Introduction to the General Data Protection Regulation (GDPR)

Information Pack

Compliance Council

Contents

GDPR: Key Facts 3

Determining if your organisation needs to comply with GDPR 5

Examples of data protection requirements from GDPR 7

GDPR vs. Privacy Act 1988 in Australia 9

Why an Information Security Management System (ISO 27001) can help with GDPR compliance? 13

How to Become Certified to ISO 27001? 14

FAQ's 17

Where can I get more information? 19

Contact Us 20

GDPR: Key Facts

What is GDPR?

The EU's General Data Protection Regulation (GDPR) is the result of four years of work by the EU to bring data protection legislation into line with new, previously unforeseen ways that data is now used.

It introduces tougher fines for non-compliance and breaches, and gives people more say over what companies can do with their data. It also makes data protection rules more or less identical throughout the EU.

What is the purpose of the GDPR?

The purpose of the GDPR is to provide a set of standardised data protection laws across all the member countries. This should make it easier for EU citizens to understand how their data is being used, and also raise any complaints, even if they are not in the country where its located.

Number of potential organisations that will have to comply with GDPR?

Any organisation that collects and process the data of the EU citizens are affected by the GDPR. Each organisation is affected regardless of the size of the organisation and the industry in which the organisation operates. The latest analysis from Veritas suggests that 86 percent of organisations worldwide are concerned that a failure to adhere to GDPR could have a major negative impact on their business.

Abovementioned report may be seen via https://www.veritas.com/content/dam/Veritas/docs/reports/gdpr-report-en.pdf

What are the penalties for not complying with GDPR and how can they be enforced?

There are certain requirements set by EU GDPR to be followed. If an organisation is unable to follow those requirements, they will be penalised with a heavy fine, depending on the offence.

Read on to know details of the offences and the fines that will be imposed on the organisations, if they fail to meet the requirements of EU GDPR.

Category 1: Fine of 10m or 2% of global revenue

A company may be charged with a fine of 10 million Euros or 2% of their annual global revenue if:

- An offence related to child consent. As per EU GDPR, the minimum age for an individual to give consent to access their data has been changed to 16 from 13.
- An offence related to data procession, storage or security of data accessed. The new requirements oblige organisations to inform consumers about the way data is accessed, stored, and processed.
- An offence related to transparency of information.
- An offence related to breach notification. Organisations, according to this new set of regulations, are required to notify EU government in an event of data breach within 72 hours of its occurrence.

Category 2: Fine of 20m or 4% of global revenue

GDPR may penalise a company with a fine of 20 million Euros or 4% of their annual global revenue in the cases of:

- An offence related to data processing.
- An offence related to obtaining the consent of an EU citizen. Every organisation is bound to obtain the content of EU citizens to access their data as per the new requirements laid by EU GDPR.
- An offence related to data subject rights.
- An offence related to not adhering to the Data Protection Regulation Order.
- An offence related to transfer of EU consumer data to third parties. In case a customer has revoked their consent to access and use their personal data, organisations are bound to stop sharing their data with third party companies.

Determining if your organisation needs to comply with GDPR

Who will the GDPR apply to?

The GDPR applies to the data processing activities of businesses, regardless of size, that are data processors or controllers with an establishment in the EU. Generally speaking, a controller says how and why personal data is processed and a processor acts on behalf of the controller. Where a business has 'an establishment' in the EU, activities of the business that involve processing personal data will need to comply with the GDPR, regardless of whether the data is actually processed in the EU.

The GDPR also applies to the data processing activities of processors and controllers outside the EU, regardless of size, where the processing activities are related to:

- offering goods or services to individuals in the EU (irrespective of whether a payment is required)
- monitoring the behaviour of individuals in the EU, where that behaviour takes place in the EU (Article 3).

Data controllers and processors that are covered by the GDPR but not established in the EU will generally have to appoint a representative established in an EU member State (some exceptions apply) (Article 27). The representative is the point of contact for supervisory authorities and individuals in the EU on all issues related to data processing, to ensure compliance with the GDPR.

Australian businesses with customers in the EU, or that operate in the EU, should confirm whether they are covered by the GDPR, and if so, take steps to ensure compliance by 25 May 2018. Please note that some of the definitions with regards to applicability of the regulation (e.g. citizens, residents, travelling natural person which is an EU citizen, data owners) are not crystal clear at this stage and EU Authorities are expected to publish additional guidance to clarify the definitions by the 25th of May 2018.

