COMPLIANCE ADVICE

New EU General Data Protection Regulation

16 May 2018 NAT 009/18

SUMMARY

From 25 May 2018, the European Union's General Data Protection Regulation (GDPR) will commence. The GDPR may apply to Australian businesses that process and hold the personal data of European citizens, irrespective of the organisation's size or location.

The following advice may assist you in finding out more about whether the GDPR will affect your business. It is not legal advice or opinion.

Who is affected?

The GDPR may apply to an Australian business – irrespective of size – if:

- it has an establishment in the European Union (EU) which processes personal data as part of its activities in the EU; or
- it does not have an establishment in the EU, but offers goods and services or monitors the behaviour of individuals in the EU.

For example, Australian businesses may be subject to the GDPR if they have:

- an office in the EU;
- a website that targets EU customers e.g. by enabling them to order goods or services in a European language (other than English) or enabling payment in euros;
- a website that mentions customers or users in the EU; or
- 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.

Small and medium-sized enterprises (SMEs) that process personal data as described above may be subject to the GDPR. However, if processing such data is not its core business and that activity does not create risks for individuals, there are some obligations that may not apply to an SME.

For instance, in such circumstances, an SME will not be required to keep records of their processing activities (if it has less than 250 employees), or appoint a data protection officer.

On the other hand, if an SME's main business and regular activity involves processing data that creates risks for individuals, such as monitoring individuals or processing sensitive data or criminal records, then the SME will be subject to these GDPR requirements (amongst other things).

Failure to comply

For the most serious infringement of the GDPR, businesses can be fined up to 4% of their annual global turnover or €20 Million (whichever is higher) by the data protection authorities.

Other options available to the data protection authorities for infringements of the GDPR include a reprimand, or a temporary or definitive ban on processing. In the case of likely infringement, a warning may be issued.

Damages can also be claimed by an individual if a business infringes the GDPR and the individual has suffered material damages e.g. financial loss, or non-material damages such as reputational loss or psychological distress. These can be claimed directly from the business or before the relevant courts of the EU Member State.

What is personal data and processing?

The GDPR applies to the processing of personal data. Under the GDPR, personal data is any information that relates to a directly or indirectly identifiable natural person (i.e. individual).

Examples of personal data includes 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.

The processing of this data includes collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

What is a data controller and processor?

A data controller is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. So if a business decides "why" and "how" the personal data should be processed, it is the data controller.

A data processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. For example, this could be a third party external to the company, or – in the case of groups of undertakings – one undertaking may act as processor for another undertaking.

Accountability obligations of data controllers are outlined under Articles 5, 25, 30, 35 to 43 of the GDPR. Obligations of data processors are outlined under Article 28.

What are the requirements?

The next sections summarise some of the basic requirements in the GDPR. Further information about the GDPR requirements can be found below under "Other sources of information".

Principles relating to processing

The GDPR outlines the principles for businesses processing personal data including around: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; and storage limitation.

These principles are described under Article 5 of the GDPR.

Lawfulness of processing

Processing is lawful only if at least one of a set of conditions is met. These conditions include, but are not limited to:

1. The data subject (i.e. individual) has given consent to the processing of their personal data for one or more specific purposes.
2. Processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract.
3. Processing is necessary for compliance with a legal obligation to which the controller (i.e. business) is subject.

Other conditions are outlined under Article 6 of the GDPR.

Consent

Consent is any freely given, specific, informed and unambiguous indication of the individual's wishes by a statement or by a clear affirmative action. This signifies agreement to the processing of personal data relating to them.

Conditions for consent are detailed under Article 7 of the GDPR, while Article 8 outlines conditions applicable to a child's consent in relation to information society services.

Individual rights

Articles 12 to 23 of the GDPR provides a range of rights for individuals.

There are new individual rights in the GDPR with no equivalent rights under Australia's *Privacy Act 1988* (Cth) (Australian Privacy Act).

