



Commander Privacy Policy

Jurisdiction: National

Effective Date 1/07/2020

Commander Privacy Policy

The Commander brand (we, us, our) comprises M2 Commander Pty Ltd and M2 Energy Pty Ltd (trading as Commander Power & Gas). These companies are members of the Vocus Group, being wholly owned subsidiaries of Vocus Group Ltd (ABN 96 084 115 499) of Level 10, 452 Flinders Street Melbourne Victoria 3000.

We provide data, voice, electricity and mobile products and services to our customers with a focus on business customers. We are committed to protecting the privacy and personal information of our customers. This Privacy Policy describes the practices and processes we have in place to properly manage and safeguard that information.

Privacy laws that apply to us

We are required to comply with the Privacy Act 1988 (Cth) and are bound by the Australian Privacy Principles ('APPs') set out in that Act. The APPs establish minimum standards for the collection, use, disclosure and handling of personal information. They apply to personal information in any form, including written, verbal and digital form. The APPs can be accessed at the website of the office of the Australian Information Commissioner: www.oaic.gov.au

- We are also subject to other laws relating to the protection of personal information. Where we:-
- provide telecommunications carriage services, we are subject to privacy obligations under the Telecommunications Act 1997 (Cth);
- provide electricity and gas, we may be subject to requirements relating to the privacy of retail customer information;
- undertake direct marketing activities, we must also comply with the Do Not Call Register Act 2006 (Cth) and the Spam Act 2003 (Cth); and
- If we collect health information, we may be required to comply with statutory requirements relating to health records.
- In this Privacy Policy, unless the context otherwise requires:
- 'Privacy Law' refers to any legislative or other legal requirement that applies to our collection, use, disclosure or handling of personal information.

'Personal information' means information or an opinion about an identified individual or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether the information or opinion is recorded in material form or not. Personal information includes sensitive information.

'Sensitive information' means personal information about an individual's racial or ethnic origin, political opinions or memberships, religious beliefs or affiliations, philosophical beliefs, professional or trade association/union memberships, sexual preferences and practices or criminal record.

Whose personal information do we collect?

We collect personal information about individuals who are our:-

- Prospective Customers. This includes people we think may be interested in our products and services as well as people who have expressed interest in obtaining or learning more about those products and services, people who visit our webpages, and Current and Past Customers;
- Current Customers. This includes people who purchase our products or services or who hold an account with us; and
- Past Customers. These are people who have purchased our products or services but do not currently have an active account with us.

We will refer to these individuals collectively as 'customers'.

Can you deal with us without identifying yourself?

In some situations, customers and other individuals may be able to deal with us anonymously or using a pseudonym. For example, you can make a general inquiry to one of our call centres without providing any personal information. You may also make a complaint or log a service fault anonymously, unless the inquiry or complaint relates to a particular account.

However, please note that if you do not wish to be identified we may not be able to provide the information or assistance you require.

What personal information do we collect?

The personal information we collect will depend upon the nature of our customers' interactions with us. The personal information may include:

- name, date of birth, email address, telephone number(s) and residential address. For corporate and business customers, we may collect information about nominated contacts, including name and title or position, date of birth, telephone number(s) and email and business addresses;
- purchasing patterns, consumer preferences and attitudes for marketing purposes, including to analyse markets, develop marketing strategies and to identify and develop products and services that may be of interest to its customers;
- payment details (such as credit card or debit card details) provided when purchasing our products and services; and
- employment applications.

When you become, or apply to become, a Current Customer, we collect a range of other information that it needs to assess your application and manage your account(s). This includes:

- **Proof of identity information**, including passport number, driver licence number, Medicare number or other government identifiers. We need this information to ensure you are who you say you are, and to keep our customer records accurate and up-to- date. We also may be required to obtain proof of identity information by law. For example, the *Telecommunications Act 1997* requires us to obtain specified proof of identity information before providing mobile telephone services.