For example: Australian businesses that may be covered by the GRPR include:

- an Australian organisation with an office in the EU
- an Australian organisation whose website targets EU customers for example by enabling them to order goods or services in a European language (other than English) or enabling payment in euros
- an Australian organisation whose website mentions customers or users in the EU
- an Australian business that tracks individuals in the EU on the internet and uses data processing techniques to profile
- individuals to analyse and predict personal preferences, behaviours and attitudes.

What information does the GDPR apply to?

The GDPR applies to 'personal data'. This means 'any information relating to an identified or identifiable natural person' (Article 4). This has similarities with the definition of 'personal information' in the Privacy Act, which is defined as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable' (s 6(1) of the Privacy Act).

Under the GDPR, additional protections apply to the processing of 'special categories' of personal data, which includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (Article 9). Additional protections also apply to similar categories of 'sensitive information' in the Privacy Act (for example, APP 3.3 (collection of solicited personal information), APP 6.2(a) (use or disclosure of personal information) and APP 7.4 (direct marketing)).

Example: The GDPR makes clear that a wide range of identifiers can be 'personal data' including a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

GDPR's Impact on Australian Companies

Organisations in Australia, which are concerned with offering goods or services to residents of EU or monitoring their behaviour will be affected by EU GDPR implementation. These organisations may include that are associated with exporting goods in EU, providing financial services in that particular region or have direct clients in EU.

The biggest impact of EU GDPR that is going to be on Australian organisations is that they will no longer have full control over digital data. Any Australian business that gathers and/or analyse EU citizen's consumer data will be affected by the new law.

Examples of data protection requirements from GDPR

Individual's Consent

If an organisation wants to store data about a consumer that belongs to EU countries, they must obtain their consent first. The minimum age of a person who can give their consent has been increased to 16 from 13.

Breach Notification

Any company that has access to the EU citizens must notify EU government in case of a data breach event. This notification must be made within 72 hours of discovery of that incident that has led to a security breach.

Availability of Data in Machine-Readable Format

As per new regulations laid by EU GDPR, organisations are required to maintain consumer data in a machine-readable and commonly used format. This is due to the fact that individuals are now given the right to transport their personal data from one controller to another. Therefore, organisations are bound to provide them their personal data if requested by them.

Sharing of Data

Upon the request of the EU citizens, controllers hired by organisations will have to delete their personal data. Moreover, they will also be obliged to stop sharing data with third-parties.

Purpose of Data

EU GDPR provides customer right over their data. They can get hold of electronic companies containing private records of the processing, use, and purpose of their personal data. Organisations are bound to provide all this information to consumers upon their request.

Data Processing Officer

Any company, which is storing consumer data on a large scale, needs to hire a Data Processing Officer to supervise their policies related to data access and use. An existing staff member can take on this additional role. Organisations can also hire a dedicated employee or appoint a contractor to perform the duties of a DPO.

Privacy by Design

Privacy by design is a concept that is requirement within GDPR. . This requirement means that organisations will have to demonstrate that privacy controls have been considered as part of the design phase in a project.

If your organisation is dealing with consumer data in EU, the first thing you need to do is to identify the data your company is accumulating, the purpose it is accessed, and the systems/channels used for its processing. ISO 27001:2013 outlines security controls that will assist an organisation with implementing privacy by design.

According to Article 23 of the EU GDPR, data controllers can only store and process the private data of the EU citizens that is compulsory for the fulfillment of their duties. Furthermore, data access has also been limited to only those individuals who will be in charge of its processing.

As per GDPR, it is the duty of controller to effectively form and implement appropriate policies that will help the organisation to comply with the new standards. This step will ensure data protection methods and privacy in design approach is followed.

Implementing privacy in design approach doesn't imply that it is required by a company to spend a huge portion of their budget on the design of a project. The idea is to employ data protection strategies from the beginning rather considering them in the later stages. The basic requirement that companies need to follow is to take into consideration different factors related to data i.e. it's purpose, nature, scope, processing, and context. Furthermore, organisations also need to consider certain other aspects if they are storing and processing personal data of consumers. These aspects include ways to generate data and process it.

In addition to privacy by design is "privacy by default", organisations are bound to make sure that personal data of the consumer, which they have collected is used for the particular purpose(s) it was collected for. Organisations must employ data protection policies on a technical level. Following such practices will also limit the use, processing, and access of personal data.

GDPR vs. Privacy Act 1988 in Australia

GDPR

After four years of preparation and debate the GDPR was finally approved by the EU Parliament on 14 April 2016. It entered force 20 days after its publication in the EU Official Journal and will be applied in all members states two years after this date. It will be enforced from the 25th May 2018.

Privacy Act 1988 in Australia

The Australian Privacy Principles (APPs) in schedule 1 of the Privacy Act, outline how most Australian Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses (collectively called 'APP entities') must handle, use and manage personal information.