These include:

- Right to erasure i.e. right to be forgotten: An individual shall have the right to obtain from the business the erasure of personal data concerning them without undue delay. The business is obligated to erase personal data without undue delay, subject to certain grounds and conditions under Article 17.
- Right to restriction: An individual shall have the right to obtain from the business restriction of processing subject to certain conditions under Article 18. Such personal data shall, with the exception of storage, only be processed with the individual's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the EU or of a Member State.
- Right to data portability: An individual shall have the right to receive the personal data concerning them, which they have provided to a business, in a structured, commonly used and machine-readable format. The individual also has the right to transmit that data to another business without hindrance from the business to which the personal data has been provided. These are subject to certain conditions under Article 20.
- Right to object: An individual shall have the right to object, on grounds relating to their particular situation, at any time to processing of personal data concerning them, subject to certain conditions under Article 21. The business shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the individual or for the establishment, exercise or defence of legal claims. The individual also shall have the right to object relating to personal data processed for direct marketing purposes, and scientific or historical or research or statistical purposes.

Other individual rights in the GDPR include:

- Right to information (Articles 13 to 14).
- Right of access (Article 15).
- Right to rectification (Article 16).

Data breach notifications

Data controllers (i.e. business) shall notify the relevant supervisory authority of a personal data breach within 72 hours after becoming aware of the breach. An exception to this time requirement under Article 33 of the GDPR is if the breach is unlikely to result in a high risk to the rights and freedoms of an individual. If a personal data breach is likely to result in a high risk to the rights and freedoms of the individual, the business shall notify the individual without undue delay.

Data processors (i.e. business) are also required to notify the controller without undue delay after becoming aware of a personal data breach.

A draft breach notification is not required under certain conditions according to Article 34(3).

International transfers

Personal data may be transferred outside the EU to countries or international organisations that provide an adequate level of data protection. Article 45 of the GDPR sets out the elements that the EU Commission will consider when assessing the adequacy of the level of protection.

In the absence of a decision on an adequate level of data protection, or appropriate safeguards, there are limited circumstances where international transfers are permitted, as outlined under Articles 46 and 49.

What happened before?

Prior to the GDPR, the Data Protection Directive (DPD, Directive 95/46/EC) was adopted by the EU in 1995.

As directives are generally suggestive, the DPD was adopted by various EU member states, which resulted in local versions of the DPD.

However, policy makers considered that common ground was needed around data protection laws across the EU. They also recognised that the DPD was adopted at a time when the internet was in its infancy. Over the last 20 years, data generated, collected and used has grown significantly. They therefore sought comprehensive reform of data protection rules in the EU, leading to introduction of the GDPR.

The effect of the GDPR is that it harmonises data protection laws across the EU and replaces existing national data protection rules. And as the GDPR is a regulation (compared to a directive), it is directly binding and applicable.

Comparison between the GDPR and the Australian Privacy Act

In addition to the GDPR, from 22 February 2018, all organisations with an annual turnover of more than $3 million and existing obligations under the Australian Privacy Act need to comply with Australia's new mandatory data breach notification scheme. This is called the Notifiable Data Breach (NDB) scheme.

Some Australian businesses covered under the Australian Privacy Act may also need to comply with the GDPR. Similarly, some Australian businesses not subject to the Australian Privacy Act may need to comply with the GDPR.

There are similarities between the GDPR and the Australian Privacy Act. Australian businesses may already have measures in place to comply with the Australian Privacy Act that will be required under the GDPR.

However, there are also differences between the GDPR and Australian Privacy Act. For example, as discussed above, the GDPR includes new individual rights without equivalents in the Australian Privacy Act.

Therefore, if an Australian business determines that it is subject to the GDPR, they should evaluate their personal data handling practices to ensure they meet the GDPR requirements.

A table comparing the GDPR and the Australian Privacy Act is included at the end of this advice.

Other sources of information

Information about the GDPR was sourced from:

- OAIC Privacy business resource 21: Australian businesses and the EU GDPR;
- Asia Pacific Privacy Authorities EU GDPR – General Information Document;
- UK Information Commissioner's Office Guide to the GDPR; and
- European Commission, 2018 reform of EU data protection rules.

A copy of the GDPR can be found here.

Further information about the NDB can be found in our Member Advice (Ref: NAT 002/18).

Do you require further advice?

Further information about the implications of the GDPR for your business should be sought from an independent legal and cyber security expert.

For information about workplace advice and services relating to internal data breaches within your business, contact our Legal Practitioner Directors: Michael Mead on 02 9466 5538 or Frances Thomas on 02 9466 5545.

Tony Melville
Head of Communications

Table: Comparison between the GDPR and 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: OAIC's APP GLs
Data breach notifications	Mandatory DBNs by controllers and processors (exceptions apply): Arts 33-34	From 22 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

Source: OAIC