wotton kearney

GDPR – How one website advertisement could cost you millions from 25 May 2018

25 MAY 2018

GDPR comes into force Friday, 25 May 2018 and it is not too late to consider the impact to your business in AU/NZ.

The General Data Protection Regulation (GDPR) affects businesses across the globe, despite originating in the European Union (EU) and comes into force on Friday 25 May. It is not too late to consider the impact as an Australian or New Zealand business owner.

What makes this new regulation unique are the obligations imposed on businesses worldwide to comply with prescriptive rules on managing, distributing and caring for data. There are significant and mandatory obligations to report data breaches to regulators - and so even a simple website cookie advertisement could expose you to costly and time consuming legal scrutiny.

What is GDPR?

GDPR is a new set of data protection laws that applies to all EU countries and has potentially wide ranging implications for how data is obtained and retained by Australian and New Zealand businesses and potentially significant consequences for non-compliance, regardless of turnover or size.

What does this mean for your business?

GDPR does not only apply to EU based businesses, it has an extra territorial effect.

There are 2 primary reasons why AU/NZ companies should be alert to these new laws:

- The fines for not complying are significant and potentially crippling for a business – up to either €20m or 4% of your turnover (if higher than €20m); and
- Even if GDPR does not apply to you directly, contracts you enter into for your business may require you to comply with it - if you don't; it may affect your ability to acquire business that you used to.

Does GDPR apply to my AU/NZ business?

Naturally, GDPR applies to AU/NZ companies that have an EU subsidiary or establishment. However, even organisations without bricks and mortar in the EU, will still have to comply if the business:

- Offers goods or services to individuals in the EU (either citizens of an EU country or non-EU citizens domiciled in the EU); or
- Monitors the behavior of individuals in the EU.

The primary purpose of these obligations is the protection of an EU individual's right and freedom to how its own data is used.

How is doing business defined in the EU?

The GDPR guidance provides non-exhaustive criteria to take into account when considering whether you do business in the EU, namely:

- a physical presence in the EU – offices, agents or representatives;
- a website advertising to EU customers or referencing goods or services provided to EU customers; or
- a website that can be viewed in an EU language.

Even if you don't fit the criteria above, GDPR will still apply even if you *monitor* the behaviour of individuals in the EU.

What does this mean? Those businesses that collect data on European residents primarily to profile and document that individual's preferences will also be caught by GDPR. An example may be the use of website cookies.

Remember it is personal data not company data

It is important to note that personal data includes anything which can identify an individual such as contact information (including business email addresses), or even their IP address.

AU/NZ businesses will need to not only understand the EU data held but also data held by agents and suppliers - how EU data may be collected, how it is transferred and what is done with it.

Therefore regardless whether a business directly provides goods and services to the EU or not, there needs to be consideration of what data is held and whether there is a need to retain it. Deleting unnecessary data will significantly reduce exposures.

Further, processing personal data may be lawful under certain circumstances – such as where your customer has provided consent or where it is necessary for the purposes of legitimate interests of your business.

Key considerations

In complying with GDPR, the key things for AU/NZ business to understand are:

- The reasons why you have personal data and whether you require **consent**
- Whether you also have **special category data** (such as health information) which requires further justification as to why you have it and what you do with it;
- The restrictions on the **profiling** of individuals and the right to request that they are not profiled by your business;
- The concept of the **rights** of an individual introduced by GDPR, namely their rights and ownership over their own data and how it is used by businesses;
- Unless you fall within an exemption, you may need to **appoint a representative** based in the EU as a liaison between you and local authorities and individuals for managing the data;
- GDPR introduces a **mandatory data breach notification** regime – with a requirement to notify the relevant EU supervisory authority within 72 hours; and
- The **penalties** for non-compliance are potentially significant and crippling – in additional to the potential reputational damage to your business.

What should you do to prepare for GDPR?