GDPR vs. Australian Privacy Act

	EU GDPR	AUSTRALIAN PRIVACY ACT
Who does this apply to?	Data processing activities of businesses, regardless of size, that are data processors or controllers	Most Australian Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses.
What does it apply to?	Personal data – any information relating to an identified or identifiable natural person: Art 4(1)	Personal information (PI) – information or an opinion about an identified individual, or an individual who is reasonably identifiable: s 6(1)

Jurisdictional link	Applies to data processors or controllers: • with an establishment in the EU, or • outside the EU, that offer goods or services to individuals in the EU or monitor the behaviour of individuals in the EU: Art 3	Applies to businesses: • incorporated in Australia, or • that 'carry on a business' in Australia and collect PI from Australia or hold PI in Australia: s 5B
Accountability and governance	Controllers generally must: • implement appropriate technical and organisational measures to demonstrate GDPR compliance and build in privacy by default and design: Arts 5, 24, 25 • undertake compulsory data protection impact assessments: Art 35 • appoint data protection officers: Art 37	APP entities must take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs and to enable complaints: APP 1.2 Businesses are expected to appoint key roles and responsibilities for privacy management and to conduct privacy impact assessments for many new and updated projects
Consent	Consent must be: • freely given, specific and informed, and • an unambiguous indication of the data subject's wishes which, by a statement or by a clear affirmative action, signifies agreement to processing: Art 4(11)	Key elements: • the individual is adequately informed before giving consent, and has the capacity to understand and communicate consent • the consent is given voluntarily • the consent is current and specific: Office of the Australian Information Commissioner (OAIC)'s Australian Privacy Principle Guidelines

Data Breach notifications	Mandatory DBNs by controllers and processors (exceptions apply): Arts 33-34	From 22nd February 2018, mandatory reporting for breaches likely to result in real risk of serious harm
Individual rights	Individual rights include: • right to erasure: Art 17 • right to data portability: Art 20 • right to object: Art 21	No equivalents to these rights. However, business must take reasonable steps to destroy or de-identify PI that is no longer needed for a permitted purpose: APP 11.2. Where access is given to an individual's PI, it must generally be given in the manner requested: APP 12.5
Overseas transfers	Personal data may be transferred outside the EU in limited circumstances including: • to countries that provide an 'adequate' level of data protection • where 'standard data protection clauses' or 'binding corporate rules' apply • approved codes of conduct or certification in place: Chp V	Before disclosing PI overseas, a business must take reasonable steps to ensure that the recipient does not breach the APPs in relation to the information: APP 8 (exceptions apply). The entity is accountable for a breach of the APPs by the overseas recipient in relation to the information: s 16C (exceptions apply)
Sanctions	Administrative fines of up to €20 million or 4% of annual worldwide turnover (whichever is higher): Art 83	Powers to work with entities to facilitate compliance and best practice, and investigative and enforcement powers: Parts IV and V

Why an Information Security Management System (ISO 27001) can help with GDPR compliance?

Organisations working in Australia, which have access to EU citizen's data must take the following steps in order to comply with the EU GDPR:

- Any such organisation, with access to personal data of EU citizens must have a risk-based methodology in place to manage their privacy.
- They need to identify the data they are processing. For this purpose, they should form and implement effective policies and strategies. Moreover, they also need to identify the channels through which they are accumulating and sharing the said data.
- These companies must also keep in consideration data breach notifications on regular basis. Failing to do so may land them in difficult situations as they will be charged a heavy fine.
- Moreover, they also need to assess the obligation of appointing a Data Protection Officer, who will be responsible for supervising data protection strategies, which they will be implementing.

To comply with the above requirements an organisation should consider developing and implementing an Information Security Management System that complies with the requirements of ISO 27001:2013 which is the international standard for information security management and is considered best practice.

It is regarded as the appropriate safeguard personal information method which focuses on the keeping consumer data safe and secure. With the advancement in technology, its new addition in the GDPR has been made for the protection of the nature of data which can happen from an unanticipated breach of information.

The Australian Privacy Act 1988 prohibited this kind of screening and only limited itself to basic tools for data protection.

How to Become Certified to ISO 27001?

Businesses become certified to ISO 27001 following an audit from a third-party certifying body. Before attaining certification, their information security management system must be deemed compliant with the criteria outlined in ISO 27001.

The certification process is different for every business, depending on its size, industry and the current state of its management systems. In Australia, the general timeframe for attaining certification can be anywhere from 6 to 12 months.

