes to personal information we may hold about you and / or your approved contacts and / or associates.

ii) It is solely your responsibility to keep your personal information accurate.

**7) Protection of Information**

a) We value the information that you provide to us and will take all reasonable steps to protect your personal information from loss, misuse or unauthorised alteration. All personal information is stored in AWS cloud servers and databases situated in Oregon, USA which have built-in safeguards to ensure the privacy and confidentiality of your information.

b) Aizatron keeps up to date with latest developments in security technology and takes all reasonable and necessary measures to safeguard and protect your personal information.

c) We may use your personal information collected to compile profiles for statistical purposes in accordance with the Electronic Communications Transactions and Act 25 of 2002.

d) Accordingly, we retain all your data disclosed to us for a period of 5 years for historical, analytical, statistical and research purposes. We have established appropriate safeguards against the records being used for any unauthorised purposes and no information contained in the profiles or statistics will be able to be linked to any specific user. Should you however wish your data to be deleted, we shall do so within a reasonable time.

e) We also store the history of all alerts.

## 8) Information Security

a) We are legally obliged to provide adequate protection for the personal information we hold and to stop unauthorized access and use of personal information. We will, on an on-going basis, continue to review our security controls and related processes to ensure that your personal information remains secure.

b) Our security policies and procedures cover:

- Physical security;
- Computer and network security;
- Access to personal information;
- Secure communications;
- Security in contracting out activities or functions;
- Retention and disposal of information;
- Acceptable usage of personal information;
- Governance and regulatory issues;
- Monitoring access and usage of private information;
- Investigating and reacting to security incidents.

c) When we contract with third parties, we impose appropriate security, privacy and confidentiality obligations on them to ensure that personal information that we remain responsible for, is kept secure.

d) We will ensure that anyone to whom we pass your personal information agrees to treat your information with the same level of protection as we are obliged to.

## 9) Sharing of Information

a) We may be required to share your and / or your approved contacts and /or associates' full names and profile images to verify identity;

b) Other than the instances mentioned in this policy, Aizatron shall not disclose your personal information to any unauthorised third party unless your prior written consent is obtained or we are required by law to disclose your personal information.

c) If there is a change of control of our business or a sale or transfer of business assets, we reserve the right to transfer to the extent permissible by law our user databases, together with any personal information and non-personal information contained in those databases to a potential purchaser. We would seek to only disclose information in good faith and where we have sought to maintain confidentiality. If you are concerned about your personal information migrating to a new owner, you may request that your personal information be deleted.

**10) Contact us**

a) Please ensure that you have read and understood the terms and conditions of this Privacy policy before you provide us with your personal information.

b) We reserve the right in our sole discretion to amend this Privacy Policy from time to time. The amended version of the Privacy Policy shall supersede and replace all previous versions thereof.

c) You should check this page periodically to ensure that you are happy with any changes. Your continued use of our App following any such amendments will be deemed to be confirmation that you accept those amendments.

d) Should you have any questions relating to our Privacy Policy or if you believe that any information we hold on you is inaccurate, out of date, incomplete, irrelevant or misleading, please email us at ***connect@aizatron.com***. We will respond to any request within a reasonable time and will endeavour to promptly correct any personal information found to be incorrect.

**This policy is effective from 1 December 2021.**