

HAVE YOU HEARD OF THE EU'S NEW GENERAL DATA PROTECTION REGULATION AND ARE YOU READY FOR IT?

By Leanne Jezercic, Senior Associate

14 May 2018

The General Data Protection Regulation, also known as "GDPR", is a new privacy law that's now only now days away from regulating how European data is handled. It was created to protect EU citizens but is broad enough to potentially impact businesses all over the world. It has generated a lot of attention in the media mostly tied to the massive penalties it brings.

So, why do businesses in Australia need to care about it? And how different is the GDPR to Australian privacy laws?

We answer these questions and give some guidance regarding what you need to do before the GDPR kicks in on 25 May.

Why does Australia need to play by EU rules?

The GDPR is extra-territorial by nature so it does not only apply to businesses established in the EU – rather it applies to protect the rights of EU citizens. So, if an Australian company:

1. has an 'establishment' (such as an office) in the EU; or
2. offers goods or services to EU customers (e.g. accepts payment in euros, or advertises to EU customers, including in native European languages); or
3. monitors an EU citizen's data for their behaviour (e.g. tracking their behaviour on the Internet or profiling a person to analyse their personal preferences), and that behaviour takes place in the EU;

then it will need to comply with the GDPR.

Aussie businesses need to take note of their obligations under the GDPR because the penalties for breach are much more severe than under Australian privacy laws, with fines of up to 20 million euro (roughly \$30 million AUD) or 4% of the company's global annual turnover, whichever is higher. And there is no 'small business exception' under the GDPR, so all Aussie businesses with a European connection, no matter the size, must comply with the GDPR.

GDPR vs. Australian privacy laws – 'same same' but different?

There are similar requirements between the GDPR and Australian privacy law and so Aussie businesses should have most of the compliance measures set up. However, the GDPR introduces some new requirements and new rights for individuals, which in turn leads to new compliance obligations for business. These include:

1. Under the GDPR, an individual must give specific and unambiguous consent to the processing of their personal information and organisations need to be able to demonstrate that consent was obtained. Importantly, silence, pre-ticked boxes or inactivity are not considered consent under the GDPR. This is different to the Australian consent requirement which may be either implied or express, although express consent is generally required for sensitive information. Under the GDPR, the consent must cover all processing activities. Therefore, if an organisation obtains consent to sign the individual up to a newsletter, they cannot later use the information for some other data processing purpose without separate consent to do so. This will likely have the biggest impact to businesses in Australia as the processes for consent may need to be reviewed and potentially realigned for those businesses with exposure under the GDPR.

2. An individual can also withdraw their consent at any time, and separate to this, there is a “right to be forgotten” under the GDPR – i.e. an individual has the right to have their personal data erased if it is no longer required for the reasons which it was collected. There is no equivalent right in Australian privacy laws, although there is a softer requirement to take reasonable steps to destroy or de-identify information if it is no longer needed for any permitted purpose.
3. The GDPR contains more rigorous and time-sensitive reporting requirements for breaches of data security, with organisations obligated to report breaches within 72 hours of becoming aware. In Australia we have a recently introduced mandatory data breach reporting scheme although it only applies to ‘eligible’ breaches likely to result in the real risk of serious harm. [Read more](#) about data breach notifications.
4. An individual has a right to “data portability” under the GDPR, meaning a right to receive the personal data concerning them in a structured format, and to transmit that data to another controller. While the APPs must take “reasonable steps” to allow for access to personal information, there are some exceptions, but the GDPR makes this non-negotiable.
5. The GDPR requires the appointment of a data protection officer to each organisation, which is not mandatory under Australian privacy laws.

What should Aussie businesses do?

If this is the first you’ve heard of GDPR, then you should take this opportunity to check whether the GDPR will apply to you, i.e. Do you have an establishment in the EU? Do you offer goods or services to individuals who are in the EU? Do you monitor any behaviour of individuals in the EU?

If you answered ‘yes’ to any of these questions, you should get advice on your specific obligations asap. Some of the things you may need to do include:

- get an understanding of all of the multiple touchpoints where personal information is collected and ensure a means of consent has been provided;
- know what data you hold, how it is stored and where it came from;
- update privacy policies and service agreements, where others are handling personal data on your behalf;
- appoint a data protection officer to monitor and ensure compliance with the GDPR;
- have a plan in place for notification of data breaches;
- develop procedures for handling individual requests for data.

Contact us

If you would like more information about whether the GDPR applies to you and what you need to do to ensure compliance, please get in touch with either of our team below.

Leanne Jezercic
+61 2 8935 8805
leanne@anisimoff.com.au

Heidi Bruce
+61 2 8935 8806
heidi.bruce@anisimoff.com.au



www.anisimoff.com.au



<https://www.facebook.com/AnisimoffLegal>



<https://twitter.com/AnisimoffLegal>



<http://www.linkedin.com/company/anisimoff-legal>