GDPR one year on

AFTER A YEAR OF OPERATION, IT IS TIMELY TO REFLECT ON THE IMPACT OF THE GENERAL DATA PROTECTION REGULATION ON AUSTRALIAN BUSINESSES AND HOW IT IS SHAPING THE DIRECTION OF PRIVACY REGULATION. BY ARVIND DIXIT AND LYNTON BROOKS

GDPR – a refresher

On 25 May 2018, the *General Data Protection Regulation* (GDPR) came into effect across the European Union (EU) signifying one of the most comprehensive reforms to European privacy laws in recent history. The objectives of the GDPR were to harmonise and strengthen privacy laws across the EU in response to growing concerns from the public and regulators that many companies are not doing enough to protect their customers' personal data. Under the GDPR, individuals are given new rights to manage how their data is collected, used and shared. European regulators, known as data protection authorities, are also given stronger enforcement powers, including the power to sanction companies with fines of up to €20 million or 4 per cent of annual worldwide revenue for serious contraventions.

Since its inception, the GDPR has frequently been used as a benchmark by legislators, regulators and law reform proponents around the world to promote changes to their own local laws. Australia has been no exception with a number of upcoming regulations and current reform proposals drawing inspiration from principles under the GDPR.

SNAPSHOT

- The GDPR has been one of the most significant reforms to European data protection and privacy laws.
- A number of recent and proposed changes to Australian laws and regulations are inspired by the GDPR.
- Australian businesses should take heed of the GDPR as it is having a significant influence on the future direction of Australia's privacy laws.

Relevance of GDPR to Australian businesses

Direct application of the GDPR

For some Australian businesses, the GDPR is directly relevant to their operations because of its broad extra-territoriality provisions (ie, those businesses are bound by the GDPR even though they may not have an establishment in the EU).

Under Article 3 of the GDPR,[1] a company without an establishment in the EU can still be subject to the GDPR if the company either offers goods or services to persons in the EU, or monitors the behaviour of such persons, where this involves any processing of personal data. The GDPR will apply if the company demonstrates an intention to specifically target EU individuals – for example, businesses that have localised versions of a website in different European languages, display pricing in European currencies or


ADOBE STOCK

tailor marketing content to European audiences. Companies that monitor someone in the EU will also fall under the GDPR, even if they did not know that the person monitored was in the EU. "Monitor" in this context includes things such as behavioural advertising, profiling, surveillance and tracking through cookies and other technologies where this involves personal data.[2]

Indirect impact of the GDPR

Many Australian businesses will have felt the impact of the GDPR even though they themselves are not bound by its terms. This has primarily occurred when an Australian company is entering into an agreement with an overseas organisation which is itself subject to the GDPR. Often that organisation will seek contractual commitments from the Australian company that it comply with the GDPR in its collection, handling and use of personal information. Australian companies have adopted a variety of methods to negotiate and mitigate the risk of these types of contractual commitments (including both technical and legal risk mitigation techniques) in circumstances where their IT systems and internal privacy processes may not adequately allow for full GDPR compliance. The extent to which a company can push back on these obligations however, is very much driven by its relative size and bargaining power.

Another impact of the GDPR being felt by Australian businesses is the evolution in Australia's privacy landscape which is currently occurring and which is very much driven by some of the same principles which underpin the GDPR.

Impact of GDPR on Australia's privacy landscape

Consent and transparency

Consent and transparency have been key recurring issues in some of the more notable GDPR enforcement decisions over the past 12 months. Under Article 6, an organisation must show that it has a lawful basis for any processing of personal data. The consent of an individual is one such lawful basis. For consent to be valid, it should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the individual's agreement to the processing of their personal data.

In addition to having a lawful basis for processing personal data, under Article 5 organisations must also ensure that they only process data in a fair and transparent manner. In addition, when collecting personal data about an individual, under Articles 13 and 14, organisations must provide the individual with certain prescribed information such as how they intend to process that data, the purposes of that processing, how long the data will be retained and with whom it may be shared. This information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

There have been calls for reform in Australia supporting similar requirements for transparency and consent be introduced under the *Privacy Act 1988* (Cth) (Privacy Act). In particular, the Australian Competition and Consumer Commission's (ACCC) Digital Platforms Inquiry Final Report, released in July this year, has recommended:

- the introduction of an express requirement that collection of personal information of consumers is accompanied by a notification of this collection that is concise, transparent, intelligible and easily accessible, written in clear and plain language and provided free of charge (broadly mirroring the language used in the GDPR)
- strengthening the consent requirements in the *Privacy Act* so that consent must be obtained whenever a consumer's personal information is collected, used or disclosed (subject to some limited exceptions, such as where the collection, use or disclosure is necessary for the performance of a contract with the consumer, is required by law or is otherwise required for an overriding public interest reason)
- clarifying that valid consent under the *Privacy Act* requires a clear affirmative act that is freely given, specific, unambiguous, and informed.[3]

These recommendations, if implemented, would bring Australia's notice and consent requirements in line with the GDPR, and would potentially be stricter than the GDPR in some regards. They would also have serious ramifications for Australian businesses that rely on implied or "opt-out" consent as a means of using or disclosing personal information.

