GDPR: READY OR NOT, HERE IT COMES

The European Union's (EU) General Data Protection Regulation (GDPR) – the most significant overhaul of Europe's data protection laws in recent memory – will come into force on 25 May 2018. From that date, any organisation to which the GDPR applies will need to ensure that all of its relevant data processing practices (including those ongoing under pre-existing arrangements) are compliant with its provisions.

This guide is designed to help you compare and understand the key similarities and differences between the Australian privacy laws and the GDPR. It also sets out a 10-step plan you can implement to ensure your organisation is well placed to achieve cross-border privacy compliance.

2018

BUT IT'S A EUROPEAN LAW...

While the GDPR applies first and foremost to organisations based in the EU, it has an extremely broad extra-territorial reach which may have a significant impact on the data handling practices of many Australian businesses and government agencies.

DOES IT APPLY TO MY ORGANISATION?

With the implementation deadline fast approaching, if you have not done so already you should consider as soon as possible whether or not your organisation is subject to the GDPR.

For a summary of what the GDPR is, its extra-territorial reach and the circumstances in which it might apply to Australian organisations, please see our recent insight here. If you are still in any doubt as to whether or not the GDPR will apply to your organisation, or what you need to do to ensure that you are compliant, you should seek legal advice immediately (which we can facilitate).

THE GDPR APPLIES TO MY ORGANISATION. NOW WHAT?

If the GDPR applies to your organisation, the next thing you should do is consider how the GDPR interacts with your organisation's obligations under Australian privacy laws. While the GDPR and the *Privacy Act 1988* (Cth) (**Australian Privacy Act**) share many common principles and requirements, the GDPR does not offer any exemptions for organisations based in jurisdictions with pre-existing privacy and data protection laws, even where those laws are "equivalent" to the GDPR. Instead, such organisations will be required to comply with both their local privacy laws as well as the GDPR.

The good news is that for many Australian organisations, GDPR compliance will simply involve building in an additional layer of protections into the organisation's compliance frameworks, rather than a step-change. This could even be seen as an opportunity to review and update existing data handling practices to make them "best of breed", in a world where management of data is increasingly seen as a core commercial differentiator. However, for other organisations (including those that have previously relied on the small business exception under the Australian Privacy Act), achieving compliance will require significantly more work.

COMPARISONS OF KEY REQUIREMENTS IN THE AUSTRALIAN PRIVACY ACT AND THE GDPR

The following table sets out at a high level the extent to which each of the key requirements under the GDPR are more or less onerous than the Privacy Act.

KEY

less onerous and/or narrower in scope
broadly equivalent in scope;
slightly more onerous and/or wider in scope; or
significantly more onerous and/or wider in scope.

Australian Privacy Act requirement	Equivalent requirement(s) under the GDPR
APP1 Compliance practices and privacy policy APP entities must take reasonable steps to implement practices, systems and procedures to ensure compliance with the APPs.	**Articles 24 and 25** Controllers must implement appropriate technical and organisational measures that ensure and demonstrate GDPR compliance – this is often referred to as "privacy by design".
APP2 Anonymity and pseudonymity Individuals must have the option of dealing anonymously or under a pseudonym with APP entities unless impracticable to do so.	No direct right, but pseudonymisation is encouraged (including for the purpose of being an appropriate measure to satisfy Articles 24 and 25 above). Note also that pseudonymisation has a specific definition and treatment under the GDPR, the application of which is subject to some debate.
APP3 Data collection APP entities must not collect personal information unless the information is reasonably necessary for its functions or activities, and such collection is lawful and fair.	**Article 6** Processing is lawful only if the data subject gives consent for a specific purpose, a contractual obligation exists, or it is necessary to achieve one of a limited list of "legitimate interests".
APP4 Unsolicited information APP entities who possess personal information not obtained from the relevant individual need to consider (1) if it could have lawfully collected the information if it had solicited it, and (2) if the answer is no, destroy or de-identify the information.	**Article 14** Where personal data has not been sourced from the data subject, a controller must provide the data subject with certain information, including the controller's contact details, categories of data, purpose of processing, recipients and the rights of the data subject.
APP 5 Notice When collecting personal data APP entities must notify the relevant individuals of certain information, including why the information is being collected and who the information will be disclosed to (including overseas recipients).	**Article 13** At the point of collecting personal data the controller is to provide the data subject with certain information, including purpose of the processing, recipients and the rights of the data subject.
APP 6 Purpose of use/disclosure APP entities may only use or disclose personal information for the purpose it was collected (primary purpose). Secondary use or disclosure is subject to consent and other exceptions.	**Article 6** Processing is lawful only if the data subject gives consent for a specific purpose, a contractual obligation exists, or it is necessary to achieve one of a limited list of "legitimate interests".

