PAGE SEAGER
LAWYERS

Privacy Update

Will your business be affected by the new EU data protection laws?

1 What is the General Data Protection Regulation ("GDPR")?

The European Union (EU) GDPR 2016/679 contains new data protection requirements which will affect some Australian businesses.

In a move that is widely considered to be the biggest shake-up of data protection legislation for 20 years, the GDPR will come into force on 25 May 2018.

The aim of the GDPR is to harmonise privacy laws across the EU (and beyond) and also to strengthen the controls individuals have over how their personal data is used.

2 When will GDPR apply to an Australian business?

Your business may be subject to the GDPR if:

(a) Your business is established in the EU

The test to consider here is whether there is an *effective and real exercise of activity through stable arrangements* in the EU.

This may mean that Australian businesses could be caught if operating through a branch or subsidiary located in the EU.

(b) Your business offers goods or services to individuals in the EU (irrespective of whether payment is required)

It is considered that the interpretation of this category will be closely based on a test used in relation to consumer contracts in the *Brussels Regulation* and *Rome I Regulation*.

This test looks at a number of factors to decide if goods or services are "offered in the EU".

The following are strong indicators that a company is offering goods or services to individuals in the EU:

1. **Language** – if, for example, the language of an EU Member State is used on the website of your business and that language is not relevant to customers in Australia.
2. **Currency** – if, for example, your business allows payment in the currency of an EU Member State and that currency is not generally used in Australia (e.g. showing prices in Euros).
3. **Domain name** – if your website has a top level domain name of an EU Member State, for example, the use of ".de".
4. **Delivery to the EU** – if your business delivers physical goods to the EU.
5. **Reference to citizens** – if your website refers to individuals within the EU to promote your

goods/services (e.g. website refers to French customers who use the product/service).

6. **Customer base** – if your business has a large proportion of customers based in the EU.

7. **Targeted advertising** – if your business target advertises at individuals within the EU (e.g. newspaper advertisements in the EU).

However, Article 3 of the GDPR makes it clear that the *mere accessibility* of your website to EU citizens or the fact that your website is in English should not by itself make your business subject to the GDPR.

In order to fall within this category, a business must show intent to draw in EU customers e.g. by using a local language or currency.

(c) Your business monitors the behaviour of individuals within the EU

The meaning of this provision is not entirely clear. "Monitoring" individuals under Recital 24 of the GDPR specifically includes the tracking of individuals online to create profiles, particularly in order to make decisions concerning that individual or analysing or predicting that person's personal preferences, behaviours and attitudes.

It *could* apply broadly to your business if you profile your customers to offer personalised recommendations.

Alternatively, it could relate to more intrusive activities, such as tracking individuals across multiple sites or using Apps to track an individual's location.

3 Consequences for your business

If your business falls into one of the above categories, your processing of personal data about individuals in the EU will need to be GDPR compliant.

This means:

(a) You may need to review your Privacy Policy

To ensure that Privacy Policies are easy to understand and transparent, the GDPR contains certain mandatory information which should be included in your business' Privacy Policy, such as:

1. The purpose and legal basis of processing and the categories of personal data processed.

2. A list of the individual's rights including the right to withdraw consent.

3. How long the data will be stored.

In addition, if some of your data subjects are located in a non-English speaking EU country, it is likely that your business' Privacy Policy will need to be translated into local languages (if directed at a particular jurisdiction).

(b) Your customers have certain rights

The GDPR introduces potentially significant new rights for individuals in certain circumstances, including:

1. the **right to be forgotten** – i.e. the right for individuals to require erasure of personal data;

2. the **right to data portability** – i.e. the right for individuals to obtain, reuse and transmit their personal data which they have supplied for their own purposes in a machine-readable format;

3. the **right to restrict processing** of personal data; and

4. the **right to object to processing** of personal data.

These rights are complex and businesses will need to have procedures in place to manage such requests.

(c) You may need to appoint a representative in the EU

Article 27 of the GDPR requires you to appoint a representative in the EU, unless an exemption applies.

4 Penalties for non-compliance

Penalties for contraventions of the GDPR could result in significant fines of up to €20 million or 4% of annual global turnover (whichever is higher).

Page Seager's Corporate and Commercial team has extensive experience in privacy and data protection laws. If you require any further advice on how the GDPR is likely to affect your business, please contact:

Kathryn Speed
E: kspeed@pageseager.com.au