ReadyTech Group Privacy Policy

Last Updated: November 23, 2020

1 About this Privacy Policy

1.1. This Privacy Policy describes how the ReadyTech Group manages personal information about ReadyTech Group corporate customers and the individuals whose data is processed by or on their behalf using the ReadyTech Group's online platforms (whether or not they are platform end users). All such individuals are referred to in this Privacy Policy as "data subjects".

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).

1.3. Details about how we manage personal information about our New Zealand customers and their data subjects is **available here** and information about how we manage personal information about customers and their data subjects that is governed by the General Data Protection Regulation 2016/679 (GDPR) is **available here**. This Privacy Policy also includes details about how we manage personal information of our employees and other personnel, which is **available here**.

1.4. The ReadyTech Group includes ReadyTech Holdings Limited (ASX: RDY) and its subsidiaries. In this Privacy Policy, references to the ReadyTech Group are to the relevant member or members of the group.

1.5. If we decide to change this Privacy Policy, we will post the updated version on our website. Our policy is to be completely transparent about our privacy practices.

2 Our online platforms

2.1. The ReadyTech Group owns and operates a range of learning, payroll, student management, human resources management and related online platforms. We enter into contracts with our corporate customers through which they subscribe to or license access to one or more of our platforms. We do not enter into contracts with any data subjects.

2.2. The functionality provided by each platform to a customer depends on the particular platform and the requirements of the relevant contract that we have with the customer.

2.3. Our platforms provide customers with functionality that can be used by them to collect, process and disclose personal information about their end users and other data subjects.

3 Customer responsibility for data subject privacy

3.1. Our customers are required to comply with all applicable privacy laws.

3.2. We rely on our customers to obtain all relevant privacy consents and authorisations from data subjects required by law, in order for the personal information that is entered into our platforms to be collected, disclosed and otherwise processed by us.

3.3. We also rely on customers to ensure that all personal information of their data subjects held by us is accurate, up to date, complete, relevant and not misleading.

3.4. We encourage customers to ensure that their data subjects are familiar with their privacy policies so that their data subjects understand how the relevant customer will collect, use and otherwise process personal information about them, via the platform or otherwise.

4 The types of personal information we collect and hold about customers and data subjects

4.1. Our platforms can be used to collect and hold the following types of personal information:

(a) **Content entered into our platforms about data subjects:** All information, including personal information, that is entered into our platforms (either by end users or otherwise) is stored in systems managed by our customers and/or by us on their behalf. The types of personal information collected may include names, contact details, employment information and payroll data, as well as any other personal information entered into the platforms by, about or on behalf of a data subject.

(b) **Information about customer personnel:** We collect contact details of our customers' personnel, such as names, contact information and billing information, including credit card details. 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. For customer personnel who are data subjects, we also collect the information about them referred to in paragraph (a) that is entered into our platforms.

(c) **Information required for the support, maintenance and security of our platforms:** In order to support and maintain a platform for a customer, we collect and process end user information including IP addresses, email addresses, user access logs, usernames, passwords, information included by customers in technical support tickets and error messages.

5 How we collect personal information

5.1. Our policy is to not collect personal information by means that are unfair or unreasonably intrusive in the circumstances.

5.2. We collect information about prospective customers from public and private databases and when they otherwise voluntarily disclose it to us, in order to market and sell our services and promote their use of our platforms.

5.3. After a prospective customer enters into a contract with us for their use of one of our platforms, we will collect personal information about their data subjects in one or more of the following ways:

(a) when end users enter personal information into the platform;

(b) when a customer provides personal information to us (for example, for the purposes of migrating data from a customer's legacy database to the platform);

(c) when it is provided to us by third parties such as government agencies on behalf of a customer or pursuant to an agreement with a customer, for it to be entered into and/or processed by the platform;

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

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

6 How we use customer and data subject personal information

6.1. Information about how we use customer and data subject personal information is 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 prospective customers' personnel	• To inform, market and promote our services and platforms to prospective customers and negotiate contracts with them.	• Necessary for our legitimate interests (in order to operate and grow our businesses).
Personal information about the personnel of customers who we have entered into contracts with	• To setup, configure, host or procure the hosting, of a platform for a customer and the use of the platform by its end users. • To communicate with customers about their current and prospective use of our platforms, including with respect to their end users' current and anticipated usage of the platforms, and to discuss and implement customers' software development requirements. • To provide customers with technical support and maintenance services including by responding to help desk tickets, scheduling upgrades and enhancing our platforms.	• Necessary for our legitimate interests (in order to operate, administer and grow our businesses including to operate our platforms, IT systems and networks, manage our hosting environments and ensure the successful delivery of our services). • Performance and enforcement of contracts with our customers. • Compliance with our legal obligations.

