Smartcom Business Communications Pty Ltd (Smartcom) is an Australian company registered with ASIC as ABN: 43 119 984 977. References in this document to 'we, us or our', refers to Smartcom.

1. Privacy Policy

The Privacy Act 1988 (Cth) (Privacy Act), and the Australian Privacy Principles (APPs) govern the way in which Smartcom must manage your personal information. This policy sets out how we collect, use, disclose and otherwise manage personal information about you. We recognise that your privacy is important and we are committed to protecting the personal information we collect from you. It is our intention to comply with the Privacy Act and the APPs.

2. Collection of Personal Information

We only collect personal information, that is, information that can identify you, in fair and lawful ways and only to an extent which is reasonably necessary for us to operate our business. Our primary purpose in collecting information is to provide products and services to our customers and fulfil our contractual obligations. In addition to this primary purpose, we will use the data for secondary administrative purposes. For clarity, administrative purposes includes things such as managing accounts and billing, assessing credit worthiness and managing business and product development.

We collect some types of personal information to assess your credit situation when you apply for Services.

In addition to secondary administrative purposes, we may use some information for tertiary marketing purposes. This means that we may contact you with offers we believe may be relevant to you. Nonetheless, you will always be able to 'opt-out', allowing us to use personal information that we collect for marketing purposes.(Refer Clause 9)

We may be required to collect information to comply with our obligations as a supplier of telecommunication and software services. This may be the collection of data mandated by law, regulation or at the order of a regulator or court.

If we are collecting personal information for another purpose, we will endeavour to make it clear why we are collecting the data, how it will be used or disclosed, and where you can get more information about how we protect your privacy.

Note: Telecommunications providers, have an obligation to retain certain network data and customer information (called 'metadata') for a period of at least two years for use by criminal law enforcement agencies. Refer https://www.ag.gov.au/dataretention for more detail.

3. Use of Personal Information Data

The personal information that we collect and hold about you, depends on your interaction with us. Generally, we will collect, use, and hold your personal information if it is reasonably necessary for, or directly related to the performance of our functions and activities and for the purposes notified to you, or as disclosed above. Our policy is to not use any information for purposes not connected to providing services or the good management and ongoing operation of our business without your consent, unless we are compelled to do so by law.

4. Information Generally Collected & its Purpose

We may collect and hold personal information about you that is relevant to providing you with the services you are seeking. While we may collect a wide variety of personal information from time to time, there are types of personal information which we are likely to collect from customers or people entering our premises. These include:

1. When customers submit an order form for a service, they provide us with information including their contact and identifying details (eg: ABN, ACN, registered address), the details of a representative and addresses for both billing and service delivery. This information is used for administrative purposes, including assessing whether we are able to deliver the service, assessing whether the delivery of the service to that customer might entail a credit risk and if the service is delivered, the information will be used to administer the account. We will also use the information to deliver the service and we may need to share the information with third parties in order to arrange for the service to be delivered.

2. Our facilities, including data centres, offices and other premise may be secured by monitored electronic locks which use access-passes or biometrics. Prior to receiving an access-pass, pass-holders will be required to provide their name, contact details and in some cases biometric information. This information along with the unique ID of access-passes will be used to keep record of access-passes for both security (eg: ensuring the pass allows access only to the extent necessary for the pass-holder) and administrative purposes (eg: invoicing for lost or damaged passes). Where biometric information is stored it shall be used exclusively for security purposes. We may allow third party security companies to access the information in connection with security work they undertake for us. We may allow law enforcement agencies to access the information in connection with investigations relating to our facilities.

3. Our facilities, which may include data centres, offices and other premises, are under video and camera surveillance. The personal information and image of people entering our facilities may be collected by us and stored for a reasonable period of time. We may also collect personal information and images from third parties (eg: landlords). The information will only be used by us in connection with security and management of our facilities, but may be provided to law enforcement agencies, government bodies, staff, subcontractors, insurers, tenants or landlords for use in connection with those purposes.

