Australian Government
Office of the Australian Information Commissioner

October 2016

Privacy business resource X

Australian businesses and the EU General Data Protection Regulation

This resource aims to assist Australian businesses to understand the new requirements in the EU General Data Protection Regulation and how they can comply with Australian and EU privacy laws.

Key messages

- The European Union General Data Protection Regulation (the GDPR) contains new data protection requirements that will apply from 25 May 2018.
- Australian businesses with an establishment in the EU, or that offer goods and services in the EU, or that monitor the behaviour of individuals in the EU may need to comply.
- The GDPR and the Australia *Privacy Act 1988* share many common requirements, including to:
    - implement a privacy by design approach to compliance
    - be able to demonstrate compliance with privacy principles and obligations
    - adopt transparent information handling practices.
- There are also some notable differences, including certain rights of individuals (such as the 'right to be forgotten') which do not have an equivalent right under the Privacy Act.
- Australian businesses should determine whether they need to comply with the GDPR and if so, take steps now to ensure their personal data handling practices comply with the GDPR before commencement.

Introduction

The European Union General Data Protection Regulation (the GDPR) contains new data protection requirements that will apply from 25 May 2018. These will harmonise data protection laws across the EU and

replace existing national data protection rules.[1] The introduction of clear, uniform data protection laws is intended to build legal certainty for businesses and enhance consumer trust in online services.[2]

Some Australian businesses covered by the Australian *Privacy Act 1988* (Cth) (the Privacy Act) (known as APP entities), may also need to comply with the GDPR if they offer goods and services in the EU or monitor the behaviour of individuals in the EU. These privacy laws include some similar requirements. Underpinning both laws is a shared focus on fostering transparent information handling practices and business accountability, to give individuals confidence that their privacy is being protected. Both laws require businesses to implement measures that ensure compliance with a set of privacy principles, and both take a privacy by design approach to compliance. In addition, data breach notification and privacy impact assessments, mandated in certain circumstances under the GDPR, are expected in similar circumstances in Australia. Both laws are technology neutral, which will preserve their relevance and applicability in a context of continually changing and emerging technologies.

Given these similarities, Australian businesses may already have some of the measures in place that will be required under the GDPR. Even so, they should begin taking steps to evaluate their information handling practices and governance structures, seeking legal advice where necessary, to implement the necessary changes well before commencement of the GDPR. Where additional measures are implemented and these are not inconsistent with the Privacy Act, Australian businesses could consider rolling these out across their Australian operations – this could improve consumer trust through enhanced privacy practices and allow for more consistent internal privacy practices, procedures and systems across the business.

Who will the GDPR apply to?

The GDPR applies to the data processing activities of businesses that are data processors and 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[3] 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 data processors and controllers outside the EU where the business' activities involve:

- offering goods or services to individuals in the EU (irrespective of whether a payment is required);[4] or
- monitoring the behaviour of individuals in the EU, where that behaviour takes place in the EU (Article 3).[5]

---

[1] Existing national data protection rules are based on the 1995 Data Protection Directive (Directive 95/46/EC)

[2] European Commission, Joint Statement on the final adoption of the new EU rules for personal data protection, 14 April 2016

[3] 'Controller' means the 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; and 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (Article 4, GDPR).

[4] A processor or controller 'offers goods or services' if 'it is apparent that the controller or processor envisages offering services to individuals in the EU' (Recital 23, GDPR).

[5] A processing activity 'monitors the behaviour' of individuals where individuals are tracked on the internet. This includes profiling an individual to make decisions about that person or to analyse or predict that person's personal preferences, behaviours and attitudes (Recital 24, 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 May 2018.

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.

Example:

Australian businesses that may be covered include:

- an Australian business with an office in the EU
- an Australian business whose website enables EU customers to order goods or services in a European language (other than English) or enables payment in euros[6]
- an Australian business whose website mentions customers or users in the EU[7]
- 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.[8]

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).[9]

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).

[6] GDPR, recital 23
[7] GDPR, recital 23
[8] GDPR, recital 24
[9] The Privacy Act applies to 'personal information' defined as information or an opinion about an identified individual, or an individual who is reasonably identifiable (whether the information or opinion is true or not and whether recorded in a material form or not) (section 6).

