Australian Government
Office of the Australian Information Commissioner

Updated June 2018

Privacy business resource 21

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 of any size may need to comply if they have an establishment in the EU, if they offer goods and services in the EU, or if they monitor the behaviour of individuals in the EU.
- The GDPR and the Australian 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.[1] These will harmonise data protection laws across the EU and replace existing national data protection rules.[2] The introduction of clear, uniform data protection laws is intended to build legal certainty for businesses and enhance consumer trust in online services.[3]

Some Australian businesses covered by the Australian *Privacy Act 1988* (Cth) (the Privacy Act) (known as APP entities), may need to comply with the GDPR if they:

- have an establishment in the EU (regardless of whether they process personal data in the EU), or
- do not have an establishment in the EU, but offer goods and services or monitor the behaviour of individuals in the EU.

These privacy laws include some similar requirements. Both laws foster 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. Data breach notification is required in certain circumstances under the GDPR and under the Privacy Act (from February 2018).[4] In addition, 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 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, 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.[5] 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.

---

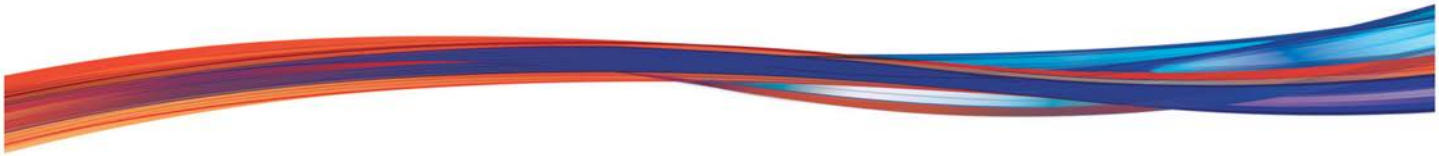
[1] EU member States have a two-year period to implement the Directive into their national law. Member States must adopt any relevant legislation for compliance with the Directive by 6 May 2018.

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

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

[4] Privacy (Notifiable Data Breaches) Act 2017 (available at www.legislation.gov.au).

[5] '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).



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)[6]
- monitoring the behaviour of individuals in the EU, where that behaviour takes place in the EU (Article 3).[7]

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 May 2018.

Example: Australian businesses that may be covered by the GRPR include:

- an Australian business with an office in the EU
- an Australian business 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[8]
- an Australian business whose website mentions customers or users in the EU[9]
- 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.[10]

Australian Privacy Act

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.[11]

[6] 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).

[7] 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).

[8] Recital 23, GDPR.

[9] Recital 23, GDPR.

[10] Recital 24, GDPR.

[11] More information about the Australian Privacy Principles is available on the OAIC website, www.oaic.gov.au.

The Privacy Act applies to businesses that are incorporated in Australia. It also applies to businesses outside Australia if they collect personal information from, or hold personal information in, Australia and carry on a business in Australia (s 5B of the Privacy Act).

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).[12]

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'[13] 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.

What are some of the new requirements in the GDPR?

Outlined below are some of the new and enhanced requirements in the GDPR and how these compare to requirements in the Privacy Act and expectations of good privacy practice in Australia. This resource does not, however, outline all of the key requirements in the GDPR, particularly where those requirements are broadly similar to existing requirements. Examples of key responsibilities that are not considered in detail in this resource include:

- 'principles relating to data processing' in Article 5
- the 'lawfulness of processing' requirements in Article 6
- the 'processing of special categories of personal data' requirements in Article 9
- 'security of processing' requirements in Article 32.

While some important changes are described below (such as the addition of an 'accountability principle' and changes to the definition of 'consent'), these important requirements are not outlined in this resource as they

[12] For more information about the meaning of 'personal information', see Chapter B of the APP guidelines.

[13] 'Sensitive information' is defined in s 6(1) of the Privacy Act.

are broadly similar to existing requirements. For more information, see 'Where can I get more information?' below.

Accountability and governance

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

- demonstrate that they comply with all the principles set out in Article 5 of the GDPR ('Principles relating to the processing of personal data') (Article 5(2))
- implement appropriate technical and organisational measures, including data protection policies, to ensure and be able to demonstrate that processing complies 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 by default, the 'state of the art' and the 'cost of implementation' are also relevant considerations.

Example 1: To meet the principles of data protection by design and default, a data controller's internal policies and practices could include:

- minimising the processing of personal data
- pseudonymising personal data as soon as possible
- transparency as to the functions and processing of personal data
- enabling the individual to monitor the data processing
- enabling the controller to create and improve security features.

