Privacy Policy

JAGCAUS Pty Ltd trading as Pro Computers

Version 1.0 - 8 November 2021

1 About this Privacy Policy

1.1 We are committed to complying with our privacy obligations in accordance with all applicable data protection laws, including the Australian Privacy Principles contained in Schedule 1 to the Privacy Act 1988 (Cth).

1.2 If we decide to change this Privacy Policy, we will post the updated version on this webpage so that you will always know what personal information we gather, how we might use that information, where we store it and whether we will disclose it to anyone. Our policy is to be open and transparent about our privacy practices.

2 Our IT products and services

2.1 We provide a range of information technology products and services, including the sale of hardware, third party software subscriptions and licences, managed cyber security services, and technical support services (collectively, **services**).

2.2 Our customers are Australian companies. We enter into contracts with them for their subscription, licensing or use of one or more of our services and for our supply of software and hardware products to them. We do not enter into contracts with any end users of our services. End users are the personnel of our customers. End users are not our customers.

2.3 The functionality, technical specifications, products and services that we provide to our customers depend on the particular requirements set out in the contract with the customer.

2.4 Some of our services provide functionality that customers can collect, process and disclose personal information about their end users.

3 Customer responsibility for end user privacy

3.1 We rely on our customers to obtain all relevant privacy consents and authorisations from their end users required by applicable law for the personal information that is entered and transmitted via our services to be collected, disclosed and otherwise processed by us. We also rely on our customers to ensure that all of their end users' personal information held by us is accurate, up to date, complete, relevant and not misleading.

3.2 We rely on our customers to handle all notifiable data breach obligations under applicable law in respect of end user personal information that is jointly held by a customer and us.

3.3 We encourage our customers to ensure that their end users are familiar with the applicable customer's privacy policy so that their end users understand how they collect, use and otherwise process personal information about them.

4 The types of personal information we collect and hold

4.1 We collect the following types of personal information:

(a) Content entered into and transmitted via our services about end users: All information, including personal information, that is entered into and transmitted via our services (either by end users or otherwise) is stored in systems owned by us or third party vendors that is managed by us for our customers. The types of personal information collected may include names, contact details, as well as any other personal information

entered into and transmitted via the services by, about or on behalf of an end user. In the course of providing our services we may host or procure the hosting of customer databases or content. These databases and content may include personal information of end users.

(b) Information about customer personnel: We collect contact details of customer personnel, such as names, contact information and billing information. For customer personnel who are also end users, we also collect the information about them referred to in paragraph (a).

(c) Information about our suppliers and contractors: We collect personal about our suppliers and contractors in the course of engaging their services. The types of personal information we collect about them include names, contact details, addresses and occupation.

(d) Information required for the support, maintenance and security of our services: In order to support and maintain the products and services that we provide to our customers, we collect and process end user information, including IP addresses, email addresses, user access and security logs, usernames, passwords and any personal information included in technical support tickets and error messages.

(e) Managed services technical data: When providing our services, we may monitor or access customer or end users' computers, networks and other equipment remotely or on-site. In the course of doing so, we will collect and process information about that equipment and any software and data processed by that equipment. This information includes IP addresses, server names and addresses, database names, network names, serial numbers, WiFi passwords, computer names, application names, browser history, user access logs, usernames, passwords, technical support log tickets, bandwidth capabilities, error messages, social media handles, FTP server addresses, hostnames, subnet masks, router names, hosting account usernames and passwords and software subscription details. This information, either independently or when combined with other information, may identify a person.

(f) Computer and network usage data of our employees and contractors: As part of our recruitment and management of personnel and contractors, we collect and process all of the following personal information: names, phone numbers, ABN details, business and company names, residential addresses, professional references, information included on resumes, academic transcripts, employment history, skills and qualifications, national police checks and criminal history records, bank account details, tax file numbers, superannuation details and relevant identification documents (such as driver's licence and passports for visa and working permits). We also collect employee medical information, emergency contact details, dates of birth and next of kin details. Subject to applicable laws, we may carry out electronic surveillance of our personnel when they use our computer equipment, smartphone devices and networks (such as IP addresses, usage patterns, access logs and usernames, computer names, traffic firewalls, and websites visited).

(g) Domain name-related data: These records may contain, but are not limited to, the following information: the original creation date of a domain name registration, renewal, or request for service; the date and time of a registration or renewal application to us and by us to the proper registry; communications (electronic or paper form) constituting submissions, forwarding, modifications, or terminations of service and related correspondence between you and us; records of your account, including dates and amounts of all payments and refunds.