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.

What are some of the new requirements in the GDPR?

Accountability and governance

The GDPR sets out expanded accountability and governance requirements. These include that data controllers must:

- demonstrate that they comply with the 'Principles relating to the processing of personal data' – this is referred to as the 'accountability principle' (Article 5).
- ensure and demonstrate through the implementation of appropriate technical and organisational measures, including data protection policies, that their processing activities comply with the GDPR (Article 24).
- implement technical and organisational measures to show that they have considered and integrated data protection into their processing activities – this is referred to as 'data protection by design and by default' (Article 25).

In assessing which technical and organisational measures should be implemented, relevant considerations include the nature, scope, context and purposes of processing as well as the risks for the rights and freedoms of individuals. For data protection by design and default, the 'state of the art' and the 'cost of implementation' are also relevant considerations.

These obligations are similar to Australian Privacy Principle (APP) 1.2, which requires APP entities to 'take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs (and any applicable registered APP code) and to enable complaints'. The OAIC's Privacy management framework: enabling compliance and encouraging good practice, which provides steps the OAIC expects Australian businesses to take to meet their ongoing compliance obligation under APP 1.2, also has a similar focus on strong privacy governance. Like the GDPR, APP 1.2 and the Privacy management framework adopt a privacy by design approach to privacy protection, where entities are considered better placed to meet their privacy obligations if they embed privacy protections in the design of their information handling practices. In addition, like the GDPR APP 1.2 calls for an evaluation of the circumstances, including areas assessed to have greater risk, when deciding on the reasonable steps to be taken to comply with the APPs.[10]

[10] The OAIC's APP guidelines provide that the reasonable steps that an APP entity should take will depend upon circumstances that include the nature of the personal information held, the possible adverse consequences for an individual, the nature of the APP entity and the practicability, including time and cost involved (paragraph 1.6). The OAIC's Privacy management framework also provides steps the OAIC expects entities to take to meet their ongoing compliance obligations under APP 1.2.

Under the GDPR, data controllers must also:

- appoint **data protection officers** to monitor and advise on compliance with the GDPR and with internal privacy policies and procedures (Article 37). It has been described as a 'privacy champion' role that includes the role of a business advisor on the responsible and innovative use of personal data.[11] This requirement only applies to certain businesses. While there is no such obligation under the Privacy Act, in its Privacy Management Framework, the OAIC recommends that organisations embed a culture of privacy by appointing key roles and responsibilities for privacy management, including a senior member of staff with overall accountability.

- undertake a **compulsory data protection impact assessment** prior to data processing, where a type of processing is likely to result in a high risk for the rights and freedoms of individuals (Article 35). While not directly outlined as a legal requirement under the Privacy Act, a privacy impact assessment would be required for many new projects or updated projects involving personal information due to the requirement of APP 1.2.

Consent

Consent is relevant to the operation of many requirements and restrictions on handling personal data under the GDPR. For example, personal data may only be processed under the GDPR, if one of the 'conditions for processing' set out in Article 6, apply. One condition for processing is that the individual 'has given consent to the processing of his or her personal data for one or more specific purposes' (Article 6(1)(a)) (there are also other permitted conditions for processing personal data). In addition, 'explicit consent' is generally required to process 'special categories' of personal data (Article 9).

The GDPR includes a new definition of consent, which states that it must be:

- freely given
- specific
- informed, and
- an unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing' (Article 4(11)).

Consent is not freely given if the individual has no genuine or free choice or is unable to refuse or withdraw consent at any time (Article 7 and recital 42). Businesses also need to make the withdrawal of consent as easy as giving consent, and, before individuals give consent, must inform individuals about this right to withdraw consent (Article 7(3)).

Specific requirements apply in relation to children's consent. If an individual below 16 years wishes to use online services, consent must be obtained from the child's parent (Article 8(1)). However, member States may introduce domestic laws to lower this age to not less than 13 years.