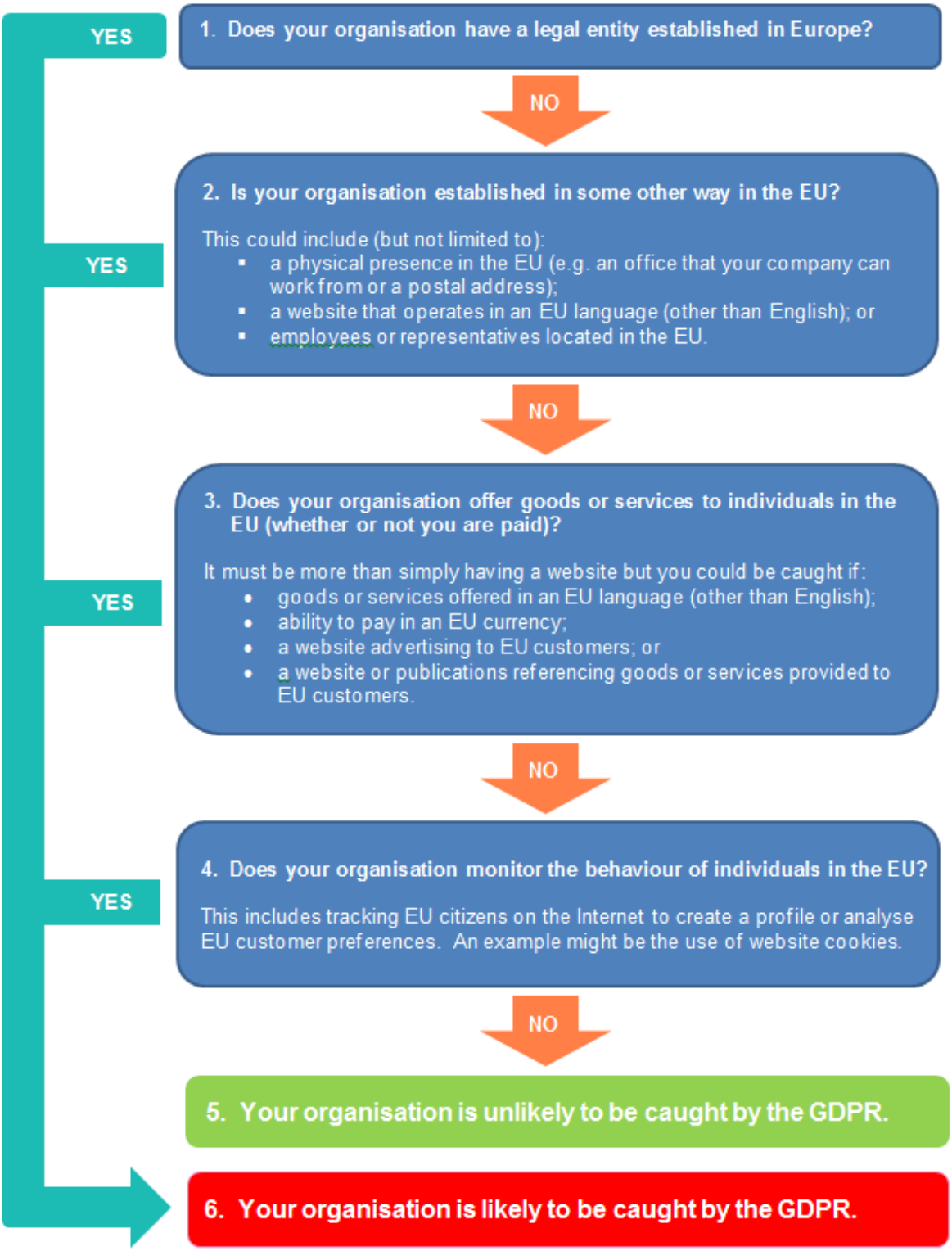
- Determine whether you do business in the EU
- Consider conducting a data audit on what data you hold about EU residents
- Consider deleting or at least anonymizing unnecessary data
- Consider whether you need to obtain additional consent for the data you retain
- Review privacy and data retention policies and their compliance with GDPR
- Ensure that you have an appropriate and compliant data breach response procedure in the event of a breach
- Ensure that your employees are aware of how to appropriately collect and use data
- Consider whether your cyber insurance covers you for your GDPR obligations and risks

W+K Cyber Team Contacts

For advice on how to comply with the GDPR, please contact:

Kieran Doyle
Special Counsel, Sydney
T: + 61 8273 9828
kieran.doyle@wottonkearney.com.au

Mark Anderson
Partner, Auckland
T: + 64 9 280 0524
mark.anderson@wottonkearney.com


YES
1. Does your organisation have a legal entity established in Europe?
NO
YES
2. Is your organisation established in some other way in the EU?
This could include (but not limited to):
a physical presence in the EU (e.g. an office that your company can work from or a postal address);
a website that operates in an EU language (other than English); or
employees or representatives located in the EU.
NO
YES
3. Does your organisation offer goods or services to individuals in the EU (whether or not you are paid)?
It must be more than simply having a website but you could be caught if:
goods or services offered in an EU language (other than English);
ability to pay in an EU currency;
a website advertising to EU customers; or
a website or publications referencing goods or services provided to EU customers.
NO
YES
4. Does your organisation monitor the behaviour of individuals in the EU?
This includes tracking EU citizens on the Internet to create a profile or analyse EU customer preferences. An example might be the use of website cookies.
NO
5. Your organisation is unlikely to be caught by the GDPR.
6. Your organisation is likely to be caught by the GDPR.