- **Financial and credit information**, including credit history, employment history, remuneration details, bank account and credit card information, information about assets and income and details of relevant court judgments and bankruptcies. We need this information to assess creditworthiness and financial suitability of Current Customers and Prospective Customers.
- **Information about certain medical conditions and concession entitlement.** Having a certain medical condition may entitle the person to concessional tariffs or other benefits that may be available with our products or services. For example, in the case of electricity and gas, we may need information about medical conditions to ensure secure power supply for medical devices.
- **Information relating to occupancy.** We may need information to establish a customer's right to occupy the property to which we provide services, and for this purpose may require copies of tenancy agreements, mortgage records or utility bills or supply records.
- **Information relating to change of name or status**, which may include marriage certificates, death certificates and other official documentation. We may need this information where we are asked to close or transfer an account.
- **Employment information**, including information about employment history including current and past employers. We may need this information to assess the financial position of a person who applies to become our customer.
- **Insurance information.** In providing insurance products and services, we may need to collect information to assess the risks of providing insurance, including information relating to pre-existing conditions, claims history and previous insurance.
- **Integrated Public Number Database (IPND).** In providing telecommunications services, we are required by law to collect certain personal information about you (including your name, address, telephone service number and other public number customer details), and to provide it to operator of the Integrated Public Number Database ('IPND') for inclusion in the IPND.

We also collect information about the way our customers use our products and services. This includes information about:

- service usage (including energy consumption patterns, use of communications services, internet usages);
- responses to offers made and/or promotions run by us or our affiliates;
- payment patterns and history; and
- inquiries and complaints.

We may collect personal information about associates of its customers, such as family members, employees or agents. For example, we may collect personal information about nominated or authorised representatives, the holder of a credit card that is used to pay a customer's account, a person who acts as a secondary account holder, a person who acts as guarantor for a credit contract, the landlord of a tenanted property or the nominated contact on a business account. If you supply us with personal information about another individual, we ask you to assist us by referring that person to this Privacy Policy.

We have adopted the position proposed by the Privacy Commissioner that a young person is able to give their consent when he or she has a sufficient understanding and maturity to understand what is being proposed. We will make an objective determination before collecting that information

as to whether the person involved would be able to provide informed consent to the use of their personal information.

We also collect personal information about individuals who are involved in providing our products and services. This includes:

- Our staff, and staff of other companies in the Vocus group; and
- Our service providers and suppliers, agents and affiliates, and their staff.

How do we collect personal information?

We collect information about Prospective Customers and Current Customers directly and via our agents, service providers and affiliates. We may collect this information:

- when you make an inquiry at a kiosk, dealer, or event, which is operated by us;
- through our door to door sales activities;
- through our call centres;
- through our websites, or websites operated by our affiliates;
- through social media platforms such as Twitter and Facebook; and
- through the purchase of marketing lists, databases and data aggregation services.

When you apply to become our customer, we will ask you to consent to us collecting information from particular third parties. We will only collect personal information from those parties if you consent. If you do not consent, we may not be able to provide the service or product you require. We are authorised to collect some personal information from third parties under Privacy Law.

We will handle any unsolicited personal information which it receives in accordance with its obligations under Privacy Law.

Why do we collect personal information?

We collect personal information in order to:

- provide products and services to customers;
- manage and administer the products and services we provide, including for billing and credit control purposes (which may involve identity verification, credit checking, assessing entitlement to concessions, supplying and servicing a product, connecting and administering a service, billing and collection in relation to the service and investigating and rectifying complaints or faults).
- Inform customers about changes and improvements in our products and services;
- create aggregate data through demographic profiling and statistical analysis of the database, and to allow for more efficient operations of our business;
- market our products and services to customers;
- market third party products and services to customers;
- manage job applications;

- manage relationships with our staff, contractors, agents, affiliates and service providers;
- establish, exercise or defend any legal claims; and
- comply with our legal obligations.

We need to use personal information for most of our business activities, although the information we require depends on the circumstances. If we are unable to collect the personal information we need, we may be unable to meet the expectations of our customers or provide the products and services they wish to receive.

The personal information we collect may be shared within the Vocus Group for the purposes outlined above.

