Privacy Policy

1 About this Privacy Policy

1.1 This Privacy Policy describes how we, Franco Enterprises Pty Ltd trading as MicrotechDPS, manage personal information about our customers (**you**) and your end users, our suppliers, agents and contractors that we interact with or engage, for the purposes of supplying products and services to you and to operate our business.

1.2 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). We also comply with the *EU General Data Protection Regulation 2016/679* (**GDPR**) in relation to personal data processed by us, which is governed by the GDPR.

1.3 If we decide to change this Privacy Policy, we will post the updated version on our website 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 provision of the managed information technology services

2.1 We provide a range of services for the supply of certain managed information technology services such as managed cloud back up services, managed hardware and server services, hardware and software resale services, managed antivirus services, managed Microsoft Office 365 services, hosting services, project-based professional consulting and support services, voice services and managed network services (collectively, the **Services**). We enter into contracts with you for your subscription, licensing, supply or use of one or more of our Services (as applicable).

2.2 The functionality, technical specifications, products and Services that we provide depends on the particular requirements set out in the contract that we have with you.

2.3 Some of our Services provide functionality that can be used by you to collect, process and disclose personal information about your end users.

3 Your responsibility for end user privacy

3.1 You are required to comply with all applicable privacy laws.

3.2 We rely on you to obtain all relevant privacy consents and authorisations from your end users required by law, in order for the personal information that is

entered and/or transmitted via our Services to be collected, disclosed and otherwise processed by us. We also rely on you to ensure that all of your end users' personal information held by us is accurate, up to date, complete, relevant and not misleading.

3.3 We encourage you to ensure that your end users are familiar with your privacy policy so that your end users understand how you collect, use and otherwise process personal information about them, including where you engage us to do so on your behalf.

4 The types of personal information we collect and hold

4.1 We collect the following types of personal information:

(a) **Information about your personnel**: We collect contact details of your personnel, such as names, addresses, positions, email addresses, contact information and billing information, including credit card details and direct debit information. Credit card details are not held by us, but are held by payment gateway providers that we use. Other than the last 4 digits of a credit card, all such credit card information is not accessible by us. If you choose to pay by direct debit, we may collect your name and the name of your financial institution, BSB and account numbers through our direct debit authorisation form.

(b) **Content entered into and/or transmitted via our Services about your end users**: All information, including personal information, that is entered into and/or transmitted via our Services (either by your end users or otherwise). The types of personal information collected may include names, contact details as well as any other personal information entered into and/or transmitted via the Services by, about or on behalf of your end user. In the course of providing our Services we may host your databases or content specifically at your request, that you have provided to us. These databases and content may include any type of personal information.

(c) **Information about our suppliers and contractors**: We collect personal information about our suppliers and contractors in the course of engaging their services. The types of personal information collected include names, contact information, email and postal addresses, occupation as well as any other information voluntarily provided to us that we need in order to manage our engagement of them.

(d) **Information required for the support, maintenance and security of our Services**: In order to support and maintain Services that we provide to you, we collect and process your end user information including IP addresses, email addresses, user access logs, usernames, passwords

and any information included by you in technical support tickets and error messages.

(e) **Managed services technical data**: When providing our Services, we may monitor or access your computers, networks and other equipment remotely or on site. In the course of doing so, we will collect and process information about those computers, networks and other equipment and any software and data processed by that equipment. This information includes IP addresses, server names, database names, network names, serial numbers of equipment used, MAC addresses, computer names, application names, browser history, user access logs, usernames, passwords, technical support log tickets, bandwidth used, error messages, social media handles, FTP server addresses, hostnames, subnet masks, router names and server addresses.

(f) **Computer and network usage data**: Subject to applicable laws, we may carry out electronic surveillance of our employees and contractors when they use our computer equipment, smartphone devices and networks to monitor compliance with our policies. This surveillance includes tracking and monitoring, reviewing and logging emails sent and received, websites visited, content viewed and files uploaded/downloaded. It also includes IP addresses, server names, database names, network names, serial numbers of equipment used, MAC addresses, computer names, application names, browser history, user access logs, usernames, passwords, technical support log tickets, bandwidth used, error messages, social media handles, FTP server addresses, hostnames, subnet masks, router names and server addresses.

(g) **Telecommunications Data**: As an internet service provider, we are required to retain data about communications under Part 5-1A of the *Telecommunications (Interception and Access) Act 1979* (**TIA Act**). This information is retained for 2 years from the date that the data is created. We are also required under the TIA Act to retain subscriber information for 2 years from the date the relevant account is closed. The data that we retain in accordance with our obligations under the TIA Act may be disclosed to law enforcement agencies and other government bodies. For further information about the specific types of personal information that we may be required to collect and retain under the TIA Act, please contact us.

