enableHR®

Public Privacy Policy

FCB GROUP

FCB WORKPLACE LAW

FCB HR

FCB SMART VISA

HR ASSURED™ smarter workplace solutions

Introduction

This notice and information applies across all websites that we own and operate and all services we provide, including our online and mobile HRIS services products, and any other apps or services we may offer (for example, events or training). For the purpose of this notice, we refer to the services we provide as our 'services'.

When we say 'personal data' we mean identifiable information about an individual, like their name, email, address, telephone number, bank account details, payment information, support queries, community comments and so on. If a person can't be identified (for example, when personal data has been aggregated and anonymised) then this notice doesn't apply.

We may need to update this notice from time to time. Where a change is significant, we will inform those users that may be affected that we have an obligation to inform – usually by sending an email.

Last Updated: 9th November 2018.

Who is enableHR?

When we refer to 'we' (or 'our' or 'us'), that means:

- **enableHR Pty Ltd** – Australia (ABN: 84 123 231 005);
- **enableHR Limited** – New Zealand (NZBN: 9429041375488); and
- any related body corporate of the above (including but not limited to HRACloud and FCB Group).

Our Head Office is in Sydney, Australia, but we operate and have offices across Australia and New Zealand. Address details for all enableHR offices are available on our Contact Us (Australia and New Zealand) pages.

We provide an easy-to-use online platform for businesses and their partners through a cloud based HRIS platform and software. If you want to find out more about what we do, see our Features page.

FCB Group provides Australian and New Zealand businesses with employment related legal advice, HR consulting, migration services and technology solutions. For more information, please visit www.fcbgroup.com.au.

How do we protect your data?

We take the privacy of data that we hold seriously, and ensure everything is done with the utmost:

- Openness, Honesty & Transparency – we endeavour to share as much pertinent information as possible with our users, regarding the security of their information, both in terms of what we are doing to protect it, as well as notifying them if something goes awry;

- Security – we strive to deliver industry leading security to protect the data – regardless of whether that information is explicitly entered into our systems or captured through other interactions with our services;

- Responsibility – we accept the responsibility that comes with being the custodian of the data we process on others' behalf.

The technologies, policies and procedures we have in place to achieve these principles are outlined in "

Appendix 1 – Security Mechanisms & Policies".

What data do we collect?

The data we may collect falls into three categories:

- Data provided to us directly – when you use some parts of our services you will provide us with personal information about yourself or other people. For example, you may provide information about your employees in order to effectively manage their employment with you. While you are not required to provide this information to us, not doing so may limit the functionality that our services can deliver to you;

- Data we collect automatically – when you browse our websites or use our services, we track implicit information such as the date and time, where you access them from (your IP address) and the type device you are using. We use this data to understand the information and functionality our current and prospective users are looking for, to provide the best service to them. Some of this information is collected using cookies and similar tracking technologies;

- **Data provided by trusted third parties** – we may from time to time collect data from publicly available third-party sources, or through our trusted sales and marketing partners. We use this data to provide tailored communication with you regarding our services.

How do we use cookies?

enableHR uses cookies and other tracking mechanisms to provide:

- **Continuity in your access to our services** – across multiple requests or over a period of time. The information we store in these cookies identifies you anonymously to our services in order to correlate a particular user session and to provide you with the relevant service experience;

- **Service usage** – to collect and track which areas of our service our users are making use of, and to provide our product teams with the metrics of that use to make informed product design decisions;

- **Website tracking** – to anonymously collect and track which areas of our website see the most traffic and to improve the quality of content we provide to our prospective customers.

If you wish to opt out of our tracking of our service usage and website tracking, you can do so by limiting advertiser tracking in your browser.

How do we use your data?

We primarily use personal data to deliver our services to you and your staff. We also use this data to:

- **Support you** – through your use of our HRIS software and through our technical support channels;

- **Communicate with you** – to inform you of: significant product or service changes; related services such as training or education sessions; operational updates; seeking your input on the review and feedback of our services;

- **Market to you** – to inform you of our own service offerings or of those of select services we choose to partner with;

- **Anonymously report on your behaviour** – to generate aggregated and anonymous reports of user behaviour across our websites and services, to improve our service and website offerings.

