



# Privacy Policy

"At the end of the day, the goals are simple:  
Safety and security".

Author: Corporate Excellence Team  
Version: 1.0  
Revision: 19-August-2019



## Table of Contents

Introduction .....	3
Purpose and Aims .....	3
Key Principles of this Policy .....	3
Scope.....	4
What Personal Information do we collect? .....	5
How we use Personal Data/ Information .....	5
How we Share, Disclose and Process Data/Information.....	6
Rights of Data Subject.....	6
Transferring of Data.....	11
Client Confidential Information .....	12
Governance and Improvement .....	12
Breach of Policy.....	13
Contact .....	13
Enzen Brand Values.....	14
Document Control Information.....	14



## Introduction

This privacy policy sets out how Enzen collects, uses and protects any information that is obtained or given to Enzen either during the course of employment/contract with Enzen, through the provision of services to or from Enzen, or via the use of Enzen's website.

Enzen is committed to ensuring that your privacy is protected. Should we ask you to provide or obtain certain personal information in the provision of our support/services, by which you can be identified, this data will be only be used in accordance with this Privacy Policy.

Enzen may change this policy from time to time to reflect changes in our processes or legislation. Enzen will ensure that such changes are always notified where possible and applicable.

Breaches of this policy shall be subject to investigation and may lead to disciplinary action, which could result in dismissal. Breaches of this policy may also result in legal action which could lead to criminal prosecution.

## Purpose and Aims

This document details the steps that we have undertaken to safeguard personal data and data/information supplied by our clients. This Policy is built to make the Privacy Policy clear, so it is understood and adhered to by our employees/contractors/ partners (data subjects).

By implementing this policy, we aim to achieve:

- Transparent and lawful collection, storing and protection of data that we process
- Fulfil the data controller's and processors duty of care in regards to data protection
- Fulfil our contractual, legal & regulatory requirements, as applicable

## Key Principles of this Policy

1. Enzen is committed to ensuring that personal data or organizational data which is collected, stored, managed, and maintained by Enzen is safeguarded, and that data is processed in an ethical and lawful manner.
2. Enzen holds four types of information which are covered by this policy
  - **Organisational** information – publicly available information about organisations and some confidential information
  - **Personal** information – information about individuals such as names, addresses, job titles
  - **Sensitive** personal information – in general this kind of information is only held about employees/contractors as applicable
  - **Client Confidential** information – Data/information supplied by client as part of an engagement or contract
3. Enzen shall strive to implement applicable control measures consistently.
4. Enzen will only hold information for specific purposes. It will inform individuals (Data subjects), what those purposes are.
5. Information will not be retained longer than necessary, or beyond the point that the data is no longer required for its stated purpose.
6. Enzen shall ensure the integrity of the data maintained and the applicable processing methods as applicable and agreed shall be followed.
7. Information about Enzen's employees/contractors will not be disclosed to other organisations or to individuals who are not authorised to receive such data/details.



Data shall be shared where there is a legal requirement.

8. Enzen has processes & procedures in place to ensure the security of personal data. Records containing confidential personnel data (soft/ hard copies) are disposed of in a secured way as per the data/ record retention policy/ as agreed part of the contract.
9. Enzen has a set of procedures covering all areas of its work which are followed to ensure and achieve the aims set out above.
10. Access rights relating to programmes and projects being delivered by Enzen, will be assigned based on role & responsibility. The access rights will be reviewed and revisited at the set frequency.
11. There may be situations where Enzen works in partnership with other organisations on Programme/projects which require data sharing. Enzen will clarify which organisation is to be the Data Controller and will ensure that the Data is controlled and managed correctly as per the data protection compliance requirement(s) as applicable. This is in regard to any data which Enzen has collected and has full controls.
12. All member of the staff shall be given training on the data protection and information security management overview, which covers the data protection policy, Procedure and guidelines procedures, also covering their responsibilities with respect to data protection and information security.
13. Enzen will carry out an annual review of its Privacy policy and related procedures and also whenever changes in the business/programme, legal and regulatory system requires.

## Scope

This Privacy Policy applies to Enzen Australia, the delivery of the services, support we provide to our esteemed customers and the company website [www.enzen.com](http://www.enzen.com).

When delivering services to our clients, we endeavour to document separate agreements with our clients, which govern the delivery of project/programmes data access, and the processing of their customer data as per the scope of work awarded to Enzen and our partners.

This policy applies to all individuals working and doing business with Enzen Australia including but not limited to all levels and grades, including senior managers, officers, directors, employees (whether permanent, fixed-term or temporary), consultants, contractors, trainees, seconded staff, sponsors, or any other person associated with us, or any of our subsidiaries or their employees, wherever located.