4.2 We also collect and use non-personally identifiable data for marketing purposes.

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. We only collect personal information that is necessary to provide the Services, to operate our business and to comply with applicable law.

5.2 We collect personal information about your personnel in one or more of the following ways:

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

(b) during the preparation, negotiation and finalisation of the contract for the provision of Services and for billing purposes thereafter; and

(c) when it is voluntarily disclosed to us (such as via telephone, our website, e-mail and online forms).

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

(a) when your end users enter personal information into our Services or our Services are used to otherwise collect or store their personal information;

(b) when you provide and/or disclose personal information to us (for example, for the purposes of migrating data from your legacy database to a new service);

(c) when it is transmitted via an API in accordance with our obligations to do so pursuant to a contract;

(d) for the purpose of providing and supporting our Services;

(e) when it is voluntarily disclosed to us (such as via telephone, our website, e-mail and online forms).

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

(a) when we trade business details with our suppliers, vendors and contractors;

(b) for workplace health and safety reasons;

(c) during the preparation, negotiation and finalisation of a contract that we enter into;

(d) through websites, public registers and directories such as telephone directories and business name and company searches;

(e) when it is otherwise voluntarily provided to us.

6 How we use personal information

6.1 We use personal information about you, your 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 your personnel	• To provide the Services. • To setup, configure, support, host or procure the hosting, of a platform for you and the use of our Services by your end users. • To communicate with you about their current and prospective use of our Services, including with respect to your end users' current and anticipated usage of the Services, and to discuss and implement your software development requirements. • To provide data migration and implementation services in respect of databases that require integration into our Services. • To provide digital transformation services by accessing your premises, personnel applications and IT environment to make	• 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 ensure the successful delivery of our Services). • Performance and enforcement of our contracts with you. • Compliance with our legal and statutory obligations in accordance with our supplier agreements and applicable law.

	recommendations and prepare a report. • To provide you with technical support and maintenance services including by responding to help desk tickets, scheduling upgrades and enhancing our Services. • To provide professional services to you (including training, consulting and other services). • To send out billing information and notices to you and process payments. • To discuss our security requirements and to understand your security requirements in respect of the Services. • When conducting research and development of our products and services. • To provide actual and potential 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. • In order to identify you when contacted with technical support questions. • To administer our contractual relationships with you (and to enforce our contractual rights and their contractual obligations).	

	• To streamline and personalise your experience while dealing with us. • To configure new Services for you or to make changes to existing Services, as requested by you. • To arrange and manage deliver of products to you.	
Personal information about your end users	• As required to provide and support the Services supplied to you and to process the personal information of your end users on your behalf. • 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 you that require us to view and/or update end user data. • When performing cyber security services. • When conducting research and development of our products and services. • To configure new Services for you or to make changes to existing Services, as requested by you. • Backing up and restoring data that includes end user personal information (where we are engaged to do so). • To carry out security audits, investigate security incidents and implement	• Performance of our contracts with you. • Necessary for our legitimate interests (in order to administer and our businesses including to allow you 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.

	security processes and procedures that require access to your end users' personal information.	
Personal information about suppliers and contractors	• To establish, maintain and manage our relationship with our suppliers and contractors, including functions such as recruitment, payroll, appraisals, and any disciplinary action (including any termination of any employment or engagement) and managing any claim in relation to any injuries, illnesses they have and any workers compensation claims by them; • To send out billing information and notices to suppliers and contractors and process payments or make payments. • For workplace health and safety reasons (i.e. ensuring our contractors are adequately trained and safe). • When conducting research and development of our products and services. • To procure new services from our suppliers and contractors in accordance with your requirements.	• Performance of our contracts with our suppliers and contractors. • Necessary for our legitimate interests (in order to administer and our businesses including to allow you 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 How we hold and secure personal information

7.1 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.

7.2 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 to 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.

7.3 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 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) implement anti-virus and security controls for email and other applicable computer software and systems;

(g) have data backup archiving and disaster recovery processes in place;

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

(i) 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.

8 Disclosure of personal information

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

(a) in order to provide our products and Services to you;

(b) when we provide third-party software and/or hardware to you in accordance with our contracts with you, we will have to comply with certain obligations under our agreements with such third parties including to comply with any request by such third party vendors to disclose personal information including your contact details contained in telephone recordings, system notes and records that we create of any transaction between you and us;

(c) when we agree to provide transition services to you, we will disclose your or your end users' personal information that we host, hold, process and/or access to an authorised third-party provider of your choosing;

(d) when performing contracts, we may outsource certain obligations to third party contractors in accordance with our contractual rights (such as hosting, software development 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 which require them to comply with privacy and confidentiality obligations that apply to personal information that we provide to them or that they access on our behalf;

(e) 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;

(f) 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;

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

(h) 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;

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

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

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

(l) where required by law.