Example 2: When developing, designing or using a product, service or application that processes personal data, developers should be encouraged to take account of individual's right to data protection and encouraged to ensure controllers and processors can fulfil their data protection obligations.[14]

[14] Recital 78 of the GDPR.

Additional governance requirements under the GDPR include:

- Controllers and processors must, in certain circumstances, appoint a data protection officer to monitor and advise on compliance with the GDPR and with internal privacy policies and procedures (Article 37).[15] 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.[16] This requirement only applies to certain businesses.
- Controllers must undertake a compulsory data protection impact assessment (DPIA) 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). Where a DPIA indicates that processing operations involve a high risk in the absence of mitigation measures being taken, the controller needs to consult with a supervisory authority before processing begins (Article 36).
- Controllers (and their representatives) must keep records of processing activities under their responsibility (exceptions may apply to some small businesses) (Article 30).
- Controllers are encouraged to draw up codes of conduct to contribute to the proper application of the GDPR. These can take account of the specific features of the sector involved and the needs of small and medium-sized enterprises (Article 40).

Australian Privacy Act

The Privacy Act includes similar requirements to the 'accountability' and 'privacy by default and design principles' in the GDPR. For example, APP 1.2 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 also has a similar focus on strong privacy governance. It provides steps the OAIC expects Australian businesses to take to ensure good privacy practice and to meet their ongoing compliance obligation under APP 1.2. It also 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.

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. APP 1.2 also 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.[17]

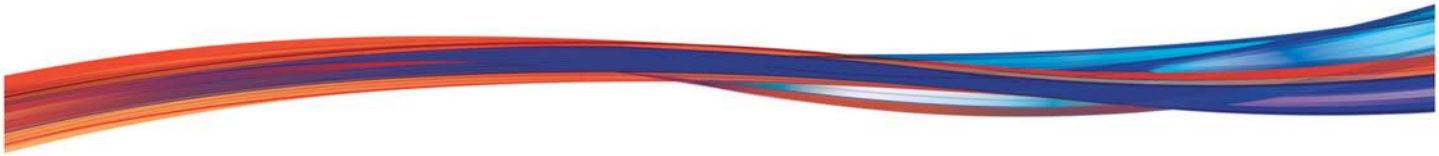
As regards privacy impact assessments (PIAs), the requirement in APP 1.2 means that a PIA would be required for many new projects or updated projects involving personal information.

---

[15] The requirement to designate a data protection officer only applies to a business whose core activities 'consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subject son a large scale', or whose core activities 'consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.'

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

[17] 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.



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
- 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)).

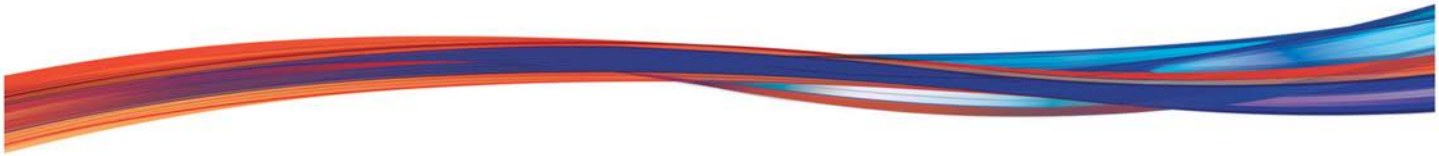
The data controller needs to be able to demonstrate that the individual has consented to the processing. Consent is not freely given if the individual has no genuine or free choice or is unable to refuse or withdraw consent at any time (Article 7 and recital 42). Businesses also need to make the withdrawal of consent as easy as giving consent, and, before individuals give consent, must inform individuals about this right to withdraw consent (Article 7(3)). When consent is given in the context of a written declaration, which also concerns other matters, it has to be clearly distinguishable from other matters and provided in an intelligible and easily accessible form using clear and plain language (Article 7(2)).

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 a person with parental responsibility for the child (Article 8(1)). However, member States may introduce domestic laws to lower this age to not less than 13 years.

Example 1: Silence, pre-ticked boxes or inactivity are not considered consent.[18]

Example 2: A controller that uses data analytics to process the personal data of customers may require prior informed and express consent to do so.

[18] Recital 32 of the GDPR.



Example 3: The practice of 'bundling' together multiple requests for an individual's consent to a range of different data processing operations (known as 'bundled consent') is not considered consent where separate consents are appropriate in the circumstances.[19]

Australian Privacy Act

In Australia, 'consent' means 'express consent or implied consent'.[20] 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.