However, at Compliance Council, our experienced compliance consultants have designed an efficient framework to assist your business gain ISO 27001 certification in as little as 8 steps. We call this our 8 Step Process;

1 Gap-Analysis

- Assessing your organisation against AS/NZS and ISO Standards
- Report provided with audit criteria, organisational gaps and recommendations
- Preparation of a project plan in consultation with the internal stakeholders

2 Consultation Workshop

Workshop conducted covering variety of topics to be discussed and considered as part of the Management System, including:

- Special client requirements that need to be met
- Organisational Objectives and how they can be incorporated into the Management System
- Current organisational structure and the way that operations are currently managed

3 System Documents

- Management System Framework that is adapted based on gap-analysis and consultation workshop
- Framework acts as the “bones” of the Management System, as it rarely changes from organisation to organisation. When adapting and adding to the framework it can be pictured as adding “flesh” to the original “bones”

4 Implementation Planning

- Implementation planning meeting conducted with internal stakeholders to develop an implementation plan
- Plan will be executed over a week period with the intention of preparing the organisation for the Stage 2 Certification audit
- Implementation consultant will explain requirements for the audit and the time required from internal stakeholders

5 Awareness Training

- Management System awareness training for manager, supervisors, and employees

6 Implementation Activities

Consultant will execute the activities over a period which include, but are not limited to:

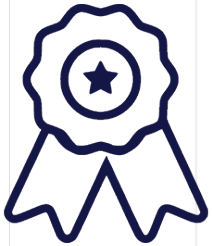
- Preparation of records and various registers for the documented controls
- Conduct the initial management review meeting with key internal stakeholders

7 Internal Audits

Our consultant will conduct a full round review of the management system implementation against the criteria of the initial gap-analysis in consultation with internal staff. This is to ensure that the organisation is adequately prepared for the on-site certification audit.

Conduct internal audits in consultation with internal staff to identify areas for improvement.

8 Third Party Certification Audits



As a part of Stage 1 Audit, the management system consultant will also provide a soft copy of your management system to your chosen Conformity Assessment Body (CAB) who will conduct the document review audit.

Audit conducted on-site by Conformity Assessment Body. The consultant will attend the audit and work directly with the auditor to reduce the amount of time required from internal staff.

FAQ's

What constitutes personal data?

Any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address.

What about Data Subjects under the age of 16?

Parental consent will be required to process the personal data of children under the age of 16 for online services; member states may legislate for a lower age of consent but this will not be below the age of 13.

What is the difference between a EU regulation and an EU directive?

A regulation is a binding legislative act. It must be applied in its entirety across the EU, while a directive is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to decide how. It is important to note that the GDPR is a regulation, in contrast previous legislation, which was a directive.

Does my organisation need to appoint a Data Protection Officer (DPO)?

DPOs must be appointed in the case of: (a) public authorities, (b) organisations that engage in large scale systematic monitoring, or (c) organisations that engage in large scale processing of sensitive personal data (Article 37). If your organisation doesn't fall into one of these categories, then you do not need to appoint a DPO.

How does the GDPR affect policy surrounding data breaches?

Proposed regulations surrounding data breaches primarily relate to the notification policies of organisation that have been breached. Data breaches which may pose a risk to individuals must be notified to the DPA within 72 hours and to affected individuals without undue delay.

Will the GDPR set up a one-stop-shop for data privacy regulation?

The discussions surrounding the one-stop-shop principle are among the most highly debated and are still unclear as the standing positions are highly varied. The European Commission text has a fairly simple and concise ruling in favor of the principle, the EU Parliament also promotes a lead Data Protection Act and adds more involvement from other concerned Data Protection Act's, the Council of the EU's view waters down the ability of the lead DPA even further. A more in-depth analysis of the one-stop-shop policy debate can be found here: https://www.eugdpr.org/controversial-topics.html.

How many countries could be impacted by GDPR?

GDPR affects all the organisations that regularly collect and process the personal data of the EU citizens. This means that all the countries of the world are likely to be affected since the companies that handle the EU citizens' personal data are found in the countries of the world. Thus, 195 countries are likely to be affected.

Where can I get more information?

The following resources may assist Australian businesses to assess whether they are covered by the GDPR and the steps to be taken to comply:

- European Commission, Reform of EU data protection rules
- Article 29 working group (from 25 May 2018, the European Data Protection Board) GDPR guidance
- The Article 29 working group has also developed a general factsheet for Asia Pacific Privacy Authorities (APPA) members. This document may inform entities and interested stakeholders about the GDPR requirements.
- Preparing for GDPR – 12 Steps to take now
- UK ICO website GDPR guidance.

Contact Us

To discuss how our experienced consultants can assist your business with regards to bringing the operations fully-compliant with GDPR, get in touch with us today.

Contact us

1800 771 275

info@compliancecouncil.com.au

Compliance Council