9 Third party websites

9.1. Some of our Services 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. You and your end users should consider the privacy policies of any relevant third party website prior to sending personal information to them.

10 Interacting with us without disclosing personal information

10.1. 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, or a person registers an end user account as part of one of our services, 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.

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

11 Offshore disclosure

11.1. As a provider and user 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.

12 How to access and correct personal information held by us

12.1 Subject to identity verification, any person can contact us directly to access and correct personal information that we hold about them.

12.2 Some of the Services that we provide may allow end users to amend personal information contained in their accounts, or delete their accounts, at any time, by logging into their accounts where such functionality is available or by contacting you in the first instance. Once an account is deleted, we may still be required to retain the data in accordance with our contract with you or by law.

12.3 End users who wish to make enquiries about the personal information held by them, should contact you in the first instance. Where possible we will refer any enquiries for access to personal information from your end users to you for you to manage.

12.4 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.

13 Retention and de-identification of personal information

13.1 For the purposes of the *Privacy Act 1988* (Cth), instead of destroying the personal information 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 may be used in accordance with this Privacy Policy 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.

14 Contact details

14.1 Any person who wishes to contact us for any reason regarding our privacy practices or the personal information that we hold about them, or make a privacy complaint, may contact us using the following details:

Privacy Representative and Data Protection Officer
MicrotechDPS

2 Footmark Court
Wodonga VIC 2690
privacy@microtechdps.com.au

14.2 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.

14.3 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:

Telephone: 1300 363 992
Email: enquiries@oaic.gov.au
Address: GPO Box 5218, Sydney NSW 2001

GDPR

15 Personal Data

15.1 This section of our Privacy Policy applies to personal data of customers and end users that may be collected by us that is governed by the EU General Data Protection Regulation 2016/679 (GDPR). Article 4(1) of the GDPR defines 'personal data' as any information relating to an identified or identifiable natural person.

16 Collection of personal data

16.1 Customers are responsible for the collection of personal data of your end users and for obtaining the relevant consents and authorisations necessary for us to process your end users' personal data in accordance with this Privacy Policy. Paragraph 5 above sets out how we collect personal data about customers, end users and suppliers and contractors.

17 Purpose of processing your, your end users' and our suppliers' and contactors' personal data and our legal basis for doing so

17.1 The table in paragraph 6.1 above sets out the legal basis under which we process personal data for the purposes of Article 6(1) of the GDPR.

18 Who will receive personal data

18.1 Detailed information about who we disclose personal information to is set out in paragraph 8 above. This applies equally to personal data governed by the GDPR.

19 International transfers

19.1 We only transfer your, your end user's and our suppliers' and contractors' personal data governed by the GDPR internationally as set out in paragraph 11 above in compliance with the GDPR. We have legally binding agreements in place that govern the receipt and processing of personal data transferred offshore. Information about other appropriate or suitable safeguards is available from us for customer personnel and data subjects whose personal data is governed by the GDPR, on request.

20 Retention of personal data

20.1 It is our policy to retain personal data in a form which permits identification of any person only as long as is necessary for the purposes for which the personal data was collected for the minimum length of time permitted by applicable law and only thereafter for the purposes of deleting or returning that personal data (except where we also need to retain the data in order to comply with our legal obligations, or to retain the data to protect any other person's vital interests or where we de-identify it on the basis set out in this Privacy Policy).

20.2 Except as otherwise set out in our agreements with you, where you require your or your end users' personal data to be returned, it will be returned to you at that time, and we will thereafter delete all then remaining existing copies of that personal data in our possession or control as soon as reasonably practicable thereafter, unless applicable law requires us to retain the personal data in which case we will notify you of that requirement and only use such retained data for the purposes of complying with those applicable laws.

21 Requirement to provide personal data to us

22 Please see paragraph 10 above for information about the requirement to provide personal information to us and the limitations that apply where personal information is not provided. Those requirements and limitations apply equivalently to personal data governed by the GDPR.

23 Rights under the GDPR

23.1 Under the GDPR, data subjects have a number of rights, including:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object to processing

23.2 You and your end users have the right to lodge a complaint with any relevant supervisory authority.

23.3 Your end users are encouraged to contact you in the first instance, if they wish to exercise any of their applicable rights under the GDPR.