MARSH

May 2018

CLIENT ALERT

IMPLICATIONS OF THE GENERAL DATA PROTECTION REGULATION (GDPR) ON CYBER RISK FOR AUSTRALIAN COMPANIES

On **25 May 2018**, the EU General Data Protection Regulation 2016/679 (GDPR) becomes directly applicable in all EU member states. The introduction of the GDPR hails the most significant change to data protection law in Europe in over 20 years, replacing the European Directive 95/46/EC, which preceded the internet boom and birth of social media, and existing standalone national data protection rules.

The GDPR is intended to foster clear, uniform data protection laws across the EU, building legal certainty for entities and enhancing consumer trust in online services. While primarily applicable to EU member states, the GDPR can have broad extra territorial reach and may have implications for Australian businesses.

KEY CHANGES

Among the key areas of change under the GDPR are:

Greater transparency for individuals

In scope companies must provide individuals with clear and transparent information about how their personal data is used (including details of the recipients of the data, the purpose of the processing, the legal basis on which the company relies when using the data, and the period for which the personal data will be stored).

Enhanced rights for individuals

Individuals will have expanded rights over their personal data. In certain circumstances, these include a right to oblige a data controller to delete their personal data ("the right to erasure," also known as "the right to be forgotten"), a right to request their personal data in a structured, commonly used, and machine-readable format ("the right to data portability") and a right not to be subject to a decision based solely on automated processing. The GDPR also introduces more stringent consent requirements, limiting the circumstances in which consent may be relied upon to use personal data.

Mandatory data breach notification requirements

In scope companies are required to provide notification of data breaches within 72 hours of becoming aware of the breach, unless it is unlikely to result in a risk to the rights and freedoms of individuals. The GDPR also introduces mandatory notification to affected individuals where the breach is likely to result in a high risk of harm to those individuals.

Statutory obligations on data processors

The GDPR imposes obligations on both data controllers (who determine how and why personal data is processed) and data processors (who act on controllers' documented instructions only). While data controllers are already subject to statutory obligations; the GDPR will, for the first time, introduce statutory obligations on data processors in respect of their data processing activities.

Higher fines

The GDPR gives authorities the power to impose administrative fines for contravention of this regulation. Maximum fines for the most serious breaches will increase to €20 million or 4% of the company's total worldwide annual turnover (whichever is higher).

Member States will also have the legal capacity to impose further non-financial penalties and sanctions which must be "effective, proportionate and dissuasive[1]". Additionally, individuals can have the right to claim compensation for any damage suffered as a result of violating the GDPR.

Will Australian companies be impacted?

The GDPR can have broad extra territorial reach and may apply to Australian businesses.

Australian organisations may be subject to the GDPR if they have an establishment within the EU, offer goods or services to EU individuals or monitor the behaviour of EU individuals.

Examples of Australian businesses that may be impacted by the GDPR include[2]:

- an Australian business with an office in the EU
- an Australian business whose website targets EU customers, for example, by enabling them to order goods or services in a European language (other than English) or enabling payment in euros
- an Australian business whose website mentions customers or users in the EU
- an Australian business that tracks individuals in the EU on the internet and uses data processing techniques to profile individuals to analyse and predict personal preferences, behaviours and attitudes

GDPR and privacy legislation in Australia

February 22, 2018 marked the commencement of the *Privacy Amendment (Notifiable Data Breaches) Act 2017* in Australia, introducing a mandatory Notifiable Data Breaches scheme following an eligible data breach. This is applicable to companies governed by the Australian *Privacy Act 1988*, being most Australian Government agencies, all private sector (public listed/unlisted or private non-government entities) and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses.

The GDPR has a number of common features with the Privacy Act, notably a privacy by design approach to compliance and the adoption of harmonised, transparent information handling practices. However there are many differences, with the GDPR overall carrying more stringent compliance obligations and containing provisions for significantly higher penalties.

How the GDPR will apply to Australian businesses remains to be seen, and will depend on the potential application of international law, facts and circumstances of the specific company and general market forces. Marsh recommends you consult with your legal advisors in assessing whether GDPR will apply to your organisation. Marsh can assist with arranging insurance solutions to manage potential risks arising from these new laws.

In order to prepare for the GDPR we recommend that our businesses assess their risk, including:

- Assessing personal data held, where it came from and who it is shared with. This could include situations where your website or any apps offer goods and services directly to individuals within the EU, or where websites track or monitor (eg: via cookies) the behavior of individuals within the EU
- Consulting legal advisors to determine whether GDPR will apply
- Ensuring employees and management are aware of the GDPR and its potential impact to your business
- Ensuring a documented process to safeguard or, if required, delete personal data.

If you would like further information on the GDPR and how Cyber insurance can assist in risk transfer, please contact your servicing broker, Kelly Butler or Kristine Salgado.

Kelly Butler
National Cyber Leader, Australia
+61 3 9603 2194
kelly.butler@marsh.com

Kristine Salgado
Managing Principal, FINPRO
+61 3 9603 2871
kristine.salgado@marsh.com

[1] Article 83 EU GDPR "General conditions for imposing administrative fines"

[2] Office of the Australian Information Commissioner, 'Australian businesses and EU General Data Protection Regulation', Privacy business resource 21, updated March 2018.