Under this policy information must be collected and dealt appropriately in accordance with the policies and procedures set, which are aligned with Australian Privacy Principle (APP) 1.3. To fulfil our commitment to personal data protection, this policy implies that all data collected, whether on paper, stored in a computer database, or recorded on other material is safeguarded and that Enzen fulfils all its contractual, applicable legal & regulatory obligations.



## What Personal Information do we collect?

In the course of your employment/engagement, we may request certain information from you to enable us to meet our statutory obligations as employer/service provider/data controller.

We will collect the information via correspondence by phone, email, completion of forms or other applications and platforms such as Google Forms, Survey Monkey or similar.

The personal information we collect may include:

Name	Bank details
Address	Identity documentation inc. Passport, visa data, driving licence
Email address	Education history
Phone number	Work History
Date of birth	Health History
Tax File Number	Names of spouse and or dependants
Criminal Record (where applicable)	Equality & Diversity Data
Company Info & insurances (contractors only)	Absence Data

When collecting data, Enzen shall ensure that the individual user:

- Clearly understands why the information is needed, who it will be shared with and how it will be stored
- Understands what it will be used for and what the consequences are should the individual user decide not to give consent to collect/ processing
- As far as reasonably possible, grants explicit written consent for data to be processed
- Has received sufficient information on why their data is needed and how it will be used
- Is made aware of their rights, as detailed in the 'Rights of Data Subjects' section of this policy.

## How we use Personal Data/ Information

Any personal data collected from our employees is used to ensure we fulfil our legal obligations with respect to areas such as employment law, health & safety regulations, payroll, pensions, other benefits such as death in Service, or the flexible benefits available, and client legal requirements.

We may on occasion, where requested to by regulatory bodies, for regulatory or legal reasons, also be required to collate additional personal data.

Enzen is a Controller of Employee/Contractor's (data subject) Data and they (Data subject) have a responsibility to keep Enzen informed of the changes to their personal circumstances i.e. changes to their personal data.

## How we Share, Disclose and Process Data/Information

This section describes how Enzen may share and disclose Information.

Enzen may share data with the following third-party service providers and partners in order to meet our statutory obligations:

Data Processors	Name of the Company	Frequency	Reason
Payroll Provider	BDO Australia - Adelaide	Monthly	HMRC Compliance and payroll processing
Superannuation	Statewide Super Fund	As per individual requests	Compliance with Law
Immigration Consultancy Services	Konnecting Skilled Migration & Recruitment	As per individual requests	Compliance with Immigration Law
Government agencies	Australian Government Department of Home Affairs Australian Government Department of Human Services Australian Tax Office	As per individual requests	To comply with regulatory requirements.
Background Checks including Criminal background checks	National Crime Check	As per individual requests	To comply with client requirements and meet out employment obligations as applicable
Banks / Financial Institutions	Various	As per individual requests	Data shared only when required to do so by the employee.
Oracle Human Capital Management	Pricewaterhouse Coopers ('PwC')	One Time	As partner, to carry out Oracle Cloud Implementation

On commencement of employment / engagement with Enzen, we shall obtain consent from employees to collect, store and process their data as well as share their data with the selected parties above where applicable.

We may on occasion, where requested to by regulatory bodies, for regulatory or legal reasons, disclose other information relating to personal information.

## Rights of Data Subject

Rights as applicable under the Privacy Act 1988.



## Data Retention in line with The Privacy Act 1988

Enzen retains the data as per the data retention policy listed below (this list is not exhaustive) in line with the Privacy Act 1988:

Data Set Name	Data Examples	Lawful Basis	Storage Method	Retention Period	Method of Disposal
Personnel Data for Human Resources	Employment contracts, personal details, training records, equality & diversity data, absence data, working time opt out agreement Consent/Consent withdrawals	Legal, Contractual, Legitimate Interests: Employment Law, Equality Acts	Held on paper and electronic personnel files, accessible only to Head of People & Culture Australia, BDO Australia.	7 Years	Deletion from Server Hardcopy secure shredding Authority – P&C Manager
	Performance appraisal records, capability & disciplinary	Legitimate Interests: Employee Performance Review	Held on paper and electronic personnel files, accessible only to Line Manager and Head of People & Culture Australia.		
	VEVO Visa & Work Entitlement	Legitimate Interests: Confirm employee work entitlement within Australia	Held electronic personnel files, accessible only to the Head of People & Culture	7 Years	Deletion from Server Hardcopy secure shredding Authority – P&C Manager
Personnel data for payroll	Payroll payments	Legal: For payroll payment and ATO purposes	Payroll system accessible only to Financial Manager / Head of People & Culture, BDO Australia	7 Years	Deletion from Server Hardcopy secure shredding Authority – Finance Manager
Personnel data for superannuation	Superannuation payments	Legal, Contractual, Legitimate Interests	Superannuation data only available to: Financial Manager, Head of People & Culture, BDO Australia, Superannuation Fund	7 Years	Deletion from Server Hardcopy secure shredding Authority – Finance Manager