[11] CIPL and its GDPR Project Stakeholders, Privacy & Information Security Law Blog (6 October 2016)

Example:

As silence, pre-ticked boxes or inactivity are not considered consent (recital 32), opt-out consent does not appear to be permitted.[12]

In Australia, the four key elements of consent are:

- the individual is adequately informed before giving consent
- the individual gives consent voluntarily
- the consent is current and specific
- the individual has capacity to understand and communicate consent.[13]

The Privacy Act does not specify an age after which individuals can make their own privacy decisions. While it must be determined on a case-by-case basis, an entity may generally presume that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise.[14]

Mandatory data breach notification

Data controllers must advise the relevant supervisory authority of a data breach within 72 hours of becoming aware of the breach unless the breach is unlikely to impact the rights and freedoms of individuals. Data processors must notify the controller of a breach without undue delay (Article 33). In addition, when a data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must notify the individual without undue delay (Article 34).

While data breach notification is not universally mandatory in Australia, it is highly recommended as good privacy practice. In addition, having in place a data breach policy and response plan may be a reasonable step to ensure the security of personal information as required by APP 11.[15] The OAIC has published, Data breach notification – A guide to handling personal information security breaches, which provides general guidance for agencies and organisation when responding to a data breach involving personal information they hold, and is complemented by the OAIC's Guide to developing a data breach response plan.

Privacy notices

The GDPR requires data controllers to give individuals a range of prescribed information about the processing of their personal data (Articles 13 and 14). This information must be concise, transparent, intelligible and

[12] http://www.mcmillan.ca/The-GDPR--Key-Points-for-Canadian-Businesses?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original

[13] OAIC APP guidelines, Chapter B: Key concepts

[14] For more information about consent, see Chapter B: Key Concepts in the OAIC's APP guidelines.

[15] APP 11 requires an entity that holds personal information to take reasonable steps to protect the information from misuse, interference and loss and from unauthorised access, modification or disclosure.

easily accessible, and use clear and plain language (Article 12). The GDPR supports combining this information with the use of standardized icons to give an easily visible, meaningful overview of processing to individuals (Article 12).

In Australia, APP entities that collect personal information, must take reasonable steps to give individuals notice about certain matters set out in APP 5. The OAIC also supports innovative approaches to privacy notices, for example 'just-in-time' notices, video notices and privacy dashboards to assist with readability and navigability.

Expanded rights for individuals

The GDPR includes a range of new rights for individuals. The right to erasure (known as the 'right to be forgotten') gives individuals a right to require data controllers to delete their data in certain circumstances, including where the information is no longer necessary for the purpose for which it was collected, or where the individual withdraws their consent and there is no other legal ground for processing their data (Article 17). There are exceptions to this right, including where data processing is necessary to exercise the right of freedom of expression and information. There is no equivalent 'right to erasure' under the Privacy Act, however APP 11.2 requires an APP entity that holds personal information to take reasonable steps to destroy the information or to ensure it is de-identified if the information is no longer needed for any purpose permitted under the Privacy Act.[16]

Other enhanced rights for individuals in the GDPR include:

- A right to 'data portability' – a right to receive personal data an individual has provided to an online service provider in a 'structured, commonly used, machine-readable format' and to transmit that data to another online service provider[17] (Article 20)
- A right to object at any time to the processing of an individual's personal data (including profiling[18]). If an objection is made, the processing generally must be stopped. This right only applies to certain types of processing, such as where the legal basis for processing is legitimate business interests, or for direct marketing (including profiling). There are some exceptions that permit organisations to continue processing despite an objection – but these do not apply to processing for direct marketing (Article 21).

New direct obligations on data processors

While the GDPR requirements applying to data controllers are more extensive, some new requirements apply directly to processors.

For example, the relationship between controller and processor generally needs to be set out in a contract, which includes certain prescribed terms. Australian data processing businesses covered by the GDPR should

[16] For more information about APP 11.2, see the OAIC's Australian Privacy Principle guidelines and the OAIC's Guide to securing personal information

[17] This right only applies to personal data that an individual has provided to the controller, where the processing is based on the individual's consent or for the performance of a contract and where processing is carried out by automated means.