5. Method of Collecting Personal Information Data

Personal information will generally be collected directly from you through the use of any of our standard forms, over the internet, via email, through a telephone conversation with you, or upon you entering our premises. There may however, be some instances where personal information about you will be collected indirectly because it is unreasonable or impractical to collect personal information directly from you. We will usually notify you about these instances in advance, or where that is not possible, as soon as reasonably practicable after the information has been collected.

6. Failure to Provide Information

If the personal information you provide to us is incomplete or inaccurate, we may be unable to provide you, or someone else you know, with the services you, or they are seeking.

7. Internet Users

If you access our website/s, we may collect personal information about you in the form of your IP address or domain name. We also use system information arising from your use of our services for de-identified statistical analysis.

We use cookies or digital identifiers for a number of purposes, including enabling targeted advertising. You can clear cookies or digital identifiers from your device, and also disable future use of them by changing the security settings on your web browser, or in apps. However, doing this might mean that parts of Smartcom websites and apps may not work as they should.

Our websites may contain links to other websites. We are not responsible for the privacy practices of linked websites and likewise, any linked websites are not subject to our privacy policies and procedures.

8. Social Media

When you engage with Smartcom through social media platforms such as Facebook, Smartcom may need to collect and disclose personal information through these platforms in order to respond to your inquiry. The social media platform provider will however, handle personal information in accordance with its own privacy policy.

9. Opting Out

You can always control Smartcom's use of cookies and other similar technologies by clearing your cookies, or by using the do not track function on your browser. You can also reset your mobile device advertising identifier by using the settings in your device.

We'll ensure that any marketing emails, texts and letters we send you clearly tell you how to opt-out, or you can tell us by phone. Importantly, you can opt-out at any time.

When you opt-out, you can choose to opt-out of particular direct marketing, or all direct marketing. Of course, there are some types of marketing we can't control on an individual basis, like online ads that are not targeted specifically to you.

10. Third Party Relationships

Smartcom partners with third parties to provide some products and services. If you purchase a product or service that is delivered by one of our partners, we'll give them the personal information they need to both provide products and services; and manage their relationship with you.

We may also provide limited data to third parties to assist them to provide services to banks and other entities to help fight financial fraud.

If you lease a product from us, we may need to provide other companies with the personal information that they need to administer the lease.

We may need to send faulty goods that you have already taken delivery of, to third parties for assessment, repair or replacement.

If any of your goods are replaced with another device, or if you are returning a leased device, it may be on-sold, including overseas. With devices such as phones, you should ensure that you back-up your device and do a factory reset before you provide us with your device to be replaced. Note: If you don't, or can't do a factory reset, your device may still contain your data and personal information.

Further, you should make sure that you review the privacy policy of your device manufacturer, as the terms of that policy will apply to any personal information shared with them or contained on the device sent to them. Your device manufacturer may send your device overseas or allow access to your personal information from overseas, depending on the terms of their privacy policy.

In some circumstances, we may need to refer or sell overdue debts to debt collectors or other companies. If we do this, we'll give them secure access to the personal information they need to handle the debt.

We may also update credit reporting agencies about some types of payment defaults, although we'll always tell you before we do this.

We may work with third parties to provide some types of sales, business and customer support; and hence they may have access to systems that include your personal information. These companies are subject to strict controls that protect your information from unauthorised use or disclosure, and limit their access to your personal information to the extent necessary to do their job.

While we will take reasonable steps to limit the amount of personal information sent to parties e not based in Australia, we may disclose your personal information overseas to third party service providers.

