Everest engineering

Personal information protection

ISM.12

Version 0.2.3

July 1 2025

Contents

1 Introduction

This document outlines the regulations imposed by the General Data Protection Regulation 2016 (GDPR) and the Australian Privacy Principles (APP) concerning the collection, storage, processing and use of personal information. Personally identifiable information (PII) is a subset of personal information that can be used to completely or partially identify an individual.

1.1 Personally identifiable information

Personally identifiable information (PII) is any information that can identify an individual, including information that could be combined with information from other sources. Everest Engineering and its customers have a duty to ensure that PII is protected, not only through direct handling but also in how we design systems.

PII includes direct identifiers such as:

- names;
- phone numbers;
- user names;
- license plate numbers;
- fingerprints;
- credit card numbers;
- birthplace;
- genetic information;
- email addresses and
- license and passport identifiers.

Indirect or quasi-identifiers that can be used to narrow down an individual's identity include:

- date of birth;
- postal code;
- gender; and
- race.

1.2 Scope

This policy applies to all Everest Engineering permanent employees, contractors, advisors and contracted partners using, or granted access to, information assets and information processing facilities owned by Everest Engineering, our customers (whether contracted or not) and third party partners.

1.3 Related documents

The following policies and procedures are relevant to this document:

- Data Protection Impact Assessment Process [Data Protection Impact Assessment Process](Data%20Protection%20Impact%20Assessment%20Process.md)
- Personal Data Analysis Procedure [Personal Data Analysis Procedure](Personal%20Data%20Analysis%20Procedure.m
- Legitimate Interest Assessment Procedure [Legitimate Interest Assessment Procedure](Legitimate%20Interest%20Assessment%20Procedure.md)
- Information Security Incident Response Procedure [Information Security Incident Response Procedure](Information%20Security%20Incident%20Response%20Procedure.md)
- GDPR Roles and Responsibilities [GDPR Roles and Responsibilities](GDPR%20Roles%20and%20Responsibilities.md)
- Privacy Policy (APP) [Privacy Policy (APP)](Privacy%20Policy%20(APP).md)
- Privacy Impact Assessment Process (APP) [Privacy Impact Assessment Process (APP)](Privacy%20Impact%20Assessment%20Process%20(APP).md)
- Privacy Notice Procedure (APP) [Privacy Notice Procedure (APP)](Privacy%20Notice%20Procedure%20(APP).md)

- Personal Information Analysis Procedure (APP) [Personal Information Analysis Procedure (APP)](Personal%20Information%20Analysis%20Procedure%20(APP).md)

2 Personal information retention and protection

2.1 General Data Protection Regulation

The European Union's General Data Protection Regulation (GDPR) gives rights to individuals who are *located* or citizens of a country that is part of the European Economic Area (EEA). These rights give individuals legal control over the information stored about them. The GDPR applies regardless of where the data is stored and the individual's citizenship.

To comply with GDR we must:

- in plain language, disclose what data we collect and process, including the reason for its collection and processing;
- disclose how long information is retained for;
- disclose where information will be stored, if it is transmitted to other countries or third parties;
- obtain clear consent from individuals to collect and process their information through an opt-in system; and
- allow individuals to revoke permission using an opt-out procedure that is no more complicated than how they opted in.

Given its far-reaching application, GDPR directly influences how we design our systems and the systems of our customers.

As a general approach, the best way of complying with GDPR is to:

- collect only information required to provide a service, to the point of handling only third party SSO identifiers (if possible);
- if feasible, anonymise and removing PII as soon as it is no longer needed (such as following identity verification or credit worthiness checks); and
- make it technically simple to erase PII when requested by an individual.