[18] Under Article 4(4), profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

be aware of the extent to which the GDPR prescribes specific clauses that must be included such contracts, including that:

- The processor may only process data in accordance with documented instructions from the controller (Article 28(3))
- persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality
- the processor cannot engage another processor without the authorisation of the data controller (Article 28(2))
- assists the controller to satisfy its responsibilities in terms of security obligations, data protection impact assessments and DBN notifications

The processor must also implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (this requirement also applies to controllers) (Article 32).

The way the GDPR regulates 'processors' is somewhat different to the regulation of outsourced service providers under the Privacy Act. For example, the APPs generally apply to an entity that 'holds' personal information – whether that entity has physical possession of that information (including as an outsourced service provider) or controls that information. This means that one entity can physically possess personal information that another entity controls. In such situations, both entities will 'hold' the information at the same time. If covered by the Privacy Act, each will have responsibilities in relation to handling that information under the Privacy Act. For more information about the meaning of 'holds', see Chapter B of the Australian Privacy Principle guidelines and Privacy business resource 8: sending personal information overseas.

Overseas transfers of personal data

Under the GDPR, personal data may be transferred outside the EU to countries or international organisations that provide an adequate level of data protection. The GDPR sets out in detail the factors the EU Commission is to consider when deciding whether a third country or international organisation ensures an adequate level of protection (Article 45).[19] The European Data Protection Board is required to provide the Commission with an opinion assessing the adequacy of a country or organisation's level of data protection (Article 70(1)(s)).

Where the EU Commission has not decided that a third countries' level of data protection is adequate, overseas transfers are permitted in some limited circumstances, including:

- the data controller has in place approved 'binding corporate rules' that enable transfers within a corporate group
- the data controller has entered into an agreement that contains the 'standard data protection clauses' adopted by the EU Commission or a data protection authority

[19] The European Commission website has more information about countries that are currently recognised as adequate.

- approved codes of conduct are in place, and the recipient controller or processor gives binding and enforceable commitments to apply appropriate safeguards
- an approved certification has been made by an accredited body, and the recipient controller or processor gives binding and enforceable commitments to apply appropriate safeguards (Article 46).

APP entities that disclose personal information overseas, must comply with APP 8. This generally provides that before an APP entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information (exceptions apply). An APP entity that discloses personal information to an overseas recipient is accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs (s 16C). For more information about APP 8, see the OAIC's APP guidelines, Chapter 8, and OAIC Business Resource 8: Sending personal information overseas.

Sanctions

The GDPR gives supervisory authorities the power to impose administrative fines for contraventions, with fines of up to €20 million or 4% of annual worldwide turnover, whichever is greater for certain types of contraventions (Article 83(5)).

Examples:

Infringements that are subject to a maximum penalty of €20 million or 4% of annual worldwide turnover include breach of:

- the data processing principles in Articles 5, 6, 7, and 9 (including conditions for consent)
- the data subjects' rights under Articles 12 to 22 (such as rights to transparency, access rectification, right to be forgotten to personal data and right to data portability)
- the requirements relating to the transfer of personal data to a recipient in a third country or an international organisation under Articles 44 to 49.

The Privacy Act confers on the Commissioner a range of privacy regulatory powers. These include powers that allow the OAIC to work with entities to facilitate legal compliance and best privacy practice, as well as investigative and enforcement powers to use in cases where a privacy breach has occurred. These powers are outlined in the OAIC's Privacy regulatory action policy.

Does the GDPR apply to processing personal data for law enforcement purposes?

No. The *EU Police and Criminal Justice Data Protection Data Protection Directive* 2016/ 680 applies to data protection in the police and justice sectors. It aims to protect personal data processed for prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. It applies to the cross-border processing of personal data, as well as to the processing of personal data at a national level.

EU member States have a two-year period to implement the Directive into their national law. Member States must adopt any relevant legislation for compliance with the Directive by 6 May 2018.

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*
- UK ICO website GDPR guidance
- Article 29 working group GDPR guidance (to be published soon)

For further information

GPO Box 5218 Sydney NSW 2001 | **P** 1300 363 992 | **E** enquiries@oaic.gov.au

Or visit our website www.oaic.gov.au