Data Set Name	Data Examples	Lawful Basis	Storage Method	Retention Period	Method of Disposal
Personnel Data for Safety Compliance	H&S data such as signed safety documentation, site audits, etc.	Legal: H&S Compliance  Vital Interest: Protection of harm to the employee or through omission to others.  Legitimate Interests: Insurance Accident Claims	Held on paper and electronic contract / project files, accessible to office staff only	7 years	Deletion from Server Hardcopy secure shredding Authority – HSE Manager
	H&S data such as signed medical health self-declarations and medical fitness examinations, accident reports etc.	Legal: H&S Compliance  Vital Interest: Protection of harm to the employee or through omission to others.  Legitimate Interests: Insurance Accident Claims	Held on paper and electronic personnel files, accessible only to Line Manager and Compliance Manager.	7 years	Deletion from Server Hardcopy secure shredding Authority – HSE Manager
	Drugs & Alcohol Test	Legal, Vital interest: Proof of fitness to work	Held on paper and electronic personnel files, accessible only to Line Manager and Compliance Manager.	7 years	Deletion from Server Hardcopy secure shredding Authority – HSE Manager
	Driving license checks	Legal, Vital Interest, Legitimate Interest: Road Traffic Acts	Held on paper and electronic personnel files, accessible only to Line Manager and Head of People & Culture	7 years after expiry	Deletion from Server Hardcopy secure shredding Authority – HSE Manager





Data Set Name	Data Examples	Lawful Basis	Storage Method	Retention Period	Method of Disposal
Project	Design/planning etc. as per the scope Project Completion certificate/ design etc.	Legal, Legitimate Interest:	Held as per the Scope/ contractual obligation	As per the contractual obligation	Deletion from Server Hardcopy secure shredding Authority – Account Manager
IT Infrastructure	Data stored on servers/ application Data: As per business requirement Individual's application data: As per business requirement Ex-Employee's e-mail IDs: As deemed by People & Culture Ex-Employee's Data: 3 months or as per business requirement, whichever is greater	Legal, Legitimate Interest	Data stored on servers/ application	As per the contractual obligation	Deletion from Server Hardcopy secure shredding Authority – IT Manager
Administration	Attendance Records Office Security e.g. access cards CCTV Footage	Legal, Legitimate Interest	Physical Document/ Data stored on servers/ application	As per legislation Surveillance Devices Act 1999, Information Privacy Act 2000, Public Records Act 1973, Private Security Act 2004	Confidential documents: Shredded Non-Confidential: Recycles, CCTV footage shall not be deleted, if it is required for legal or regulatory purposes, or where deletion of a record may interfere with formal internal or external investigations Authority – Admin Manager



Data Set Name	Data Examples	Lawful Basis	Storage Method	Retention Period	Method of Disposal
Process Asset Library Documents		Master list updated & maintained/ older versions moved to obsolete	Confidential documents: Shredded Non-Confidential: Re-cycles		Deletion from Server Hardcopy secure shredding Authority – Finance Manager



## Data Security

Enzen takes security of data very seriously. Enzen works towards protecting personal data that is collected from the employees/ contractors /partners from loss, misuse, unauthorised access or disclosure.

The following steps take into account the sensitivity of other Information we collect, process and store, and the current state of technology.

Control measures are built, implemented and practiced consistently in line with all applicable regulatory) & other contractual standard requirements,

We have what we believe are appropriate security controls in place to protect personal data. Risk assessment, including assessing risks to the rights and freedoms of data subjects, is at the heart of our data protection and Information Security Management system. We expect data subjects to be aware of the many information security risks that exist and take appropriate steps to safeguard their own information, beyond our sphere of control.

Risk based approach has been followed, the Information security/Data protection control requirements have been assessed for impact on the existing controls/ processes, to ensure that any associated risks shall not impact our data subject's rights/customer/partners or business interests.