Direct marketing

Personal information collected for direct marketing purposes will only be collected, used or disclosed with the consent of the customer, unless we cannot practically obtain the consent of a customer, in which case we will:

- include an 'unsubscribe' facility so customers can unsubscribe from the mailing list at any time; and
- provide details for customers to opt out of receiving further direct marketing communications; and
- Include a prominent statement to the fact that a customer may make such a request.

Direct marketing communications may be sent via post, e-mail, telephone, social media sites or other means.

Dealing with us online

Cookies

We store the Internet Protocol (IP) address of your computer when you visit our site. This information is used only to create broad demographic summaries of where our users come from.

Cookies are small units of data sent to a user's browser by a website the user visits. We use cookies to:

- facilitate the use of our website;
- improve our customers' website browsing experience;
- monitor and analyse our customers' use of our site and affiliated third party sites; and
- enable us to present customised messages and offerings to customers.

The cookies we use do not store any personal data or otherwise collect personal information. However, if an individual is logged into "Take Command" as a customer, the information we collect via cookies may be linked with their personal information.

You can configure your Internet browser to erase cookies from your computer's hard drive, block cookies or receive a warning before a cookie is stored.

If a user disables the use of, or deletes, cookies on their web browser then they may not be able to gain access to all the content and facilities of our websites.

Google Analytics

Our website(s) may use Google Analytics, a web analytics service provided by Google. Google utilizes the data collected to help us analyse how users use the websites. The information generated by the cookie about a customer's use of the website (including its anonymized IP address) will be transmitted to and stored by Google on servers in the United States. Google will use this information for the purpose of evaluating customer use of the website, compiling reports on website activity for website operators and providing other services relating to website activity and Internet usage.

Google will not associate your IP address with any other data held by Google.

We may combine information collected through Google Analytics with other information we collect, to enable us to provide you with relevant marketing content.

Use of remarketing tools

We may use Google remarketing, Facebook remarketing, pixel tags, web beacons, clear GIFs or other similar technologies to collect information of a customer's visit to any one of its websites and we may tailor advertising or content based on the customer's use of these sites. These advertisements may be delivered by third party vendors when you visit our websites or other Internet websites. You can opt-out of sharing information about your use of this site or affiliate third party sites by accessing the settings of your device or browser.

We collect information about the other websites that are visited by computers that are used to visit our site. This information may be aggregated to provide us with information about the webpages and websites visited by computers that use our site.

Note that this privacy policy does not apply to, and we are not responsible for, the use of, or the protection of information you provide to other websites linked from this website.

Do we disclose personal information to third parties?

We may disclose personal information about our customers to a range of third parties. For example:

- If we provide energy products and services, we may disclose personal information collected:-
 - For account management, provisioning and fault management purposes to the relevant electricity or gas distributor and to the operator of our billing and network management system Agility CIS System.
 - To the relevant Ombudsman or government body (Energy and Water Ombudsman (Victoria), Energy and Water Ombudsman (NSW), Energy and Water Ombudsman (Queensland) and Energy and Water Ombudsman (South Australia) (for complaint management purposes)).
- For telecommunications services, to the Telecommunications Industry Ombudsman (for complaint management purposes).
- To third party agents and service providers who we engage to provide our products and services, these may include:-

- sales agents and representatives;
- organisations that process banking transactions;
- organisations that process debt collection;
- printers, mail distributors, couriers and dispatch centres;
- call centres operated by entities outside the Vocus Group;
- IT service providers and data managers;
- legal, accounting, insurance and business advisory consultants services.

We may also disclose:-

- personal information to government agencies (such as Centrelink) for the purpose of establishing or verifying eligibility for concessions and similar entitlements.
- personal information for credit checking, collection or credit reporting purposes to a credit reporting agency or credit collection agency, in accordance with the requirements of the *Privacy Act 1988*.