5 How we collect personal information

5.1 Our policy is to be completely transparent about how and why we collect personal information and not to collect personal information by means that are unfair or unreasonably intrusive.

5.2 We collect personal information about our and our customers' personnel in one or more of the following ways:

(a) when they contact us with enquiries about our services, whether by email, via our website or via telephone;

(b) during the preparation, negotiation and performance of our contracts for the provision of products and services and for billing purposes; or

(c) when it is voluntarily disclosed to us (including, but not limited to via telephone, email and online forms).

5.3 We will also collect personal information about end users in one or more of the following ways:

(a) when end users enter personal information into or via our services or third party systems that we manage and access in the course of providing our services;

(b) when a customer provides personal information to us about their end users; and

(c) when it is voluntarily disclosed to us (including, but not limited to via telephone, email and online forms).

5.4 We collect personal information about our employees, suppliers and contractors in one or more of the following ways:

(a) when we carry out background checks during the recruitment process or otherwise;

(b) when they respond to employment or contractor opportunities that we make available, enquire about available positions within our company, and when we conduct reference checks;

(c) when we trade business details with our suppliers and contractors;

(d) for workplace health and safety reasons;

(e) during the preparation, negotiation and finalisation of a contract that we enter into and for billing purposes thereafter; and

(f) when it is otherwise voluntarily provided to us;

6 How we use personal information

6.1 We use personal information about customers, their end users and our suppliers and contractors to enforce our legal rights, comply with our legal obligations and as otherwise set out in the following table:

Category	How we use and process that personal information	Our reason for collecting the personal information
Personal information about customer personnel	• To provide services to customers. • To set up, configure, host or procure the hosting of service for a customer and for end users to use the services. • To communicate with customers about their current and prospective use of our services, including with respect to their end users' current and anticipated usage of the services, and to discuss and	• Necessary for our legitimate interests (in order to operate, administer and grow our businesses, including to operate our services, IT systems and networks, manage our hosting environments and

	implement their software, security and hardware development requirements. • To provide data migration and implementation services in respect of databases that require integration into our services. • To provide customers with technical support and maintenance services, including by responding to help desk tickets, scheduling upgrades and enhancing our services. • To provide customers with professional services (including training, consulting and other services). • To send out billing information and notices and process payments. • To discuss our security requirements and to understand a customer's security requirements in respect of the services. • When conducting research and development of our products and services. • To provide customers with information about promotional offers and new products and solutions that we make available and to process orders for new or additional managed services and other services. • In order to identify a customer or end user when they contact us for technical support. • To administer our contractual relationships with a customer (and to enforce our contractual rights). • To streamline and personalise our customer experience and processes. • To configure new services for customers or to make changes to existing services, as requested. • To handle complaints.	ensure the successful delivery of our services). • Performance and enforcement of our contracts with our customers. • Compliance with our legal and statutory obligations.
Personal information about end users	• As required to provide and support the services supplied to customers and to process the personal information of end users on their behalf. • For data migration purposes. • In order to store end user personal information in databases and systems in our hosting environments at third party data centres. • To provide technical support services to customers and their end users that require us to view end user data held in our services. • When conducting research and development of our products and services.	• Performance of our contracts with a customer. • Necessary for our legitimate interests (in order to administer and our businesses including to allow a customer to operate our services, and to enable us to operate our IT systems and networks, manage our hosting environments and ensure the successful delivery of our services).

	• To configure new services or to make changes to existing services, as requested. • Backing up and restoring data that includes end user personal information. • To carry out security audits, investigate security incidents and implement security processes and procedures that require access to end user personal information. • To handle complaints.	• To comply with our legal and statutory obligations.
Personal information about our employees, suppliers and contractors	• To provide customers with the required products and services. • To manage and govern their employment or engagement with us as required to operate our businesses. • To send out billing information and notices to suppliers and contractors and process payments. • For workplace health and safety reasons (i.e. ensuring our contractors are adequately trained and safe). • When conducting the development of our products and services. • To procure new services from our suppliers and contractors. • When escalating technical support requests, procuring subscriptions on a customer's behalf and managing their licenses. • To handle complaints.	• Performance of our contracts with customers. • Performance of our contracts with our employees, suppliers and contractors. • Necessary for our legitimate interests (in order to administer and our businesses including to allow customers to operate our services, and to enable us to operate our IT systems and networks, manage our hosting environments and ensure the successful delivery of our services). • To comply with our legal and statutory obligations.
Domain name-related information	• We may disclose information to auDA, ICANN or any third party registry that we use to conduct your registration or renewal of any domain names. Registrant contact information related to a customer's domain name registration will be made publicly available via a searchable database (a whois service) in accordance with auDA's whois policy, which is updated from time to time and available at http://www.auda.org.au/policy/current-policies/ We may also disclose gTLD domain name registration information for public access via a gTLD whois search.	• Performance of our contracts with customers. • Performance of our contracts with our employees, suppliers and contractors. • Necessary for our legitimate interests (in order to administer and our businesses including to allow customers to operate our services, and to enable us to operate our IT systems and networks, manage our hosting environments and ensure the successful delivery of our services). To comply with our legal and statutory obligations.