	• To provide professional services to customers (including training and other services). • To send out billing information and notices to customers and process payments. • To discuss our security requirements. • To provide customers with information about promotional offers and new products and solutions that we make available. • In order to identify customers when contacted with technical support questions. • To administer our contractual relationships with customers (and to enforce our contractual rights and their contractual obligations).	
Personal information about data subjects	• As required to provide and support the functionality of the relevant platform for a customer and to process the personal information of data subjects on behalf of a customer who has engaged us to do so. • To migrate data onto our platforms from other client systems (including legacy databases). • In order to store data subject personal information in databases and systems in our hosting environments at third party data centres (this only applies to platforms that are hosted by us and not to software that is hosted independently by our customers). • To provide technical support services to our customers that require us to view and/or update data subject data held in our platforms. • Backing up and restoring data that includes data subject personal information. • To carry out security audits, investigate security incidents and implement security processes and procedures that require access to data subject personal information.	• Performance of our contracts with a customer. • Necessary for our legitimate interests (in order to administer and our businesses including to allow our customers to operate our platforms, 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

7.1. We also collect information about platform end users known as analytics data such as user location, information about devices accessing our platforms, the amount of time

an end user spends on our platform and in which parts of it, and the path navigated through it. However, all such information is de-identified data and not collected in a form that could reasonably be expected to identify an individual. In any event, we only use analytics data for the following purposes:

(a) to help us review, enhance and improve our platforms (for statistical or research purposes); and

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

7.2. We use Google Analytics in our platforms. To understand how Google uses data **click here**.

7.3. We also use cookies on our platforms. For information about how we use cookies, please go to www.readytech.com.au/cookies.

8 How we hold and secure personal information

8.1. 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 collocate systems in 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;

(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;

(e) we hold personal information that is provided to us in hard copy in files on our business premises.

8.2. 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.

8.3. We:

(a) ensure the confidentiality, integrity and availability of our information assets and information systems;

(b) apply a consistent Information Security framework across our group aligned with the ISO 27001 “Information Security Management System” standard;

(c) ensure all staff and contractors are aware of their information security responsibilities and that they are appropriately trained to meet those responsibilities; and

(d) continually improve our Information Security posture.

8.4. For example, we:

(a) only use reputable hosting providers to host data subject personal information;

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

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

(d) have an information security management framework;

(e) 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);

(f) with respect to personal information that we no longer require or where we are otherwise required to destroy it under applicable law, in the case of personal information held on physical media, we place the personal information in secure bins and destruction is verified and certified by our providers. In the case of electronic personal information, we ensure that it is securely destroyed;

(g) 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;

(h) have a Data Breach Response Plan in place; and

(i) have data backup, archiving and disaster recovery processes in place.

9 Disclosure of personal information

9.1. We only disclose customer and data subject personal information that we collect to third parties as follows:

(a) where required under a contract with a customer, we will transmit data subject personal information to third parties on behalf of the customer. For example, some of our platforms may include functionality that enables data subject personal information to be transmitted to their customer or third party systems. Customers may be able to effect those transfers using our platforms or may instruct us to otherwise do so on their behalf;

(b) in order to host databases that are integrated into our platforms, we engage reputable hosting providers who host those databases on our behalf;

(c) we transfer personal information about our customers to third party cloud-based platforms;

(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 customer and data subject 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;

(e) 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 require their representation in relation to a legal dispute;

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

(g) 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;

(h) to avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences;

(i) for the enforcement of a law imposing a pecuniary penalty;

(j) for the protection of public revenue;

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

(l) where required by law.

9.2. Customers who use our platforms to disclose personal information about data subjects to third parties are expected to only do so where permissible under applicable law.

10 Third party websites

10.1. Our platforms 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 data subjects should consider the privacy policies of any relevant third party website prior to sending personal information to them.