Australian Privacy Act requirement	Equivalent requirement(s) under the GDPR
APP 7 Direct Marketing APP entities must not use or disclose personal information to directly promote goods and services unless an exception applies, and individuals must be given the opportunity to "opt out" of direct marketing communications.	**Article 21** Where personal data is processed for direct marketing purposes the data subject has the right to object at any time and if so, personal data is to no longer be processed for such purposes. This "right to object" must be presented to the attention of the data subject at the first communication and must be presented separately from any other information.
APP 8 Offshoring APP entities who disclose personal information to a recipient outside of Australia must take reasonable steps to ensure the third party does not breach the APPs in relation to that information.	**Articles 45 and 46** Transfer of personal information is subject to certain conditions, including the controller or processor putting appropriate safeguards in place, and ensuring enforceable rights and effective legal remedies are available to data subjects.
APP 9 Government identifiers APP entities must not adopt a government related identifier as its own identifier of an individual.	**N/A**
APP 10 Data integrity APP entities must take reasonable steps to ensure personal information collected and held is accurate, up-to-date and complete.	**Article 5** Personal data must be accurate and up-to-date. Where personal data is inaccurate, every reasonable step must be taken to erase or rectify such data without delay.
APP 11 Data security APP entities must take reasonable steps to protect personal information from misuse, interference and loss.	**Article 32** Controllers and processors must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.
APP 11 Data security APP entities must take such steps as are reasonable in the circumstances to destroy or de-identify personal information (where no longer needed).	**Article 17** Data subjects have the right to obtain erasure of personal data in certain circumstances (also referred to as "the right to be forgotten").
APP 12 and 13 Access and correction APP entities must allow individuals to access and correct personal information it holds about them, subject to certain limitations.	**Articles 15,16, 17, 18 and 20** Data subjects have a number of rights with respect to their personal information, including to obtain confirmation as to whether or not their personal data is being processed, to receive personal data in a machine-readable format, to obtain rectification of inaccurate data, and to require the controller to restrict processing.
N/A	**Articles 37, 38 and 39** Controllers and processors must appoint a data protection officer (DPO) where the: + processing is carried out by a public authority or body; or + core activities consist of large scale monitoring of data subjects or large scale processing of sensitive data or data relating to criminal convictions and offences. The DPO's primary objective is ensuring the organisation's compliance with the GDPR.

The above is not an exhaustive list of requirements under the Australian Privacy Act or the GDPR and a detailed analysis is required to ensure compliance with each. Even where the two regimes are broadly equivalent, some nuanced requirements apply under each which need to be considered.

10-STEP PLAN TO ACHIEVING CROSS-BORDER PRIVACY COMPLIANCE

Assuming your organisation is already compliant with the Australian Privacy Act, we suggest implementing the following 10-step plan as part of a strategy to achieving cross-border privacy compliance:

1. **Engage leadership** – The first, and most important, step is to ensure that senior management understand the importance of achieving compliance with the GDPR and the risks of failing to do so. Senior management should be engaged with the issue of compliance with the GDPR, and be willing to contribute the necessary resources from the outset.

2. **Identify who is responsible for PI** – Regardless of whether your organisation is required under the GDPR to appoint a specific data protection officer, we recommend you do so as best practice, as it is critical to identify who in your organisation is responsible for overseeing the organisation's data protection strategy. Such person(s) should have a direct line into senior management.

3. **Train your staff** – Emphasise internally that data protection is an organisation-wide responsibility. All employees should regularly engage with your organisation's data protection policies and ensure they understand the chain of responsibility. Introducing a comprehensive data protection training program for all employees is also critical.

4. **Map your data** – Understand in detail what information your organisation is processing, holding and/or disclosing, how and to whom. Data providence and consent management are critical in enabling good data governance and compliance.

5. **Analyse current practices and contracts** – Conduct a gap analysis between your organisation's current practices and its legal obligations. As part of this analysis, you may find you need to update your organisation's privacy policies, notifications and consent mechanisms. It is also important to perform a root and branch analysis of your organisation's contracts to assess the extent to which they will require amendment to adhere to the GDPR. In particular, consider whether or not the contracts adequately allocate liability in respect of privacy breaches and whether the insurance policies will cover the liabilities under the GDPR.

6. **Put in place other "adequate technical and organisational measures"** – many Australian organisations will already have in place a number of measures designed to enable them to comply with their obligations under the Australian Privacy Act. Consider whether or not those measures adequately capture the things you are required to do under the GDPR.

7. **Conduct DPIAs** – If your organisation's proposed data processing activities are likely to result in a high risk to the rights and freedoms of individuals, it is highly likely you will be required to carry out a data protection impact assessment (**DPIA**) for each proposed processing activity. Ensure your organisation has a policy in place for when and how DPIAs should be conducted, and what happens if a DPIA identifies a high risk.

8. **Appoint a representative in the EU** – Controllers and processors not established in the EU must appoint a representative in the EU (subject to certain limited exceptions). Consider who this should be and whether it is practical to outsource this task to a third party (e.g. a law firm).

9. **Be prepared** – Make sure your organisation has a robust and well-tested data breach response plan in place which includes a clearly defined data breach reporting procedure and public relations considerations.