Australian businesses that are covered by the EU GDPR may decide to standardise their consent mechanisms to allow for more consistent privacy practices and systems across the business.

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.[21]

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 result in a high risk to 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). There are exceptions to this notification requirement (Article 34(3)).

Australian Privacy Act

A notifiable data breaches scheme commenced in Australia on 22 February 2018. The scheme applies to 'eligible data breaches'—where the breach is likely to result in serious harm to any of the individuals to whom the information relates. It requires APP entities to provide a statement to the Commissioner notifying of an eligible data breach as soon as practicable after the entity becomes aware of the breach. It also requires entities to notify affected individuals as soon as practicable after preparing the statement for the Commissioner. Like the GDPR, exceptions to these requirements. For more information, see **www.oaic.gov.au/ndb**

[19] Recital 43 of the EU GDPR.

[20] Section 6(1) of the Privacy Act.

[21] For more information about 'consent', see OAIC APP guidelines, Chapter B: Key concepts.

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 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).

Australian Privacy Act

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 and enhanced rights for individuals. The right to erasure (which encompasses the 'right to be forgotten') gives individuals a right to require data controllers to delete their data in certain circumstances, including, but not limited to 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).

Where a controller is required to erase personal data, it must also take reasonable steps to inform controllers which are processing the same personal data, of any links to, copies of, or replication of that personal data.

There are exceptions to this right, including where data processing is necessary to exercise the right of freedom of expression and information.

Another enhanced right for individuals in the GDPR is the right to object at any time to the processing of an individual's personal data (including profiling).[22] If an objection is made, the controller must generally stop the data processing. 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 rights for individuals in the GDPR include:

- A right to 'data portability'—a right to receive personal data an individual has provided to a controller in a 'structured, commonly used, machine-readable format' and to transmit that data to another controller, where the data is processed electronically. 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 (Article 20).

- A right to restriction of processing—in certain circumstances an individual has the right to obtain a restriction on processing of their personal data from the controller. Where processing is restricted,

[22] 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.

personal data may only be processed in certain limited circumstances including with the individual's consent. For example, if an individual contests the accuracy of their personal data, there may be a temporary restriction on processing to enable the controller to verify the accuracy of the personal data (Article 18).

Australian Privacy Act

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.[23]

The Privacy Act does not include an equivalent right to 'data portability' or 'right to object'. However, individuals do have a right to request access to, and correction of, their personal information under APPs 12 and 13. In giving access under APP 12, where reasonable and practicable, an entity must give access in the manner requested by the individual. For more information, see Chapters 12 and 13 of the APP guidelines.

The Privacy Act does not include a right to the restriction of processing. However, there are requirements on APP entities to take reasonable steps to ensure the quality of personal information under APP 10 and to correct incorrect personal information under APP 13.

New direct obligations on data processors

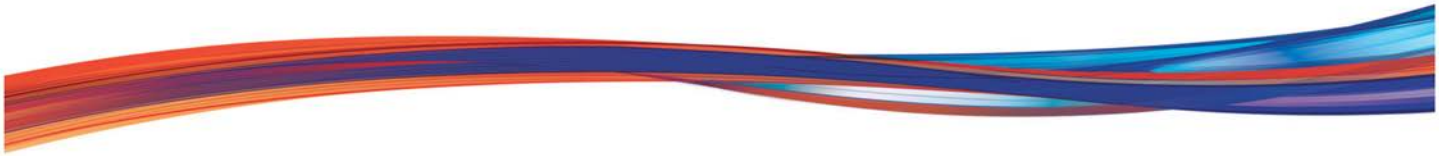
While the GDPR requirements applying to data controllers are more extensive, some new requirements apply directly to processors. A key requirement is that a controller must only use processors that provide sufficient guarantees, that they will implement appropriate technical and organisational measures that ensure compliance with the GDPR and protect the rights of the data subject (Article 28(1)).

The relationship between controller and processor generally needs to be set out in a contract, which includes certain prescribed terms. Australian data processing businesses should be aware of the extent to which the GDPR prescribes specific clauses that must be included in such contracts, including that:

- the processor may only process data in accordance with documented instructions from the controller (Article 28(3))
- the processor must ensure that persons authorized to process 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).

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



Australian Privacy Act

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).[24] The European Data Protection Board (which replaces the Article 29 Working Party) 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)).

