GDPR: a guide for Australian businesses

Peter Leonard[1]
Principal, Data Synergies

Overview

The General Data Protection Regulation 2016 (**GDPR**) effects a complete overhaul of EU data protection law. The Regulation will automatically apply across the EU from 25 May 2018. The UK government has confirmed that this application will include the UK, regardless of Brexit.

The core concepts underlying the GDPR are:

- individuals (natural persons) should have control of their personal data; and
- this is a fundamental right that the individual has when they arrive to purchase a business's product or service,
- this right should not be easy for individuals to bargain away.

The GDPR addresses individuals as consumers with little bargaining power that frequently deal with service providers headquartered outside the EU. The EU is less inclined than most Asia Pacific jurisdictions to rely upon notice and/or consent as mechanisms for privacy compliance, because (in the view of the drafters of the GDPR) these mechanisms do not provide adequate consumer protection for individuals.

The GDPR uses similar terms to many other national privacy laws, including the Australian Privacy Act 1988. However, there are very important differences in the laws, and how relevant terms are used in those laws, so superficial similarities frequently are misleading.

The GDPR defines 'personal data as:

> "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly (…), in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person."[2]

Australian businesses will note that the definition of 'personal data' is similar to the definition of 'personal information' in the Australian Privacy Act.

The European Commission interprets the GDPR definition of 'personal data' as:

---

[1] Peter Leonard is a data, content and technology business consultant and lawyer and principal of Data Synergies. Peter chairs the IoTAA's Data Access, Use and Privacy work stream. The IoT Alliance (www.iot.org.au) is Australia's peak IoT body, bringing together industry government and regulators to address issues affecting IoT adoption and implementation. Peter also chairs the Law Society of New South Wales' Privacy and Communications Committee and the Australian Computer Society's Artificial Intelligence and Ethics Technical Committee. He serves on a number of relevant advisory boards, including of the NSW Data Analytics Centre. Peter was a founding partner of Gilbert + Tobin. Following his retirement as a partner in 2017 he continues to assist Gilbert + Tobin as a consultant.

[2] See further information available through the European Commission's GDPR Portal at https://www.eugdpr.org/, including useful GDPR FAQs at https://www.eugdpr.org/gdpr-faqs.html

"Any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address."[3]

1. Extraterritoriality

The GDPR has extraterritorial effect, in contrast to the current EU data protection directive. The GDPR applies to:

- processing activities of data controllers and data processors established in the EU, whether or not the processing takes place in the EU. Broadly, a controller says how and why personal data is processed, and a processor acts on behalf of the controller.[4] Where an Australian business has 'an establishment' in the EU, activities of the group that involve processing personal data will need to comply with the GDPR, regardless of whether the data is actually processed in the EU;[5]

- the processing of personal data of data subjects who are in the EU by a data controller or data processor not established in the EU where the processing activities relate to offering goods or services to data subjects in the EU;[6] and

- the processing of personal data of data subjects who are in the EU by a data controller or data processor not established in the EU where the processing activities relate to monitoring the data subjects' behaviour in the EU.[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 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]

[3] 'What constitutes personal data?' at https://www.eugdpr.org/gdpr-faqs.html

[4] '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).

[5] 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).

[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.

- 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]

For data transfers outside the EU, the GDPR maintains the same requirements as the current data protection directive. Such transfers occur, for example, when persons located in Australia have access to data stored in the EU. When personal data collected in the EU is transferred to Australia or any other country which, from a European point of view, does not afford an adequate level of protection, important restrictions apply. Such transfer is forbidden, except if the data exporter has taken certain precautions such as:

- signing the relevant standard contractual clauses;
- adopting binding corporate rules;
- certifying into the Privacy Shield scheme.

The GDPR adds other new transfer mechanisms[11], including pursuant to an industry code of conduct approved by a relevant EU regulator. It remains to be seen how important these alternative mechanisms will become in practice.

