GDPR: The Final Countdown
What it Means for Australia

Veronica Scott, Special Counsel, and Ashleigh Fehrenbach, Associate, at MinterEllison, describe how the GDPR impacts Australian businesses, particularly in the media sector.

From 25 May 2018, the General Data Protection Regulation (2016/679) (**GDPR**) is set to replace the current EU data protection regime as the new European Data Protection law. Its purpose is to protect fundamental rights and freedoms of individuals when processing their personal data (wherever that may happen) and enable the free movement of personal data within the European Union (**EU**).

Due to the broad extra-territorial provisions in Article 3 of the GDPR, Australian businesses of any size (including media companies) may need to comply with the GDPR if they have an establishment in the EU, or if they do business in Europe by offering goods and services to individuals in the EU, or if they monitor the behaviours of individuals that takes place in the EU. The GDPR will take direct effect in all member states of the Union and in countries in the broader European Economic Area (**EEA**). The obligations that businesses will have will depend on whether they are a data controller or data processor.

The GDPR will apply in the UK at least until Brexit occurs (which will not be until at least 2019). The GDPR includes many obligations and rights that are similar to those in the Privacy Act and is founded on seven key data protection principles, with similar objectives to the APPs - to foster transparent information handling practices and business accountability in relation to data processing and handling. However, there are also additional stricter measures and individual rights in the GDPR. The GDPR also has hefty fines which gives it much sharper teeth than the Privacy Act.

Many of the requirements in the GDPR align with the steps that the Office of the Australian Information Commissioner (**OAIC**) expects Australian APP entities to take (as outlined in particular in the OAIC's Guidelines to the APPs), but which are not necessarily strictly required by the APPs. This is a reflection of the fact that the Privacy Act is broadly all principles based law, whilst the GDPR is highly prescriptive. It also includes additional rights for individuals. In short, best practice compliance with the APPs will support (but not ensure) compliance with the GDPR.

The GDPR has generated much discussion throughout the hallways of Australian law firms, as well as on a global level and is set to change the global privacy landscape for good raising the bar for data protection. The general view is that Australian businesses with a global focus should be asking:

(a) whether and to what extent they will be required to comply with the GDPR as a data controller or processor;

(b) assuming they need to comply, do any exemptions apply;

(c) what kind of steps do they need to take to achieve compliance as a controller or processor (ie those that are additional to the requirements in the Australian Privacy Principles (**APPs**) in the *Privacy Act 1988 (Cth)* (**Privacy Act**)); and

if they don't, what are the risks and potential regulatory consequences.

So, when does it apply?

The extra-territorial provisions in Article 3 of the GDPR extend its scope to the 'processing' of 'personal data' of data subjects (natural individuals) who are in the EU by a 'data controller' who is not established in the EU, where the processing activities relate to:

(a) offering the data subjects goods or services, irrespective of whether they are required to pay; or

(b) monitoring their behaviour as far as their behaviour takes place within the EU.

The definition of 'personal data' is similar to the Australian definition of personal information but specifically includes data such as identifiers. The act of 'processing' of their personal data covers all the acts and practices that are performed on it during its lifecycle, whether automated or not. It includes collection, recording, retrieval, use, storage, combining, automated processes and disclosure by transmission.

A 'data controller' includes the natural or legal person or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Data controllers have the most direct and onerous obligations under the GDPR. A 'data processor' processes personal data on the instruction of the controller (eg through a contract).

Despite these seemingly simple definitions, it is important to understand that assessments of whether or not the GDPR will apply to Australian businesses processing personal data about data subjects in the UK or other countries in the EEA are extremely fact sensitive.

Key additional requirements in the GDPR

We have outlined below the key gaps between the APPs and GDPR requirements and the main factors

that will need to be considered by media organisations in order to comply with these requirements.

Right to privacy enshrined

The GDPR gives Member States the ability to make laws in relation to some aspects of data processing. In particular for media organisations, Article 85 provides that Member States need to reconcile the right to privacy with the freedom of expression (both rights enshrined in the *European Union Charter of Fundamental Rights* (articles 8 and 10), when the processing of personal data is for purposes of, in particular, journalism, and in so far as this is necessary for the fundamental right to receive and impart information. This is a relatively vague provision and the only certainty the GDPR has provided is contained in Recital 153 "*This should apply in particular to the processing of personal data in the audiovisual field and in news archives and press libraries.*" and *"it is necessary to interpret notions relating to that freedom, such as journalism, broadly*."