11. Disclosure of Data to Third Parties
In some circumstances we may disclose personal information that we collect to third parties. You agree that we may disclose personal information which we collect to:

1. our related entities to facilitate our and their internal business processes;
2. third party service providers, who assist us in operating our business (including third party security companies), and these service providers may not be required to comply with our privacy policy;
3. Any related entity including any and all holding companies or subsidiaries and other organisations with whom we have affiliations so that those organisations may provide you with information about goods or services and various promotions;
4. Any unrelated third party which is acting on our behalf in relation to a matter directly connected to the information we collect; (eg; Credit Reporting Agencies);
5. Any third party where there is an imminent threat to public safety or to a person's life;
6. Any other party we are permitted to disclose the information to under law;
7. Any third party involved in the sale or transfer of our assets including unpaid debts.
8. You acknowledge and agree that the law may permit or require us to disclose the information we collect to a law enforcement agency, government agency, court or other party. Information which may be disclosed includes but may not be limited to;

    a. Subscriber and service information which must be disclosed to the IPND Manager to comply with our obligations as a supplier of telecommunications and software services;
    b. Communications which pass over or are stored on our network which are subject to an Interception or stored communications warrant.
    c. Where we disclose your personal information to a third party and it is appropriate and possible to do so we will take reasonable steps to ensure that our contracts with the third party require them to comply with the use and disclosure requirements of the Privacy Act 1988 (Cth) in relation to the personal information which we provide to them.

12. Information Quality
We will monitor how we collect and store personal information to identify if changes can be made to improve the quality of the information we collect. If we no longer require the information for the purposes we have disclosed we will take steps to either destroy or de-identify the information. We encourage you to update your details with us so we can deliver better service to you.

13. Security
We require that our employees and contractors perform their duties in a manner consistent with our legal responsibilities. We take reasonable steps to ensure that the personal information which we hold is available only to those who may reasonably require access to it and that that your personal information is stored safely to protect it from interference, misuse, loss, unauthorised access, modification or disclosure, including electronic and physical security measures. We will monitor how we secure the information and our policies regarding access to the information to ensure the information is kept securely.

14. Access & Correction
If we discover, or you notify us that any information is inaccurate we will take steps to correct that information as soon as practically possible. We will take reasonable steps to correct the information so that it is accurate, complete and up to date. If we refuse to correct your personal

information, we will provide you with a written notice that sets out the reasons for our refusal (unless it would be unreasonable to provide those reasons) and provide you with a statement regarding the mechanisms available to you to make a complaint.

We allow records which contain personal information about an individual to be accessed by that individual, upon request. We will respond to that request within a reasonable period. We may decline a request for access to personal information in circumstances prescribed by the Privacy Act, and if we do, we will give you a written notice that sets out the reasons for the refusal (unless it would be unreasonable to provide those reasons).

To access or correct your personal information you should contact your account manager. Where the records you are seeking access to, are complex or difficult to access, or you request access to the records more than once in a three month period, we reserve the right to charge on a costs only basis for access to the records (but not for making the request for access)

15. Complaints & Feedback

If you wish to make a complaint about a breach of the Privacy Act, the APPs or a privacy code that applies to us, please contact us using the details below and we will take reasonable steps to investigate the complaint and respond to you. If after this process you are not satisfied with our response, you can submit a complaint to the Office of the Information Commissioner. To lodge a complaint, visit the 'Complaints' section of the Information Commissioner's website, located at http://www.oaic.gov.au/privacy/privacy-complaints, to obtain the relevant complaint forms, or contact the Information Commissioner's office.

You can find out more about our complaint process and complaint handling policy on our website at; www.smartcombusiness.com/policies. If you make a complaint about privacy, we will acknowledge receipt of your complaint, and try to investigate and respond to you within 30 days. If you are unhappy with the outcome, you can lodge a complaint with the Telecommunications Industry Ombudsman or the Office of the Australian Information Commissioner.

If you have any questions or concerns about this privacy policy or the way we handle your personal information, please contact us at:

Street address: 36/71 Eagle Street, Brisbane QLD 4000
Email address: info@smartcombusiness.com
Telephone: 1300 196 386
Website: https://www.smartcombusiness.com

More Information

For more information about privacy in general, visit the Office of the Information Commissioner's website at www.oaic.gov.au.

For more information about the Telecommunications Industry Ombudsman (TIO) visit their website at www.tio.com.au.