2. Processing of Personal Data Under the GDPR

Where the GDPR applies to the processing of personal data, an Australian business should conduct an initial assessment as to whether it (or any of its affiliates) is acting as a data controller or a data processor in these processing activities. Different obligations will apply depending on the activity of the Australian business.

A **data controller** is ultimately responsible for compliance with the data protection principles, which (broadly) are to the effect that personal data must be:

- processed lawfully, fairly, and in a transparent manner in relation to individuals;
- collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest or for scientific or historical research purposes or statistical purposes will not be considered to be incompatible with the initial purpose(s);
- adequate, relevant, and limited to what is necessary in relation to the purposes for which the data is processed;
- accurate and, where necessary, up to date – and every reasonable step must be taken to ensure that personal data that is inaccurate with regard to the purposes for which it is processed is erased or rectified without delay;
- kept in a form that permits identification of data subjects for no longer than necessary for the purposes for which the personal data is processed; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and accidental loss, destruction, or damage, using appropriate technical or organizational measures.

[10] Recital 24, GDPR.

[11] Articles 44 to 49 inclusive: see also Articles 40 to 43 in relation to codes of conduct and certification.

Australian businesses will note that these principles are broadly similar to the Australian Privacy Principles.

Personal data is lawfully processed if the data subject has consented to the processing or a permitted derogation applies such as legal or contractual necessity. Further, there are strict conditions imposed on whether consent is validly obtained by the data controller.

There are also direct obligations on **data processors** under the GDPR regarding:

- security of processing operations,
- appointment of a Data Protection Officer (DPO),
- engagement of sub-processors, and
- notification of any breach of data protection obligations (including data security incidents) to the data controller.

3. Key features

Key points for Australian businesses to note include:

- **Limited exceptions** - There is no general 'small business exception' such as in Australia, nor any exception for 'employee records.
- **Notification** – No requirement to notify authorities of data processing, but a requirement to keep records of data processing activities (subject to limited exceptions for SMEs).[12]
- **Penalties** – As is now notorious, maximum penalties of 4% annual global turnover, or up to 20m Euros, whichever is higher.
- **DPOs** – Requirement to appoint a DPO where an organisation's core business involves processing personal data involving regular and systematic monitoring of data subjects, or of large amounts of sensitive personal data.[13] Member States will also have discretion to enact national provisions imposing further requirements regarding appointment of DPOs. See further as to DPOs in section 4 below of this paper.
- **Breach reporting** – breaches must be reported to the relevant regulator without undue delay and, where feasible, within 72 hours of becoming aware of it unless the breach is unlikely to result in a risk to the rights and freedoms of individuals. Data subjects must be informed without undue delay where the breach is likely to result in a high risk to the data subject's rights and freedoms unless the data has been rendered unintelligible to any third party (for example by encryption), the data controller has taken steps to ensure the high risk is unlikely to materialise or it would involve disproportionate effort to inform data subjects individually in which case a public announcement can be made. Data processors are required to inform data controllers of any breach without undue delay.
- **Consent** – organisations relying on consent to process personal data will need to show that the consent is freely given, specific and informed and is an "unambiguous indication" of a data subject's wishes and expressed either by a statement or a clear affirmative action. Consent will be purpose limited i.e. related to explicitly specified purposes.

[12] Article 30.

[13] Article 37 GDPR.

- **Privacy by design and default** – Controllers are specifically prevented from setting defaults to disclose data to all.

- **Purpose limitation** – data processing must be carried out for the original purpose(s) for which it was collected unless the new purpose is a compatible one.

- **One Stop Shop** – Organisations will be regulated by a single 'lead' regulator in the place of their main EU establishment. The main establishment will be the main administrative location in the EU unless the main decisions about data processing are taken in a different Member State in which case that will be the main establishment. Individuals will be able to make complaints in their Member State at which point that regulator will engage in a cooperation procedure which will be settled by the European Data Protection Board in the event of disagreement. Member State regulators will also be able to deal with any issues arising in their own jurisdictions subject to a cooperation procedure.