Appoint a representative in the EU[1]*:* If an Australian business does not have an establishment in the EU, it will be required to appoint a representative established in an EU member state if its data processing meets certain thresholds. The role of the representative is to be a point of contact for supervisory authorities and individuals in the EU on all issues that relate to data processing, in order to ensure compliance with the GDPR.

Appoint a data protection officer ***(DPO)***[2]*:* Some data controllers will be required to designate and give resources to a DPO, which is an independent, expert and protected role, to monitor and advise on internal compliance with the GDPR and be accessible to data subjects and supervisory authorities.

Accountability - demonstrate compliance[3]*:* Not only must businesses comply, they must be able to **demonstrate** compliance with the data protection principles in the GDPR. (These apply to the handling of the personal data across its entire lifecycle, and are very similar to the APPs):

(a) Personal data must be processed lawfully, fairly and in a transparent manner;

(b) Purpose limitation - personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (with exceptions for public interest, scientific, historical or statistical purposes);

(c) Data minimisation - personal data must be adequate, relevant and limited to what is necessary in relation to purposes for which it is processed;

(d) Accuracy - personal data must be accurate and, where necessary, kept up to date. Inaccurate personal data should be corrected or deleted;

(e) Retention - personal data should be kept in an identifiable format for no longer than is necessary (with exceptions for public interest, scientific, historical or statistical purposes); and

(f) Integrity and confidentiality - personal data must be processed in a manner that ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Lawful basis for processing: Business will be required to demonstrate that they can rely on one of the following applicable lawful bases for processing personal data:

- Necessary to perform a contract or at the request of the individual before entering the contract
- Consent
- Necessary to comply with the business's legal obligations
- Necessary for the legitimate interests of the business or a third party which don't override the individual's interests
- Secondary purposes compatible with the primary purpose of collection

Privacy *by design and by default*[4]*:* the GDPR reflects a risk based approach to data protection (with similarities to the reasonable steps approach in the APPs). Businesses are required to implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to support the Data Protection Principles, taking into account the nature, scope, context and purpose of the processing.

*Undertake data protection impact statements (****DPIAs****)*[5] *and consult with supervisory authority about high risk processing*[6]: Businesses will be required to undertake a DPIA where a type of processing is **likely to result in a high risk** to the rights and freedom of individuals and, if this is indicated by the DPIA (in the absence of risk mitigation measures), consult with a supervisory authority before undertaking the processing

1 Article 27
2 Article 37
3 Article 5 (2)
4 Article 24
5 Article 35
6 Article 36

which can issue advice, request further information or give a warning. DPIAs are similar to what are known as privacy impact assessments in Australia (which the OAIC considers should be undertaken in certain circumstances as a reasonable step to comply with APP 1). However, consistent with its more prescriptive approach to compliance, the GDPR mandates these.

Expanded rights for individuals[7]: The GDPR strengthens the rights of individuals and affords them new rights, in particular in relation to the right to be forgotten[8], the right to data portability[9], the right to object to processing[10] and the right not to be subject to a decision based only on automated processing[11].

The right to be forgotten requires businesses to delete (erase) personal data on request from the data subject (subject to certain exceptions). Data may also need to be deleted if it cannot be processed in accordance with the GDPR. If the data has been published to other data controllers, reasonable steps must be taken to inform the other controllers of the requirement for erasure. This highlights the importance of keeping records of disclosure.

The right to data portability has two aspects. First it requires (on request) the provision to the data subject of his or her personal data in a structured, commonly used and machine readable format. The second, and arguably more onerous requirement, is to transfer an individual's personal data to another controller on request.

The right to object relates to objecting to specific types of information processing including, for example:

(a) direct marketing;

(b) processing based on legitimate interests or performance of a task in the public interest/ exercise of official authority; and

(c) processing for research or statistical purposes.