11 Interacting with us without disclosing personal information

11.1. 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 on one of our platforms, 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.

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

11.3. For security purposes, only end users who identify themselves accurately and truthfully when opening any account on any of our platforms, may login to and access the functionality provided by our platforms.

12 Offshore disclosure

12.1. 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.

12.2. At present, we only disclose personal information offshore:

(a) when we upload it to our hosting providers in New Zealand and the United Kingdom as described in clause 9.1(b) and to third party cloud-based platforms as described in paragraph 9.1(c); and

(b) in the circumstances that we need to permit our contractors located in Vietnam or Philippines to access our systems in order to carry out their duties. However, this only applies in respect of personal information managed via the JR Active, JR Direct and JR Plus platforms.

12.3. Except as set out in paragraph 12.2 all personal information that we collect is held in Australia.

13 How to access and correct personal information held by us

13.1. End users who have accounts on our platforms can 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 the customer who provided them with access to the platform. Once an account is deleted, we may still be required to retain the data in accordance with our contract with the customer or by law.

13.2. Data subjects who wish to make enquiries about the personal information held by them on a ReadyTech Group platform should contact the customer who provided them with access to the platform, or who uploaded their personal information into the relevant platform in the first instance.

13.3. 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.

14 Our 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
security@readytech.com.au
Level 1, 35 Saunders Street,
Pyrmont NSW 2001

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

[Dropdown 1: New Zealand Customers and Data subjects]

This section of our Privacy Policy applies to personal information of customers, data subjects and other persons that may be collected by any member of the ReadyTech Group that is governed by the Privacy Act 2020 (New Zealand).

Collection of personal information

We will only collect personal information for a lawful purpose which is connected to a function or activity of our businesses to the extent that it is necessary for such purpose. Collection under the Privacy Act (New Zealand) does not include our receipt of unsolicited information from a person. This means that if a person provides us with their personal information and we have not asked them for such information, our receipt of that information will not be considered our collection of it and will not be afforded the protections under New Zealand Information Privacy Principles (IPPs) 1 to 4. Nevertheless, any unsolicited information that we receive from a person will be afforded the same security that other personal information is given as set out above in this Privacy Policy.

Provision of personal information to third parties

Where it is necessary for personal information to be given to a third party in connection with the provision of a service they provide to us, we will do everything reasonably within our power to prevent unauthorised use or unauthorised disclosure of the information by them.

The specific personal information that we collect, how we collect it, how we use it and who we disclose it to, is set out above in this Privacy Policy.

Requests for access to and correction of personal information

Individuals whose personal information is governed by the Privacy Act (New Zealand) are entitled to seek access to and correction of it in accordance with that legislation.

As set out above, any person who wishes to access personal information about them held in any of our platforms should contact the relevant customer in the first instance.

In the event that a person wishes to access their personal information and it is readily retrievable by us, they can also request from us either of the following:

(a) to obtain confirmation from us as to whether or not we hold such personal information; and

(b) access to the personal information and be advised if they are able to correct such personal information.

We will as soon as possible and in any event no later than 20 working days from the date on which the request is made, decide to grant or refuse the request and provide the person who made the request with or post to them, our decision. We may in our discretion charge a

reasonable fee for making information available in compliance with the request or for correcting any information in compliance with a request (in whole or in part) or for attaching a statement of any correction sought but not made, subject to our compliance with the IPPs.

If a person submits a request to access their personal information to us, we may refuse their request on one or more of the grounds set out in the Privacy Act (New Zealand).

If we refuse to comply with a request to access their personal information, we will provide the individual who made the request with our reasons for our denial and an opportunity to file a complaint with the Commissioner, to seek an investigation and a review of the refusal.

Where we hold personal information governed by the Privacy Act (New Zealand) about an individual, they are entitled to:

(a) request correction of the information; and

(b) request that there be attached to the information a statement of the correction sought but not made.

[Dropdown 2: European Customers and Data subjects]

This section of our Privacy Policy applies to personal data of customers and data subjects 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. Although we are not strictly 'controllers' of data subjects' personal data (other than with respect to data subjects who are customer personnel), in that we do not determine how and why such data will be used, as that is determined by the customer; we are committed to complying with our requirements under the GDPR in our capacity as a processer.