2.2 Australian Privacy Principles

The core tenets of the Australian Privacy Principles (APP) are similar to those of the GDPR:

- we must be open and transparent about the personal information that we collect, its storage, cross-broder transfer and the rights of individuals;
- limiting the collection and retention of solicited information in order to fulfil a primary or secondary function;
- the de-identification or destruction of unsolicited information;
- limiting the disclosure (access outside our organisation) of personal information;
- not using personal information for direct marketing unless consent is explicitly given;
- limiting the transfer and disclosure of personal information to cross-border entities;
- restricting the use and adoption of government issued identifiers;
- required controls to protect personal information;
- providing individuals reasonable access to their personal information; and
- ensuring that collected personal information is up-to-date, that actions are taken to correct mistakes and that the information continues to be relevant.

The APP also allows individuals to deal with us anonymously if doing so is practical.

2.3 Data controller

Everest Engineering will assign the role of *data controller* to one or more individuals. Data controllers are responsible for determining the purpose and means of processing of personal information. All Everest Engineering internal projects *must* have data controller sign off prior to the collection or processing of personal information. Projects for Everest Engineering customers _ should_ consult with a data controller prior to collecting or processing personal information.

The appropriate basis for processing must be identified and documented by data controllers.

2.4 Legal collection and processing of personal information

2.4.1 Explicit consent

Explicit consent allows us to collect and process the personal information of EU residents aged 16 or over. Parental consent is required for individuals under the age of 16. We must explain how this information will be used and the rights that data subjects have. In Australia, the age of consent is generally accepted to be 18.

2.4.2 Performance of a contract

Explicit consent is not required to fulfill a contract with the data subject. This will often be the case where the contract cannot be completed without the personal information in question. For example, a delivery cannot be made without an address to deliver to.

2.4.3 Legal obligation

Explicit consent is not required if personal information is required to be collected and processed in order to comply with the law. For example, this may be the case for some data related to employment and taxation.

2.4.4 Vital interests of the individual

Explicit consent is not required when personal information is required to protect the vital interests of an individual or of another natural person. Some aspects of social care may, for example, collect personal information of another individual in order to protect the rights of someone in our care.

2.4.5 Task carried out in the public interest

Explicit consent is not required when performing tasks believed to be in the public interest or as part of an official duty by authorities. The assessment of the public interest or official duty will be documented and made available as evidence where required.

2.4.6 Legitimate interests

If the processing of specific personal information is in the legitimate interests of Everest Engineering and is judged not to affect the rights and freedoms of the data subject in a significant way, then this may be defined as the lawful reason for the processing. The reasoning behind this view must be documented.

2.5 Breach notifications

Where a breach is known to have occurred that is likely to result in a risk to the rights and freedoms of individuals, relevant supervisory authorities must be informed within 72 hours. This will be managed in accordance with our incident management procedures.

An exception to data breach notification is applicable when the data controller has taken measures to ensure that the risk to the rights and freedoms of data subjects is no longer likely to materialise or when the risk of any serious harm can be mitigated before any serious harm is suffered by the individuals to whom the information relates.

In Australia, we must notify the Office of the Australian Information Commissioner (OAIC) and all affected individuals to whom the information relates where:

- we hold personal information; and
- there is unauthorised access, disclosure or loss of that information; and
- such a breach is likely to result in *serious harm* to an individual.

3 Privacy by design

Everest Engineering adopts the principle of privacy by design. As such, we will ensure that the definition and planning of all new or significantly changed systems that collect or process personal data or information will consider privacy issues.

The impact assessment must include:

- consideration of how personal data will be processed and for what purposes;
- assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose;
- assessment of the risks to individuals in processing personal information; and
- what controls are necessary to address the identified risks and demonstrate compliance with legislation.

3.1 Contracts involving the processing of personal data

Everest Engineering will ensure that all relationships it enters involving the processing of personal information are subject to a documented contract that includes the specific information and terms required by the GDPR.

3.2 International transfer of personal information

Under the GDPR, transfer of personal information outside the European Union must be reviewed prior to the transfer taking place and the outcome of the review to be documented.

Under the APP, international transfers of personal information is permitted where the country of the recipient has a law or binding rules that have the effect of protecting PII similar to the APP. Intra-group international data transfers will be subject to legally binding agreements referred to as binding corporate rules (BCR) which provide enforceable rights for data subjects.