The right not to be subject to a decision based on automated processing is a right to avoid being '*subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning [the data subject] or similarly significantly affects [the data subject].*' Recital 58 provides as examples the '*automatic refusal of an on-line credit application or e-recruiting practices without any human intervention.*' There are some exceptions to this right that permit the automated processing.

Different data breach notification requirements[12]: The requirements are similar to Australia's mandatory breach notification requirements[13] but there are some key differences, including lower thresholds and tighter deadline for reporting to the relevant supervisory authority. Reporting of a data breach must happen within **72 hours** of becoming aware of the breach, unless that breach is unlikely to result in 'risk to the rights and freedoms' of individuals (this threshold of "risk" is potentially a lower threshold to "serious harm" in the Australian laws).

Stricter consent requirements[14]: If a business requires consent for any processing of personal data, (eg direct marketing or for lawful processing), it will need to comply with very strict requirements to establish valid consent. Consent must be freely given, specific, informed and an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the particular processing.

For the most part the consent requirements under the GDPR reflect the elements of valid consent as set out in the APP Guidelines. However there are further specific requirements under the GDPR including that a business would need to inform individuals about the right to withdraw consent, it must be demonstrable, distinguishable and based on clear affirmative action or statement.

Consent to processing of health data[15]: Australian business will require *explicit* consent to process sensitive personal data (noting that processing covers the handling of the personal data across its entire lifecycle, not just the initial collection). This entails a degree of formality, for example the individual ticking a box containing the express word "consent". Explicit consent cannot be obtained through a course of conduct.

Transparency[16]*:* Australian business will be required to give individuals a range of prescribed information about the processing of their personal data. This information must be concise, transparent, intelligible

7 Articles 15 to 22
8 Article 17
9 Article 20
10 Article 21
11 Articles 21 and 22
12 Article 33
13 *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth)
14 Article 4 (11)
15 Article 9 (2)
16 Articles 12, 13 and 14
17 Article 28

and easily accessible using clear and plain language (reflecting what the OAIC expects of Australian notices). This is similar to an APP 5 collection notice, but the GDPR requires additional information about express retention periods, the data subject's rights and, if there are overseas transfers, what safeguards are in place to permit overseas transfers.

Contracts with service providers (data processors)[17]*:* If a data controller engages a service provider who will be processing the personal data of data subjects in the EEA on behalf of the controller, it needs to use only processors who can provide sufficient guarantees in relation to safeguarding the data and ensure there is a written contract with the data processor that includes specific provisions as set out in the GDPR. Whilst current or template contracts may contain some of these clauses (e.g data security, use limitation, breach notification) businesses will need to impose more prescriptive requirements on processors. These include acting only within the scope of written authority of the controller.

Overseas transfers[18]: Unlike APP 8, the GDPR only permits the transfer of personal data outside the EEA (and onwards to another country outside the EEA) in certain prescribed circumstances, although some of the permitted circumstances are similar to the exception to the APP 8.1 reasonable steps obligation. These permitted circumstances are: transfers to countries with an "adequacy finding", transfers based on appropriate safeguards (through standard model clauses) or binding corporate roles. There are some other limited derogations, such as consent, but they have strict requirement.

Tougher sanctions[19]: The GDPR has high sanctions for non-compliance. For many breaches, supervisory authorities will be able to issue fines of up to 4% of annual worldwide turnover or €20 million. For breaches of other GDPR requirements, the fines can be up to 2% of annual worldwide turnover or €10 million. They also have a wide range of other powers such as broad investigatory powers and the powers to issue reprimands, impose a temporary or definitive limitation (including a ban) on processing, and impose administrative fines.

It will be interesting to see how the exceptions in Article 85 will be implemented. It is clear however that Australian media organisations who operate in Europe will need to carefully consider the impact of the GDPR, understand the personal data they hold about relevant individuals, how it is processed and the gaps in compliance.

Veronica Scott is a Special Counsel, and **Ashleigh Fehrenbach** is an Associate, at MinterEllison. Ashleigh is also a member of the CAMLA Young Lawyers Committee.

18 Article 45
19 Article 83 (5)