Data portability and erasure

The GDPR introduced a suite of new rights for individuals in relation to their personal data. Arguably, the most significant of these have been the right to data portability and the right of erasure (also known as the right "to be forgotten"). The right to data portability under Article 20 allows individuals to demand that an organisation transfer their personal data to another entity, including to a competitor of the organisation. The right of erasure under Article 17 means that individuals can, subject to some exceptions, demand that an organisation permanently delete their personal data from the organisation's records.

While there is no general right of data portability or erasure under Australian law (although, under the *Privacy Act* there is an obligation for organisations to delete personal information once it can no longer

be used for any lawful purpose), the new Australian Consumer Data Right (CDR) legislation, which was passed by parliament on 1 August 2019, creates a new framework for transferring data in particular industry sectors, which is similar to the right of data portability under the GDPR.

Under the new CDR framework, consumers and small businesses can request access to, or transfers of, certain designated datasets held by entities in particular industry sectors.[4]

In many respects, the CDR framework is more extensive than the right to data portability under the GDPR. For example, in the banking sector the CDR framework applies to prescribed categories of banking data (such as data about mortgage accounts, credit and debit cards, and deposit and transaction accounts) which could include some data that is not "personal information" under the Privacy Act. The CDR framework is being incrementally implemented in the banking sector, to be followed by the energy and telecommunications sectors (and potentially more broadly in the future).[5]

In terms of the right to be forgotten, the ACCC's Digital Platforms Inquiry Final Report has recommended introducing a requirement in the *Privacy Act* for organisations to erase personal information about a consumer without undue delay on receiving a request for erasure from the consumer (subject to some exceptions).[6] While the Australian government is yet to formally respond to the ACCC's recommendations, it has previously indicated that it will be introducing amendments to the *Privacy Act* which "require social media and online platforms to stop using or disclosing an individual's personal information upon request" as well as "requiring platforms to implement a mechanism to ensure they can take all reasonable action to stop using an individual's personal information if a user requests them to do so . . ."[7] There is little guidance as to precisely how this is intended to operate. If it is implemented in a broad fashion, however, it will require key systems to be re-engineered to allow for personal information to be easily extracted from existing systems and algorithms (similar to the right to be forgotten).

Breach notification

Data breach notification continues to be one of the key obligations for companies under the GDPR and has been a major focus for European regulators in the first year of the GDPR's operation. Under Articles 33 and 34, companies must notify any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data to the appropriate data protection authority and to affected individuals. Companies must notify the data protection authorities no later than 72 hours after becoming aware of a breach and individuals must similarly be notified "without undue delay".

Australia's breach notification laws are generally regarded as less onerous than the equivalent provisions under the GDPR. For example, under the GDPR all personal data breaches must be notified by default, whereas under the Privacy Act only breaches

that are likely to result in serious harm need to be notified. Likewise, the time frames for notification under the GDPR are more prescriptive compared with Australian laws. Whereas under the GDPR, breaches must be notified within 72 hours, under the Privacy Act, companies have up to 30 days to investigate a suspected data breach and, if the breach is confirmed, must notify the Office of the Australian Information Commissioner and affected individuals of the breach "as soon as practicable".

Since 1 July 2019, Australian Prudential Regulation Authority (APRA)-regulated institutions such as banks, insurers and superannuation funds have also been subject to additional notification requirements under prudential standard CPS 234, which is closer to the GDPR standard for notifying breaches. Under CPS 234, APRA-regulated institutions must notify APRA within 72 hours of becoming aware of an information security incident where the incident either materially affects the interests of customers or has been notified to another regulator in Australia or overseas (including to the Australian Privacy Commissioner or a data protection authority).[8] It is probable that other industry regulators in Australia, particularly for those industries that handle sensitive data, will follow APRA's lead and introduce their own notification requirements using similar time frames to the GDPR. This is creating an environment in Australia where a particular incident may require reporting to multiple different regulators each with different thresholds and time frames.

Preparing for inevitable change

The GDPR will continue to set the trend for privacy regulation around the world. This is clearly evident based on the nature and breadth of changes that are currently being proposed in relation to Australia's data and privacy landscape. Companies that are prepared to adapt and react early to these trends will find themselves better prepared to compete and innovate on a global stage. Conversely, those that choose to ignore emerging trends overseas may quickly find themselves falling behind the pace of change, both in terms of regulatory compliance and in meeting consumer expectations with respect to privacy. ■

Arvind Dixit is a partner at Corrs Chambers Westgarth in the technology, media, and telecommunications team.

Lynton Brooks is an associate in the technology, media and telecommunications team at Corrs Chambers Westgarth, specialising in privacy and data protection matters.

1. Article numbers in the body of the article refer to the GDPR unless otherwise specified.
2. European Data Protection Board Guidelines 3/2019 on the territorial scope of the GDPR (Article 3).
3. Australian Competition and Consumer Commission Digital Platforms Inquiry Final Report (June 2019), www.accc.gov.au/publications/digital-platforms-inquiry-final-report.
4. Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth).
5. Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth) second reading speech.
6. Note 3 above.
7. Joint media release from Attorney-General Christian Porter and Minister for Communications and the Arts Senator Mitch Fifield, "Tougher penalties to keep Australians safe online", 24 March 2019.
8. APRA Prudential Standard CPS 234 Information Security at [35].