We undertake to only communicate with the users of our services where their access to our services puts them in a position of that communication being meaningful. Users also have the option to opt out or unsubscribe from these types of services.

How do we share your data?

We will only disclose your personal data with third parties:

- within the FCB Group of companies;
- to trusted third parties where that sharing is required to deliver ongoing and reliable services to our users, or to provide relevant marketing material to those users;
- to regulators, law enforcement bodies, government agencies, courts or other third parties where it is necessary for our compliance with the applicable laws or legislation. Where possible, we will notify you that this has occurred;.
- to other parties where we have your explicit consent.

When we share your data to third parties, we will undertake a review of the laws, policies and procedures in place with those parties prior to sharing your data to ensure your data is protected by that provider as we would protect it ourselves.

A list of third-parties to which data may be shared is included in ***"Appendix 2 – Third Party Service Providers".***

How do we retain your data?

The length of time we keep your personal data depends on what it is and whether we have an ongoing business need to retain it to provide you with a service you've requested or to comply with applicable legal or record keeping requirements.

We retain your personal data while we have a relationship with you and for a period of time afterwards where we have an ongoing business need to retain it, in accordance with our data retention policies and practices. Following that period, we'll make sure it's deleted or anonymised.

What are our commitments?

enableHR is committed to meeting the standards for privacy protection as outlined in the:

- (Australian) Privacy Act 1988 (Cth) and the Australian Privacy Principals (APP);
- (New Zealand) Privacy Act 1993 and the Information Privacy Principles (IPP);
- European General Data Protection Regulation (GDPR).

APP specific information

enableHR is committed to ensuring its compliance with the Australian Privacy Principals as it relates to both data provided directly to enableHR by users and businesses in order to deliver our services, as well to the data we process on behalf of those businesses relating to their workers. This commitment includes meeting our obligations under the Notifiable Data Breach scheme.

Both enableHR and the organisation for which enableHR is providing services are acting as Entities within the APP framework, and as such have obligations relating to that role.

While enableHR will maintain its obligations under the Privacy Act (1988) and Australian Privacy Principals, clients must ensure their compliance relating to data processed by enableHR, including:

- **Valid use** – information captured and stored within enableHR should be done so for purposes valid to the engagement of that individual;

- **Worker access** – workers (employees, candidates, volunteers, etc) wishing to access information relating to their engagement should contact the relevant personnel within their organisation who can provide the relevant (potentially limited) information to the worker;

- **Correction** – workers should be able to validate and correct information stored about them within enableHR (whether that correction occurs through enableHR or some other channel).

IPP specific information

enableHR is committed to ensuring its compliance with the Information Privacy Principals as it relates to both data provided directly to enableHR by users and businesses in order to deliver our services, as well to the data we process on behalf of those businesses relating to their workers. This commitment includes following the guidelines set out in the Privacy Commissioners guidelines for data breaches.

Both enableHR and the organisation for which enableHR is providing services are acting as Agencies within the IPP framework, and as such have obligations relating to that role.

While enableHR will maintain its obligations under the Privacy legislation, clients must ensure their compliance relating to data processed by enableHR, including:

- **Valid use** – information captured and stored within enableHR should be done so for purposes valid to the engagement of that individual;

- **Staff access** – staff (workers, employees, candidates, volunteers, etc) wishing to access information relating to their engagement should contact the relevant personnel within their organisation who can provide the relevant (potentially limited) information to the staff member;

- Correction – staff should be able to validate and correct information stored about them within enableHR (whether that correction occurs through enableHR or some other channel).

GDPR specific information

Under the GDPR, an organisation which processes personal data (the "processor") on behalf of another organisation ("the controller") require a written agreement between the two specifying certain minimum provisions.