- **Data subject rights** – new rights around data portability, the 'right to be forgotten' and to prevent profiling[14].

- Continuation of right **to object to processing**, to **rectification** and **erasure**.

- **Digital consent for minors** – while the default age for giving valid consent and using online services is set at 16, Member States will be able to reduce this to as low as 13.

4. Steps that an Australian business should take to effect compliance with the GDPR

- **Map your data** – Understand personal data you control or process and what you do with that data, including any profiling activities and any uses and/or disclosures of deidentified information. Conduct an assessment of what personal data is processed or otherwise stored or held by the organization and/or its affiliates, where it is held, the categories of data subjects (e.g., employees, contractors, contact points at commercial organizations, customers), the nature of the personal data (including if it is sensitive personal data), for how long is it being retained, whether it is current or historical, how it was obtained (so far as possible), how it is used and with whom it is shared, and the locations of the recipients of the personal data (i.e., identify the data flows). A formal data mapping exercise which documents this will help you understand what you need to do to be compliant with both the GDPR and the Australian Privacy Act, and also help you demonstrate compliance.

  Identify who is responsible for PI – It is essential to have proper data privacy governance in place. Whether or not you already have a DPO, and whether or not you are required to appoint one under the GDPR, Australian businesses need to identify the chain of responsibility and reporting lines around use of personal data. It is essential for senior management to be involved from the outset and for data protection to be an issue which is scrutinised at board level. Responsibilities of DPOs at a minimum include informing the company and its employees on their obligations with respect to data protection law, monitoring the company's compliance, monitoring privacy impact assessments, cooperating with supervisory authorities and handling data subjects' inquiries.

[14] 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.

A DPO may be appointed within the company or outsourced. A DPO may carry out other tasks as well (as long as there are no conflicts of interest), but the GDPR requires that DPOs must perform their duties and tasks in an independent manner and with a sufficient degree of autonomy. This means that DPOs must not be instructed about how to deal with a matter, or whether to consult the supervisory authority. The expectations as to professional autonomy of in-house legal counsel may provide a useful analogy. The status and reporting requirements of existing compliance personnel in many organisations will not be an appropriate analogy.

- **Assess current practices** – Identify compliance gaps between current practices and future requirements.

- **Review internal policies and train your staff** – Are your internal policies compliant? Do staff know what is expected of them with regard to processing personal data including dealing with data breaches, handling subject access requests and conducting privacy impact assessments?

- **Review any data processor agreements** – Whether you are a controller or processor, you should look at existing and future agreements to ensure they adequately deal with responsibility and liability given the new direct compliance requirements for data processors.

- Look at current **privacy statements, notices and consents** – As well as more exacting 'notice' requirements[15], it will be significantly harder to meet consent requirements under the GDPR than under the Australian Privacy Act or many other national laws. If you rely on consent to process personal data, you will need to ensure already obtained consents will still be valid. You may have to collect new (replacement) consent. You must ensure consent is documented. You may also want to consider other purposes as a justification for processing the data, particularly in relation to HR data.

- The GDPR requires both data controllers and processors to implement **adequate technical and organisational measures to ensure data is processed securely and is adequately protected**. If you are already complying with APP 11 (security of PI), you should already be implementing privacy by design and default, taking technical security measures and using techniques like pseudonymisation to minimise risk. You also need to ensure regular, rolling review and updates.

- **Privacy Impact Assessments (PIAs)** – Organisations will be required to carry out data protection impact assessments (PIAs) if their proposed activities are likely to result in a high risk for the rights and freedoms of individuals. The Commission gives as examples of 'high risk' implementation of new technologies, automatic systematic processing and evaluation of personal information, large-scale monitoring of a publicly accessible area (e.g. by CCTV) and large-scale processing of sensitive data like biometrics.[16] If the PIA reveals a significant risk, the organisation must consult with their regulator before beginning the processing. If you are already complying with APP 1.2, you should already be conducting PIAs (ideally on a legally privileged basis) for determining risk and demonstrating compliance for both data controllers and data processors. Ensure there is a policy for when and how PIAs need to be carried out and decisions made, that is consistent with requirements of both GDPR and the Australian Privacy Act.

