PiperAlderman

Article Information

Authors: Jen Tan, Liam Higgins
Service: Corporate & Commercial, Privacy & Data Protection

Countdown to the introduction of the European Union's General Data Protection Regulation

We discuss the incoming General Data Protection Regulation, how it may affect Australian businesses, and outline the steps that Australian businesses can take to prepare for these changes now.

Please note: *we are authorised to advise on and practice Australian law only and, as such, this article is not legal advice on EU law but is a snapshot of how these incoming changes may be applicable to Australian businesses. We can provide you with more specific advice on how these changes apply to your business by working together with EU associates who are authorised to advise on and practice EU law.*

Snapshot of new obligations

The European Parliament and the Council of the European Union's Regulation (EU) 2016/679 General Data Protection Regulation (GDPR) is set to build certainty and uniformity to harmonise the ways in which many organisations process personal data under data privacy laws across Europe, and protect fundamental rights and freedoms of natural persons. The GDPR will apply to all EU member states from 25 May 2018 and in some cases, may extend to organisations located outside the EU, including those in Australia.

What do the new obligations broadly deal with?

The GDPR primarily relates to the steps that controllers and processors must take in "processing" "personal data" and the steps to take in the event of a personal data breach. "Processing" is broadly described as any operation performed on personal data and includes the collecting, storing, using and disclosing of personal data. "Personal data" includes information relating to an identified or identifiable natural person, such as a person's name or location or more specific factors such as physical, psychological, mental, economic and cultural data.

The GDPR distinguishes special categories of personal data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships, 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. Additional requirements are imposed in respect of these special categories of personal data.

Legal experts who specialise in cyber security can assist by working with IT security experts to raise awareness and educate the board, assist organisations to understand their legal, regulatory and contractual obligations, prepare a cyber security action plan, establish good corporate governance procedures, prepare appropriate policies, provide training, and review contracts and insurance policies to ensure you are ready for these new changes.

The new and expanded rights of a data subject

The GDPR significantly expands the rights afforded to "data subjects" (i.e. individuals) with how their personal data must be treated. These additional rights include:

- the right to be provided with information on data collection;
- the right to have access to the data;
- the right to data portability;
- the right to a restriction of processing;
- the right to object to the processing of data;

- the right of rectification of inaccurate or incomplete personal data;
- the right of erasure (the right to be forgotten); and
- the right to lodge a complaint with a supervisory authority, and to obtain an effective judicial remedy against a controller, processor or a supervisory authority.

Controllers and Processors

The GDPR imposes obligations on "controllers" and "processors" which process personal data. Generally, a "controller" is an entity which determines how and why personal data is processed, and a "processor" is an entity which processes personal data on behalf of the controller. The GDPR will apply to controllers and processors which are either:

- established in the EU and process personal data regardless of whether the processing actually takes place in the EU; or
- not established in the EU and process personal data belonging to data subjects in the EU, where that processing relates to either:
    - the offering of goods or services (irrespective of payment); or
    - the monitoring of their behaviour that occurs within the EU.

As a result of the broad application, Australian businesses may therefore be caught by these new changes as a result of their various activities.

An "establishment" is considered to exist where there is an effective and real exercise of activity through stable arrangements.

Examples where Australian entities may be affected

Australian entities may be affected where they are:

- an Australian business with an office in the EU;
- an Australian business whose website targets EU customers by enabling them to order goods or services in a European language (other than English) or enabling payment in Euros;
- an Australian business whose website mentions customers or users in the EU; or
- 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.

Obligations for processing of personal data

There must be a "lawful basis" to process personal data, which is often referred to as the "conditions for processing", which include:

- consent – which is obtained where the data subject freely gives a specific, informed and unambiguous indication signifying agreement to the processing of their personal data. In this case:
    - silence, pre-ticked boxes and inactivity will not constitute consent;
    - the data subject also has the right to withdraw consent at any time;
- contractual necessity – for the performance of, or entry into, a contract;
- legal obligations – for compliance with a legal obligation;
- vital interests – to protect the vital interests of a person or another person;
- public interest – for the performance of a task carried out in the public interest or in the exercise of official authority; and
- legitimate interests – for the purposes of legitimate interests by the controller or a third party except where such interests are overridden by the interests, rights or freedom of the natural person.