Personal information we obtain in connection with the provision of telecommunications services may be disclosed in accordance with requirements of the *Telecommunications Act 1997 (Cth)* and the *Telecommunications (Interception and Access) Act 1979 (Cth)*. This includes disclosure:

- to the Telecommunications Industry Ombudsman for the purpose of complaint management;
- in connection with directory assistance, emergency service calls or other urgent services, and in particular to the operator of the IPND for inclusion in the IPND, including your name, address, telephone service number and other public number customer details. (Information in the IPND is used to develop directories and to assist emergency service organisations. If your phone number is unlisted, your information will be marked accordingly in the IPND and its use and disclosure will be strictly controlled.); and
- to law enforcement agencies for law enforcement or security purposes; and

Personal information we obtain in connection with the provision of electricity and gas services may be disclosed in accordance with federal and state based electricity and gas legislation and codes. This includes disclosure:

- to the various State based energy Ombudsmen identified above, for the purpose of complaint management;
- in connection with electricity and gas safety cases or other urgent services; and
- to law enforcement agencies for law enforcement or security purposes.

We may also disclose personal information if required by law.

Is personal information disclosed outside Australia?

We disclose some personal information to persons or organisations that are outside Australia.

- Our customer service and marketing call centre operations are managed by a third party organization which is based in Manila, Philippines. Personal information about Prospective, Current and Past customers may be accessed by this organization for the purpose of sales and marketing, managing credit information, customer service, correspondence, provisioning, fault management and technical support activities.

- Database and webhosting services provided to us involve personal information being transferred to IT service providers based in India, Philippines, Singapore, New Zealand, the United Kingdom, Canada and the United States of America.
- We may also supply customer credit history and information that it receives from its external Credit Reporting Organisations to third parties located outside of Australia, in order to perform credit related activities and manage customer services.

How do we protect your personal information?

We recognise the importance of protecting your personal information and of ensuring that it is complete, accurate, up-to-date and relevant.

When you call us in relation to your account or service, we complete an ID check to verify your identity and to check the details we hold about you are correct and to update them if required. For some safety critical information, for example medical information required to maintain secure power supply or ensure priority assistance, we initiate checks on an annual basis.

We have documented processes for verifying personal information collected for particular transactions, such as proof of occupancy, change of occupier and priority assistance. Our staff are trained to properly handle the different types of information they receive, particularly sensitive information. We have quality assurance measures in place to monitor calls to ensure that our processes are being followed.

While some of the personal information we collect is held in hardcopy form, most personal information is stored in electronic databases.

We have extensive processes in place to ensure that our information systems and files are kept secure from unauthorised access and interference.

We have contractual arrangements in place with our agents, service providers and affiliates that require them to comply with applicable privacy laws and our privacy policies. We require third parties who are outside Australia to handle the personal information we transfer to them with the same level of protection as would apply to the information in Australia.

Can you access or correct personal information we hold about you?

You have a right to access personal information we hold about you. You are also entitled to ask us to provide you with the details we have provided about you to the IPND. You can do this by contacting us and we will provide you with the information within a reasonable time (usually 20 business days).

If your request to access personal information is particularly complex or requires detailed searching of our records, the *Privacy Act* permits us to charge you a cost to provide you with this information.

We will provide access to the information held about an individual, including for the purposes of correcting or updating that information, unless there is an exception which applies under the APPs.

You have a right to ask us to correct information we hold about you if it contains errors or is out of date, incomplete, irrelevant or misleading.

We will make the corrections provided that any changes are in line with IPND requirements. We do not charge you to access or correct your information in the IPND.

Complaints and further information

If you would like to complain about a breach of the Australia Privacy Principles, you may contact our Privacy Officer at the details below.

The Privacy Officer will investigate your complaint and notify you of the outcome within a reasonable period of time (usually 30 days). If you disagree with our decision, you may refer your complaint to the Office of the Australian Information Commissioner (OAIC) by visiting www.oaic.gov.au/privacy/making-a-privacy-complaint.

If you would like further information on the way we manage personal information, would like to request access to or correction of personal information, or wish to make a complaint, please contact:

Privacy officer

Attention: The Privacy Officer

Address: Level 10, 452 Flinders Street Melbourne Victoria 3000

Changes to our privacy policy

We may review and revise our Privacy Policy from time to time. We may notify you about changes to this Privacy Policy by posting an updated version on our website. Please check our website from time to time to ensure you are familiar with our latest Privacy Policy.

Our Privacy Policy was last updated on July 2020.