In the absence of an adequacy decision, overseas transfers are permitted in some limited circumstances, on condition that individual's enforceable rights and effective remedies are available and, where appropriate, safeguards are in place. Such appropriate safeguards include:

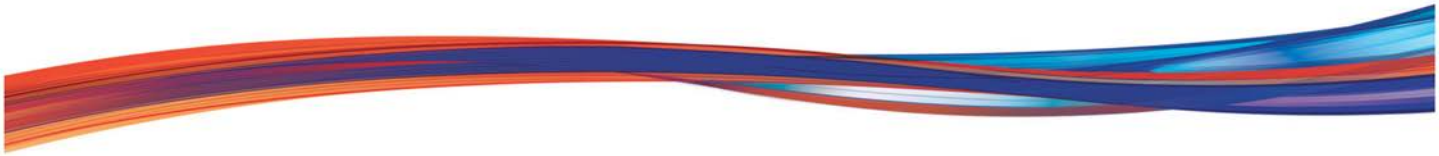
- the data controller has in place approved 'binding corporate rules' that enable transfers within a corporate group
- the data controller has entered into an agreement that contains the 'standard data protection clauses' adopted by the EU Commission or a data protection authority
- approved codes of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

In the absence of an adequacy decision or appropriate safeguards such as those outlined above, overseas transfers are also permitted in very specific situations. An example is where an individual explicitly consents to the proposed transfer after they have been provided with certain information about the possible risks associated with the transfer (Article 49).

Australian Privacy Act

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

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



for any acts or practices of the overseas recipient in relation to the information that would breach the APPs (exceptions apply) (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 by controllers or processors, with fines of up to €20 million or 4 per cent of annual worldwide turnover, (whichever is higher), for many types of contraventions (Article 83(5)).

Examples: Infringements that are subject to a maximum penalty of €20 million or 4 per cent of annual worldwide turnover include:

- 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 GDPR also requires the EU Commission and supervisory authorities to cooperate, engage and provide mutual assistance in the enforcement of data protection laws with privacy authorities outside of the EU (Article 50).

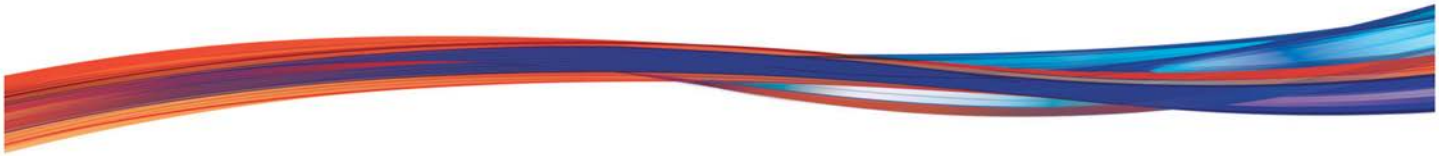
Australian Privacy Act

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.

The OAIC is also committed to internationally coordinated approaches to privacy regulation, recognising that APP entities carry on their business globally and that personal information is regularly disclosed, handled and stored overseas. This includes participating in several international forums and arrangements to:

- promote best privacy practice internationally
- address emerging privacy issues in our region
- cooperate on cross-border privacy regulation and enforcement matters.[25]

[25] More information about the OAIC's international networks is available at https://www.oaic.gov.au/engage-with-us/networks.



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.

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:

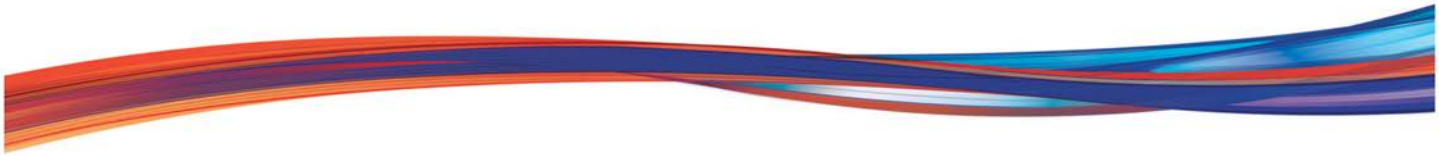
- European Commission, *2018 reform of EU data protection rules*
- European Data Protection Board (prior to 25 May 2018, the Article 29 Working Party) GDPR guidance
- Asia Pacific Privacy Authorities *EU General Data Protection – General Information Document*
- UK Information Commissioner's Office *Guide to the GDPR*.

For Australian government agencies, see Does the GDPR apply to Australian government agencies?

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



	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