- Enzen shall ensure that risks are minimised by fine tuning the existing controls and implementing new controls.
- Further information can be found under information security management system /Information security compliance policy, which details the steps that shall be adopted to ensure that risks identified with respect to data protection and security requirements are addressed and aligned with this policy.
- The effectiveness of our Information security & data protection management system implementation is measured through regular reviews and audits, and any improvement identified is documented as an action to take forward.

All of our employees/ contractors shall be made aware of:

- Their duty to comply with the information security/ data security policy and procedure and with the requirements of the Data/ Information Security management system,
- The significance of information security/ data security aspects and actual or potential impacts / benefits associated with their work
- Their roles and responsibilities in complying with the IS management system
- The potential consequences of deviation from specified policies/procedures.
- Information security/data protection updates through print media and through iSAFE (Information Security Awareness for Enzenites), prior to starting any project execution.
- The information security/Data protection management system overview as part of the on boarding

## Transferring of Data

Enzen Australia's parent company (Enzen Global Solutions Pvt. Ltd.) is based in Bangalore, India. Enzen utilise a global HR Management System, and subsequently personal data is transferred and accessible by the People & Culture teams globally.



Permissions within the HRMS have been restricted and in most cases, other than where the employee is on secondment to a respective geography, the People & Culture Teams can only access personal data relevant to their geography and based on their roles and responsibilities.

Other than this transference of data, Enzen DO NOT transfer personal data to any external Companies outside of Australia other than the one mentioned in the above section "How we Share, Disclose and Process Data/Information" This section describes how Enzen may share and disclose Information. This is to ensure we fulfil employer's duty of care and to meet our statutory obligations.

Enzen shall assess information security risks and any impact on business-critical processes and systems, and take consent prior to transferring any data to a third party or to our offshore delivery team outside Australia.

## Client Confidential Information

Enzen employees/ contractors may be provided access to information or data shared by our clients. The following care shall be taken on all client supplied material/data/information.

- The client supplied material/data/information shall be maintained in a secure environment within Australia. Written permission from the client must be obtained for transferring/copying/sharing any material/data/information to a location outside Australia. This
- The data/information provided by the client shall be treated confidential and prior written permission must be obtained from client for disclosing the same to any authorised third party.
- Do not use the data/information received from client for any purpose other than that it is intended purpose with at utmost care.
- Personal information (if any) provided by the client shall be used only as necessary for fulfilling contractual obligations with the client, as per the scope.
- Notify the client of any potential, suspected or actual unauthorised use, copying or disclosure of the Confidential Information supplied by the client. Need a ref. the of Notifiable Data Breach Scheme

## Governance and Improvement

We monitor, measure and analyse the effectiveness of our Data Protection/Information Security management system controls. We do this via:

- An effective data protection incident/ breach management process
- Weekly reviews of information security events/incidents (if any)
- Six monthly internal audits done under the guidance of our experts
- Setting, measuring and tracking of Data Protection/ Information security objectives and goals
- Regular Management Review meetings
- Continuously improve the control measures by addressing all weaknesses and improvement areas as identified by the monitoring and review processes

## Breach of Policy

Any breach of this policy and or related policy and procedure will result in immediate suspension and an investigation being undertaken, which could lead to disciplinary action or dismissal.

In severe cases of breach, the Individual may be subject to summary dismissal as a result of gross misconduct, and they may also be subject to criminal prosecution.

## Contact

Enzen Australia

1 King William Street, Adelaide

SA5000, Australia

TEL: [+61 419 106 938](tel:+61419106938)

Email: [carolyn.herraman@enzen.com](mailto:carolyn.herraman@enzen.com)

[www.enzen.com](http://www.enzen.com)





## Enzen Brand Values

It is important to Enzen that our Knowledge practitioner are protected and kept from harm, but that they also understand their responsibilities with respect to protecting our clients and complying with our legal obligations. We therefore expect all of our knowledge practitioners to uphold the following brand values:

- Integrity: We are a fair and reasonable employer, committed to meeting our legal obligations and ensuring our employees are safeguarded.
- Respect: We hold all our employees in high regard and recognise our duties to safeguard their personal data
- Excellence: We will do our utmost to ensure that our policies, procedure and controls are of the highest quality to ensure both the Company and employee is safeguarded.

## Document Control Information

Version	Revision Date	Author(s)	Effected Sections	Brief description of change
0.1	15-Aug-2019	Corporate Excellence Team	All	Initial Draft
0.2	19-Aug-2019	Corporate Excellence Team People & Culture	All	Initial Draft
1.0	20-Aug-2019	Corporate Excellence Team	All	Reviewed and Approved