7 Analytics data (other than to provide managed services)

7.1 We also collect information about end users known as analytics data, such as user location, information about devices accessing our services, the amount of time an end user spends and in which parts of it, and the path navigated through it to analyse how our website and networks are used. However, all such information is de-identified data and not collected in a form that could reasonably be expected to identify an individual where it is collected for any reason, other than for us to provide managed services to a customer. In such circumstances, we only use analytics data for the following internal business purposes:

(a) to help us review, enhance and improve our services;

(b) to develop case studies and marketing material without identifying any end user.

8 Analytics data (to provide managed services)

8.1 We also collect information about end users known as analytics data, such as user location, information about devices accessing our services, the amount of time an end user spends and in which parts of it, and the path navigated through it to analyse how our website and networks are used. We use such data to help us secure our network and our customers' systems, where required in order to provide managed services (without de-identifying the data).

9 How we hold and secure personal information

9.1 We hold and store personal information that we collect in our offices, computer systems and third party owned and operated hosting facilities. In particular:

(a) we use hosting facilities operated by reputable hosting providers;

(b) personal information that is provided to us via email is held on our servers or those of our cloud-based email providers which have restricted access security protocols;

(c) we use third party owned cloud-based customer relationship management (CRM) and marketing platform providers to hold personal information about current and prospective customers;

(d) personal information is held on computers and other electronic devices in our offices and at the premises of our personnel; and

(e) we hold personal information that is provided to us in hard copy in files and folders in secure locations.

9.2 We take reasonable steps to protect personal information that we hold using such security safeguards as are reasonable in the circumstances to take, against loss, unauthorised access, modification and disclosure and other misuse, and we implement technical and organisational measures to ensure a level of protection appropriate to the risk of accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information transmitted, stored or otherwise processed by us.

9.3 For example, we:

(a) perform security testing and maintain other electronic (e-security) measures for the purposes of securing personal information, such as passwords, anti-virus management and firewalls;

(b) carry out security audits of our systems which seek to find and eliminate potential security risks in our electronic and physical infrastructure as soon as possible;

(c) maintain physical security measures in our buildings and offices such as door and window locks and visitor access management, cabinet locks, surveillance systems and alarms to ensure the security of information systems (electronic or otherwise);

(d) require all of our employees, agents and downstream contractors to comply with privacy and confidentiality provisions in their employment contracts and subcontractor agreements that we enter into with them;

(e) continuously monitor, log analysis, and audit our devices, storage and channels. This may be performed by our suppliers and contractors;

(f) have data backup archiving, data breach response plans and disaster recovery processes in place;

(g) implement passwords and access control procedures into our computer systems; and

(h) with respect to personal information that we no longer require or where we are otherwise required to destroy it under applicable law, we ensure that such personal information is securely de-identified (where permitted by law) or destroyed.

10 Disclosure of personal information

10.1. We only disclose personal information that we collect to third parties as follows:

(a) where such disclosure is required in order for us to provide the services that a customer engages us to provide (such as an email service or other communication service);

(b) when performing contracts, we may outsource certain obligations to third party contractors in accordance with our contractual rights (such as hosting, consulting and other professional services). Professional services carried out by them may require access to an individual's personal information. We ensure that all staff and contractors are aware of their information security responsibilities, are appropriately trained to meet those responsibilities and have entered into agreements that require them to comply with privacy and confidentiality obligations that apply to personal information that we provide to them;

(c) when we engage third parties to make marketing calls, to provide customer satisfaction surveys or send marketing emails. All individuals will be given the opportunity to 'opt out' of any direct marketing calls or emails;