The GDPR also sets out accountability measures relating to the manner in which personal data should be processed and requires personal data to be processed lawfully, fairly, transparently and for legitimate purposes.

Obligations for notification of breach

A "personal data breach" occurs when there is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Where a personal data breach has occurred, notification is generally required.

Notifying the supervisory authority

In the event of a personal data breach, within 72 hours of becoming aware of it, the controller is required to notify the

supervisory authority (which is an independent public authority established by each Member State). The notification must include the following information:

- a description of the nature of the personal data breach;
- the name and contact number of the data protection officer or other contact point where more information can be obtained;
- the likely consequences of the personal data breach; and
- the measures taken or proposed to address the personal data breach.

Communicating the breach to the data subject

Where the personal data breach is likely to result in a "high risk" to the rights and freedoms of natural persons, then after notifying the supervisory authority, the controller must also communicate the breach to data subjects. Examples of "high risk" include where the breach may give rise to discrimination, identity theft, fraud or financial loss. Communication must occur without undue delay and describe in plain clear language the nature of the data breach and include most of the information notified to the supervisory authority.

What are the exceptions to notification?

Notification to the supervisory authority is not required where the personal data breach is not likely to result in a "risk" to the rights and freedoms of natural persons.

Notification to the data subject is not required where the personal data breach is not likely to result in a "high risk" to the rights and freedoms of natural persons. Additionally, communication is not required where:

- the controller has implemented and applied appropriate technical and organisational protection measures to the personal data affected;
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise; or
- communication would involve disproportionate efforts.

Other additional obligations

Additionally, the GDPR also imposes other obligations including:

- keeping records of processing activities; and
- implementing appropriate measures to ensure and be able to demonstrate that processing is conducted in accordance with the requirements of the GDPR. For example, entities should take steps to:
    - assess current practices and develop a data privacy governance structure;
    - implement appropriate privacy notices;
    - obtain appropriate consents; and
    - create a breach reporting mechanism; and
- integrating appropriate technical and organizational measures for the design and security of systems. For example, entities may be required to:
    - appoint a data protection officer;
    - conduct data protection impact assessments; or
    - implement technical measures appropriate to the risk, such as encrypting sensitive data, or by regularly testing, assessing and evaluating the effectiveness of security measures.

Penalties for non-compliance

The supervisory authority has the ability to impose substantial fines on controllers and processors of up to €20 million or 4% of the total worldwide annual turnover for breaches. In determining the magnitude of a fine to be imposed on a controller or, the supervisory authority may consider factors such as the nature, gravity and duration of the infringement and any action taken to mitigate the damage suffered.

The supervisory authority also has wide powers including to investigate, obtain personal data, access the premises and equipment of a controller or processor, issue warnings, reprimands and orders, and to impose bans on processing.

What you should do to prepare for the new obligations

Steps that could be taken to be aware and be prepared for the new obligations imposed under the GDPR include:

- considering how the GDPR will impact on your contractual arrangements;

- seeking legal advice on the application of GDPR and the obligations applicable to your business;
- increasing your board or risk compliance sub-committee's education;
- developing a cyber security action plan and data breach response plan;
- reviewing and developing your corporate governance plan and internal policies;
- preparing draft notification statements to the relevant authority and affected individuals in the event of a data breach; and
- providing further education and training to staff, management and board members on cyber security issues and your obligations under the GDPR.

Seek assistance from the experts

Most entities do not have the specific internal skills, knowledge, experience or expertise to put in place appropriate cyber security measures and protections on their own. It is therefore crucial to engage cyber security experts who are skilled and experienced to assist in managing and reducing the impact of cyber security risks, both from a legal and an IT security perspective.

Legal experts who specialise in cyber security can assist by working with IT security experts to raise awareness and educate the board, assist organisations to understand their legal, regulatory and contractual obligations, prepare a cyber security action plan, establish good corporate governance procedures, prepare appropriate policies, provide training, and review contracts and insurance policies to ensure you are ready for these new changes.

***Please note**: we are authorised to advise on and practice Australian law only and, as such, this article is not legal advice on EU law but is a snapshot of how these incoming changes may be applicable to Australian businesses. We can provide you with more specific advice on how these changes apply to your business by working together with EU associates who are authorised to advise on and practice EU law.*