GILBERT
+TOBIN

GDPR: THE FINAL COUNTDOWN

2018

GTLAW.COM.AU

In just over two months, 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 effect. While the GDPR applies primarily to organisations based in the EU, it may also have a significant impact on the data handling practices of many Australian businesses and government agencies.

The following FAQs are designed to help you understand what the GDPR is, whether or not it will apply to you and, if so, what that might mean for your organisation.

WHEN DOES THE GDPR COME INTO EFFECT?

25 May 2018. From this 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.

WHAT DOES THE GDPR DO?

It aims to harmonise data protection laws within the EU and to further protect the rights of EU citizens. It imposes a number of strict requirements on organisations that "control" or "process" the "personal data" of EU individuals and also provides those individuals with increased rights in relation to their "personal data".

KEY TERMINOLOGY

"**Personal data**" is any information relating to an identified or identifiable natural person.

"**Controller**" is an entity that determines the purposes and means of processing personal data.

"**Processor**" is an entity that processes the personal data on behalf of the controller.

WILL THE GDPR APPLY TO YOU?

The GDPR has an unprecedented extra-territorial scope. Australian organisations (whether private or public sector) of any size will need to comply with the provisions of the GDPR if they:

+ have an "establishment" in the EU, and process personal data in the "context of the activities" of that "establishment"; or
+ do not have an "establishment" in the EU, but process personal data relating to EU individuals in connection with:
  - offering them goods or services; or
  - "monitoring" their behaviour.

Concepts such as "establishment" and "monitoring" have historically been construed broadly by the European courts, and as a result careful consideration should be given as to whether your organisation conducts activities that might bring it within the scope of the GDPR.

It is important to note that while the GDPR and the Privacy Act 1988 (Cth) (Australian Privacy Act) share many common 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 (if applicable).

WHEN MIGHT YOU BE CAUGHT BY THE GDPR?

Examples of the types of practices that are likely to bring a non-European organisation within the ambit of the GDPR include where:

+ that organisation has an office or representative permanently based in the EU and processes personal data in the "context of the activities" of that "establishment", even if such processing itself does not occur in the EU;
+ a Commonwealth government agency processes personal data about an EU individual who has applied for an Australian visa;
+ that organisation targets EU individuals via advertising or marketing;
+ that organisation has a website which allows an EU individual to buy goods or services using the currency of an EU member state (although mere accessibility of a website from within the EU does not bring it within the scope of the GDPR); or
+ that organisation tracks the online behaviour of EU individuals to predict their preferences.

WHAT ARE THE KEY CHANGES INTRODUCED BY THE GDPR?

The GDPR introduces a number of new rules and concepts, some of which simply reflect a re-focusing of existing practices and others of which reflect a complete departure from such practices.

Some of the most significant changes include:

+ imposing obligations on data processors as well as data controllers (**Article 3**);
+ imposing tighter conditions and requirements in relation to obtaining consent (**Articles 7 and 8**);
+ introducing a mandatory data breach notification regime (**Articles 33 and 34**);
+ introducing enhanced rights for individuals (e.g. the right to access (**Article 15**), the right to be 'forgotten' (**Article 17**), the right to data portability (**Article 20**) and the right to object to processing carried out for certain purposes (**Article 21)**);
+ formalising the requirement to conduct data protection impact assessments in certain scenarios **(Article 35**); and
+ introducing a requirement to have a data protection officer (in certain circumstances) (**Article 37**).

The penalties for failure to comply with the GDPR are staggering. Breach of a "higher severity" obligation (including most of those listed above) may lead to a maximum administrative fine of up to **€20 million (approximately AUD 31.8 million) or 4% of the organisations' global annual turnover** for the previous financial year, whichever is greater.

WHAT DO YOU NEED TO DO TO GET READY?

With the 25 May 2018 deadline fast approaching, if you have not done so already you should consider as soon as possible whether or not you are likely to be subject to the GDPR and if so, the steps that you will need to take to ensure that you are compliant with its provisions.

If you are in any doubt as to whether or not the GDPR will apply to you, or what you need to do to ensure that you are compliant, you should seek legal advice (which we can help facilitate).

The Office of the Australian Information Commissioner has released a helpful guide to assist Australian businesses ensure compliance with the GDPR, as well as the Australian Privacy Act.

For further information, including how the GDPR differs from the Australian Privacy Act, keep an eye out for our more extensive GDPR guide, which is coming soon.

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

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
E mfai@gtlaw.com.au

ANDREW HII
Special Counsel
T +61 2 9263 4046
E ahii@gtlaw.com.au

ALBERT YUEN
Special Counsel
T +61 3 8656 3316
E ayuen@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