(d) when providing information to our legal, accounting or financial advisors/representatives or insurers, or to our debt collectors for debt collection purposes or when we need to obtain their advice, or where we request their representation in relation to a legal dispute;

(e) where a person provides written consent to the disclosure of their personal information;

(f) where it is brought to our attention that specific personal information needs to be disclosed to protect the safety or vital interests of any person;

(g) for the conduct of proceedings before any court or tribunal (being proceedings that have been commenced or are reasonably in contemplation);

(h) when we de-identify personal information and then use it for our or third party research purposes;

(i) where required in connection with a merger, sale or corporate reorganisation;

(j) in the event of a merger, dissolution, reorganisation or similar corporate event, or the sale of all or substantially all of our assets, we expect that the information that we have collected, including personal information, would be transferred to the surviving entity in a merger or the acquiring entity, and in such case all such transfers shall be subject to our commitments with respect to the privacy and confidentiality of such personal information as set out in this Privacy Policy;

(k) when required to disclose personal information in response to lawful requests by public

authorities, including for the purpose of meeting national security or law enforcement requirements, or to other third parties when compelled to do so by government authorities or required by law or regulation including, but not limited to, in response to court orders and subpoenas; or

(l) where required by law.

11 Third party websites

11.1. Our website may include links to third party websites. Our linking to those websites does not mean that we endorse or recommend them. We do not warrant or represent that any third party website operator complies with applicable data protection laws. Customers and their end users should consider the privacy policies of any relevant third party website prior to sending personal information to them.

12 Interacting with us without disclosing personal information

12.1. If a person does not provide us with their personal information, they can only have limited interaction with us. For example, a person can browse our public facing websites without providing us with personal information such as the pages that generally describe the services that we make available. However, when a person submits a form on our websites or an organisation enters into a contract with us, we need to collect personal information for identification purposes, so that we can provide our services, and for the other purposes described in this Privacy Policy.

12.2. Any person has the option of not identifying themselves or using a pseudonym when contacting us to enquire about our services.

13 Offshore disclosure

13.1. As a supplier of information technology services, including cloud services, we retain personal information on servers that may be located in a number of overseas countries. We may disclose personal information to our offshore service providers and personnel who assist us with providing our services and to assist us with the operation of our businesses generally. We will take reasonable steps to ensure that such overseas recipients do not breach the Australian Privacy Principles in relation to personal information.

14 How to access and correct personal information held by us

14.1 Subject to verification of your identity, you can contact us directly to access and correct personal information that we hold about you.

14.2 End users can amend personal information contained in their accounts, or delete their accounts, at any time by contacting the customer. Once an account is deleted, some data may be retained in our logs and/or archives and we may still be required to retain certain data in accordance with our contractual obligations or where required by law. End users who wish to make enquiries about the personal information held in respect of them, should contact the relevant customer in the first instance.

14.3 We will handle all requests for access to personal information in accordance with our statutory obligations. We may require payment of a reasonable fee by any person who requires access to their personal information that we hold, except where such a fee would be contrary to applicable law.

15 Retention and de-identification of personal information

15.1 For the purposes of the *Privacy Act 1988* (Cth), we may take such steps as are reasonable in the circumstances to de-identify the personal information that we hold about an individual where we no longer need it for any purpose for which it was collected and or if the information is not contained in a Commonwealth record and we are not required by Australian law (or a court or tribunal order) to retain it.

16 Opt-out for direct marketing

16.1 You may opt out at any time from the use of your personal information for direct marketing purposes by emailing us or by clicking on the "Unsubscribe" link located on the bottom of any of our marketing emails. Please allow us a reasonable time to process your request. You cannot opt out of receiving transactional emails related to the services.

17 Contact details

17.1 Any person who wishes to contact us for any reason regarding our privacy practices or the personal information that we hold about them, or to make a privacy complaint, may contact us using by email to privacy@procomputers.com.au.

17.2 We will use our best endeavours to resolve any privacy complaint with the complainant within a reasonable time frame given the circumstances. This may include working with the complainant on a collaborative basis or otherwise resolving the complaint.

17.3 If the complainant is not satisfied with the outcome of a complaint or they wish to make a complaint about a breach of the Australian Privacy Principles, they may refer the complaint to the Office of the Australian Information Commissioner, who can be contacted using the following details:

Office of the Australian Information Commissioner
Telephone: 1300 363 992
Email: enquiries@oaic.gov.au
Address: GPO Box 5218, Sydney NSW 2001