In using enableHR, we are the controller of certain information that we receive directly from our users (business details, usernames and passwords). Our customers are controllers (and enableHR is a processor) of the personal data that those users enter into the system on behalf of or relating to your workers (employees, volunteers, candidates, etc). As controllers, responsibility for the correct and appropriate collection and use of information processed by enableHR is the responsibility of the customer managing that data.

enableHR will to the extent we are able assist the controller in ensuring compliance with their obligations under the GDPR by providing the relevant information to the controller upon reasonable request. This includes providing access to relevant data not readily available to the controller through enableHR's services, or providing information relating to enableHR's architecture and security mechanisms.

What are your rights to the data we collect?

If you believe that an enableHR user or business has provided your personal information to us via our websites or services, you should contact that user or business for any questions you may have around their entry, use and retention of that data.

While enableHR may act as the custodian of your information as an employee, candidate, volunteer, or other relationship with a business, that particular business is responsible for providing you access with the relevant information from our systems, and for ensuring the accuracy of that information.

You are able to opt-out of our electronic marketing communications by following the instructions included in each of those communications to unsubscribe.

How do I find out more?

If you have any questions or concerns on any of this information, please send an email to PrivacyOfficer@enableHR.com and we'll work with you to resolve your query.

Appendix 1 – Security Mechanisms & Policies

- **Physical Access Control** – our hosting providers provide strong physical security to the data centres where your data is stored. This security includes authentication checks and audits and limited control to physical infrastructure;

- **Logical Access Control** – access to all of enableHR's underlying systems is via a Virtual Private Network (VPN), authenticated by Dual Factor Authentication comprising One Time Passwords and Public Key Authentication;

- **Data Access Control** – limited users within enableHR have access to the underlying systems where your data is stored. Levels of access are granted based on the job requirement of those users, and those access levels are reviewed periodically. Users of enableHR's services (including our own administrators) have their access controlled based on their permission level;

- **Logical Separation** – all enableHR infrastructure is deployed and partitioned to maintain the privacy and security of your data at different levels of application. This includes inter-segment firewalls separating our database, application and web-server tiers, host level firewalls permitting authorised traffic between hosts, and the separation of our non-production environments (which are managed by the same controls to ensure the security personal data in those environments);

- **Managed Data Security** – all data remains within data centres hosted within Australia. Data is encrypted at rest, and is available to enableHR's operational teams who require access to the data at that level.

- **Data Transfer Security** – all data ingress or egress is done via secure channels. All HTTP traffic is over TLS (HTTPS), all file transfers via Secure File Transfer (SFTP) and all SMTP email over TLS (SMTPS) where the relaying server allows;

- **User Auditing** – all user interactions within our systems are audited through multiple mechanisms, including log files auditing individual user request, parameters & payloads to our applications; access audits within our systems tracking which user accessed given information at a specific point in time, and which user changed information (including the specific information which was changed);

- Operational Control – enableHR has standard processes and policies which ensure the confidentiality of your information is maintained through all of our own staff and third-party providers, and that such providers have the required controls in place to maintain their commitment to those policies;

- Operational Continuity – enableHR has a documented disaster recovery plan which ensures continuity of service in the unlikely event that our production data centre and provider is completely offline and unavailable.

Appendix 2 – Third Party Service Providers

- Amazon Web Services, ASE IT – Primary and disaster recovery data hosting;
- Chargify, eWay – Payment processing;
- New Relic – Application performance monitoring;
- Zendesk – Client Experience support & ticketing;
- Office HQ, Virtual HQ, Fonebox – Customer service phone support;
- Mailchimp, Pardot – Email service providers;
- Salesforce – Customer Relationship Management;
- Office 365 – Email;
- Google – Analytics.

enableHR®

enablehr.com

BRISBANE
Level 5, 300 Ann Street
Brisbane QLD 4000
Phone 07 3046 2100

SYDNEY
Level 11, 83 Mount Street
North Sydney NSW 2060
Phone 02 9922 5188

MELBOURNE
Level 18, 607 Bourke Street
Melbourne Vic 3000
Phone 03 9098 9400

FCB GROUP

FCB WORKPLACE LAW

FCB HR

FCB SMART VISA

HR ASSURED™
smarter workplace solutions