10. **Stay updated** – In the months following the GDPR coming into effect, further guidance is likely to be provided which will clarify the application and implication of the GDPR. You should regularly check the latest guidance from the European Commission, and if you think it may impact your organisation, seek legal advice.

FOCUS: MANDATORY DATA BREACH NOTIFICATION

In today's world where data is one of the hottest commodities on the market and cyber security incidents make headline news every other week, the relevant question for organisations is no longer ***if***, but ***when*** they will be subject to a data breach.

Given the significant impact (financial, legal and, perhaps most damagingly, reputational) that a data breach can have on your organisation, having in place robust and well-tested measures to minimise the impact of a data breach well in advance of one occurring has never been more important.

In addition, both the Australian Privacy Act and the GDPR now impose strict new requirements on certain organisations to notify individuals and supervisory authorities in the event of certain types of breaches occurring.

AUSTRALIA

From: 22 February 2018

WHAT: The *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) introduced into the Australian Privacy Act for the first time a mandatory data breach notification obligation (the **Notifiable Data Breaches Scheme**), requiring certain entities to notify eligible data breaches" to the Office of the Australian Information Commissioner (**OAIC**) and to notify any individuals who may be potentially affected by the data breach as soon as practicable.

WHO: Commonwealth government agencies and private sector organisations who are currently subject to the APPs under the Australian Privacy Act.

WHEN: An "eligible data breach" occurs where:

+ there is unauthorised access to, or unauthorised disclosure of, personal information, or personal information is lost in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and
+ a *reasonable person* would conclude that the access or disclosure would be likely to *result in serious harm* to any of the individuals to whom the information relates.

PENALTY: While an organisation is unlikely to face penalties based on the occurrence of the breach in and of itself, the failure to notify the OAIC of an eligible data breach could result in a complaint being made to the Privacy Commissioner. Serious or repeated interferences with the privacy of an individual can result in civil penalties of up to $2.1 million.

For more information on the Notifiable Data Breaches Scheme, and an overview of the findings published in the first quarterly report on notifications received by the OAIC, see our recent insights here and here.

EUROPE

From: 25 May 2018

WHAT: While sector and industry specific notification regimes have existed in Europe for some time, the GDPR introduces for the first time a general mandatory breach notification regime that applies across the board.

WHO: All processors and controllers who are subject to the GDPR. There are separate notification regimes for processors (who must notify the relevant controllers) and controllers (who must notify the relevant supervisory authority, and also affected data subjects where the data breach impacts the data subjects' rights and freedoms).

WHEN: Where a data breach leads to "the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". Controllers and processors must each report data breaches without undue delay, and controllers must in any event notify the supervisory authority within 72 hours of becoming aware of the data breach.

PENALTY: Non-compliance could lead to administrative fines of up to €10,000,000 or (in the case of undertakings) up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is greater.

If you would like any more information on your organisation's mandatory data breach notification obligations, and what you can do to mitigate any risks, please contact us.

SIMON BURNS
Partner
T +61 2 9263 4776
M +61 448 100 727
E sburns@gtlaw.com.au

MICHAEL CAPLAN
Partner
T +61 3 8656 3333
M +61 413 605 274
E mcaplan@gtlaw.com.au

TIM GOLE
Partner
T +61 2 9263 4077
M +61 410 540 745
E tgole@gtlaw.com.au

ANDREW HII
Partner
T +61 2 9263 4046
M +61 457 808 018
E ahii@gtlaw.com.au

SHEILA MCGREGOR
Partner
T +61 2 9263 4152
M +61 414 399 976
E smcgregor@gtlaw.com.au

LESLEY SUTTON
Partner
T +61 2 9263 4296
M +61 414 265 169
E lesutton@gtlaw.com.au

MELISSA FAI
Special Counsel
T +61 2 9263 4685
M +61 404 873 252
E mfai@gtlaw.com.au

ALBERT YUEN
Special Counsel
T +61 3 8656 3316
M +61 412 023 032
E ayuen@gtlaw.com.au

EDWARD DAVIDSON
Lawyer
T +61 2 9263 4610
E edavidson@gtlaw.com.au

CLARE HARRIS
Lawyer
T +61 2 9263 4189
E charris@gtlaw.com.au

NIKHIL SHAH
Consultant
T +61 2 9263 4048
E nshah@gtlaw.com.au

GILBERT +TOBIN

SYDNEY
Level 35 International Towers Sydney
200 Barangaroo Avenue
Barangaroo NSW 2000
Australia
T +61 2 9263 4000
F +61 2 9263 4111

MELBOURNE
Level 22
101 Collins Street
Melbourne VIC 3000
Australia
T +61 3 8656 3300
F +61 3 8656 3400

PERTH
Level 16 Brookfield Place Tower 2
123 St Georges Terrace
Perth WA 6000
Australia
T +61 8 9413 8400
F +61 8 9413 8444

GTLAW.COM.AU