Collection of personal data

Customers are responsible for the collection of personal data of data subjects and for obtaining the relevant consents and authorisations necessary for us to process data subject personal data in accordance with this Privacy Policy. Paragraph 5.3 above explains how we collect data subject personal data and the sources that provide us with data subject personal data. We do not collect data subject personal data from any publicly available sources. Paragraph 5 above sets out how we collect personal data of customer personnel.

We collect all categories of personal data that an end user enters into our platforms or that is held in a ReadyTech Group platform with respect to a data subject. For more information about the categories of personal data that we collect about data subjects and customers, please see paragraph 4 above.

Purpose for processing customer and data subject personal data and our legal basis for doing so

The table in paragraph 6.1 above sets out the legal basis under which we process customer and data subject personal data pursuant to Article 6(1) of the GDPR.

Who will receive customer and data subject personal data

Detailed information about who we disclose personal information to is set out in paragraph 9 above. This applies equally to personal data governed by the GDPR.

International transfers

We only transfer customer and data subject personal data governed by the GDPR internationally as set out in paragraph 9 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.

Retention of customer and data subject personal data

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).

Requirement to provide customer and data subject personal data to us

Please see paragraph 11 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.

Automated decision making

Some of our platforms include functionality that uses automated decision making. This functionality is designed to determine when data should be flagged for further processing by one of our platforms or disclosed to third parties. The specific circumstances under which this will occur will be set out in a contract that we enter into with a customer. Data subjects can obtain more information about this from their customer. We do not use automated decision making in our capacity as a controller.

Further processing activities by us

We will not carry out any further processing activities on customer or data subject personal data, other than as set out in this Privacy Policy.

Rights under the GDPR

Under the GDPR, individuals have a number of rights, including:

(a) The right to be informed

(b) The right of access

(c) The right to rectification

(d) The right to erasure

(e) The right to restrict processing

(f) The right to data portability

(g) The right to object to processing

Customers and data subjects also have the right to lodge a complaint with any relevant supervisory authority.

Data subjects are encouraged to contact their customer in the first instance, if they wish to exercise any of their applicable rights under the GDPR.

[Dropdown 3: ReadyTech Personnel]

This section of our Privacy Policy applies to personal information that the ReadyTech Group collects, processes and manages about any person employed or engaged by the ReadyTech Group.
Personnel with any questions about our privacy practices, can contact their manager or our Privacy Representative / Data Protection Officer set out above.
Why we collect personal information about our personnel
All personnel have contracts in place which govern their relationship with us. We collect personal information of our personnel for the following purposes:

(a) enforcing our contractual rights and company policies;

(b) complying with our legal obligations; and

(c) otherwise managing our businesses.

The types of personal information we collect about our personnel and how we collect it

As part of our recruitment and management of personnel, 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).

Employee biometric fingerprint data is also collected for the purposes of recording employee start and end times who are employed by some ReadyTech Group companies.

We also collect personal information about our personnel in 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 a ReadyTech Group company, and when we conduct reference checks; and

(c) when they voluntarily provide us with personal information;

Only personnel who are employed to carry out our employment operations or ancillary functions, are permitted to access employee files.

How we use personnel personal information

We use personal information about personnel strictly for the following purposes:

(a) to recruit and assess an applicant's suitability for available positions in one of our businesses;

(b) to manage and govern their employment or engagement with us as required to operate our businesses;

(c) to administer our commercial and contractual relationships with them; and

(d) to comply with our legal obligations.

Disclosure of personal information about personnel

We will only disclose personal information about personnel that we collect to third parties as follows:

(a) when we are required to do so in the course of their employment or engagement with us. For example, during an emergency we may contact an employee's nominated next of kin using their contact details or when discussing personal matters that are affecting a person's performance at work with their managers;

(b) when recruiting employees or engaging, we may contact a law enforcement agency for the purpose of obtaining a criminal history check;

(c) when we contact professional referees for character references in the course of conducting interviews and recruiting new employees;

(d) when we disclose personal information to the Australia Taxation Office, an employee-nominated superannuation fund or in order for us to pay our personnel and comply with our superannuation and taxation obligations;

(e) as set out in paragraph 9 (as applicable).

We hold and secure personal information of our personnel in the manner set out above in paragraph 8 of this Privacy Policy.