[15] The data controller must provide a privacy notice to data subjects regarding the processing of their personal data. The privacy notice must be provided at the time of collection of the personal data or, if it was collected via a third party, within a reasonable period of being collected. The privacy notice must be concise, transparent, intelligible, and easily accessible; written in clear and plain language; and provided free of charge. The GDPR requires transparency and has certain prescribed elements which must be included in privacy policies like, for example, informing data subjects of their rights under the GDPR.

[16] http://ec.europa.eu/justice/smedataprotect/index_en.htm

- **Do you know how to handle a data breach?** – Even the most careful businesses are vulnerable to data breaches but their impact can be significantly minimised if you have a data breach plan in place. This will include knowing who your key contacts are, being able to minimise the risk to individuals, understanding when you need to report a data breach to your regulator or to affected data subjects, and the ability to identify the source of the breach and do what you can to make sure it doesn't happen again.

- **Check the latest guidance from the EU**. GDPR interpretation is still evolving. The European Commission's views on many relevant matters should become more clear over the next six months. See the most up-to-date information available through the European Commission's GDPR Portal at https://www.eugdpr.org/, including useful GDPR FAQs at https://www.eugdpr.org/gdpr-faqs.html. The OAIC also provides useful guidance including 'Privacy business resource 21: Australian businesses and the EU General Data Protection Regulation': the comparison table in section 6 below is reproduced from that Resource (with grateful acknowledgement). The UK Information Commissioner's Office also publishes useful guides, available at www.ico.org.uk. And the Article 29 Working Party's materials are often and useful: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

5. Conclusion

For many APP entities, GDPR compliance will be a step up, rather than a step change. APP entities that have fully implemented APP compliant policies, processes and practices, including privacy and security by design and by default, will find that the GDPR is still a challenge, but one that can be addressed utilising existing competencies and accessing readily available advice. For such organisations, GDPR implementation provides an opportunity to review compliance of existing privacy protective processes and practices with requirements of both the Australian Privacy Act and the GDPR. That noted, the writer's experience has been that even well established and resourced privacy and data protection teams in Australian businesses are finding areas for improvement in their APP compliance, as well as identifying key gaps between APP compliance and GDPR compliance. Other Australian businesses that have relied upon the small business exception, or that have not yet reached maturity in their Australian privacy compliance, will require a more fundamental, 'roots and branches' re-work. Certainly, many US based corporations are finding that implementing GDPR compliance requires significant business process re-engineering, changes in data handling and sometimes re-architecting of data infrastructure.

Privacy compliance review also affords a good opportunity for Australian businesses to review their existing processes of data value identification and capture, and of protection of the confidentiality of data as handled within multi-party data ecosystems. Many organisations are overdue for a careful review of data as a valuable asset of their business. Of course, the GDPR carriers heavy penalties for non-compliance. However, achieving compliance also provides an opportunity for capturing data value and for reducing regulatory friction as businesses expand across national borders, both within and outside the EU. If Australian businesses are to suffer the pain of achieving GDPR compliance, they should also seek to fully derive the gain, by undertaking one, more comprehensive review. Properly planned and managed, for APP mature Australian businesses the process of moving to GDPR compliance is exacting, but not rocket science.

Peter G Leonard
Principal, Data Synergies
Consultant, Gilbert + Tobin

M +61 411 089 003
E pleonard@datasynergies.com.au
LI https://www.linkedin.com/in/peleonard/

Comparison table (reproduced from the OAIC Guidance)[17]

	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

[17] OAIC, Privacy business resource 21: Australian businesses and the EU General Data Protection Regulation, https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation

		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