

CLIENT ALERT:

IMPLICATIONS OF THE GENERAL DATA PROTECTION REGULATION (GDPR) FOR SINGAPORE COMPANIES

On May 25th 2018 the EU General Data Protection Regulation 2016/679 (GDPR) became 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 95/45/EC, which preceded the internet boom, social media and existing standalone national data protection rules.

PURPOSE OF THE REGULATION?

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 businesses in Asia.

REGULATION OVERVIEW

Some of the key changes are outlined below:

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.

Onerous 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.

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

WILL SINGAPOREAN COMPANIES BE IMPACTED?

The GDPR can have broad extraterritorial reach and may apply to companies in Singapore.

Singapore 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 behavior of EU individuals.

Examples of Singaporean businesses that may be impacted by the GDPR include:

- A Singapore business with an office in the EU
- A Singapore 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
- A Singapore business whose website mentions customers or users in the EU
- A Singapore 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 SINGAPORE

Singapore currently has two legislations that govern the cyber business landscape.

- The Personal Data Protection Act 2012 (PDPA) that governs the collection, use and disclosure by all private organizations, was instituted on 2nd July 2014.
- Cybersecurity Act 2017 was passed into law in Singapore on the 5th February 2018, implementing new guidelines, licensing and regulatory requirements for owners of critical information infrastructure (CII) and cybersecurity service providers. The bill provides a framework for the regulation of CII and formalized the duties of CII owners in respect of their obligations to information technology infrastructure.

The GDPR has a number of common features with the Personal data Protection 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 Singaporean 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 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 to safeguard or, if required, delete personal data.

CYBER INSURANCE AS A SOLUTION

Cyber insurance is an integral part of a risk transfer strategy for any company reliant on an operational technology or information technology dependent infrastructure.

Please contact your Marsh broker for further advice on effective cyber products.

RICHARD GREEN
Cyber Leader
+65 6922 8136
Richard.D.Green@marsh.com

Marsh is one of the Marsh & McLennan Companies, together with Guy Carpenter, Mercer and Oliver Wyman. This document is not intended to be taken as advice regarding any individual situation and should not be relied upon as such. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update this publication and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, tax, accounting or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. Marsh makes no representation or warranty concerning the application of policy wording or the financial condition or solvency of insurers or re-insurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. Marsh's service obligations to you are solely contractual in nature. You acknowledge that, in performing services, Marsh and its affiliates are not acting as a fiduciary for you, except to the extent required by applicable law, and do not have a fiduciary or other enhanced duty to you.