COMMVAULT

Maddocks

Illustration by Tam Morris, 2017

The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR)

A survival guide for your organisation

Preparing for the GDPR

In a world where data continues to grow at exponential rates, many organisations are already struggling to control their data. Add to that an environment of increasing regulation where cyber-attacks and data breaches are becoming regular, front page news, and there is a need for clear and practical guidance.

We understand the immense pressure organisations are under trying to protect, secure and access their data in an increasingly complex and regulated environment. That pressure is even greater for those organisations with world-wide operations.

Maddocks and **Commvault** are pleased to share this guide to the GDPR for Asia Pacific (**APAC**) businesses. It will help you to understand the impact of the GDPR and enable your business to better manage the complexities and issues that can arise from this far reaching regulation.

We show you how APAC businesses can be caught by the GDPR, compare it to local privacy legislation and give you practical tips to prepare for this new regulation.

We understand IT managers are under increasing pressure from the board and are already juggling a lot of balls, we're here to help you catch this next one.

Is your business ready for the GDPR?

Wherever you are situated in the APAC region, as an IT manager or Chief Information Officer you could easily be forgiven for thinking you don't have to worry about the GDPR. You're already dealing with expanding compliance requirements, increasingly complex and more regular cyber-attacks, exponential growth in data all while under diminishing budgets and resources. In addition, there is increasing pressures from your organisation's board, as issues of data, cyber security and privacy move from the server room and into the spotlight of the boardroom. While it would be nice not to add one more issue to your ever expanding 'to do' list, the reality is many APAC organisations will be caught by the new GDPR and need to be duly prepared.

It is time to get into the European mindset

If your business offers goods or services to customers residing in the European Union (**EU**) or monitors their behaviour, you could be caught by the GDPR even if your business does not have an office in the EU. Although the GDPR may not be front of mind for many APAC businesses, these businesses could face staggeringly large potential fines if they are in breach of the GDPR when it comes into effect on 25 May 2018. This additional exposure and the far more onerous obligations mean the GDPR is huge news in Europe. The extensive reach of the GDPR means it should be front of mind in this part of the world also.

1 What is the GDPR?

The GDPR is a new regime of personal data protection requirements adopted by the European Parliament that will apply to businesses from 25 May 2018. Under the GDPR 'personal data' is any information relating to an identified natural person or from which a natural person can be identified. The GDPR aims to return control to EU citizens over their personal data in an increasingly data-driven world and give businesses certainty with a uniform data protection law in the EU. Unlike the current 1995 Directive (which the GDPR will replace), there is no need for any EU Member State's government to pass enabling legislation before the GDPR comes into effect.

2 Why should your business care about the GDPR? - unprecedented extra-territorial reach

While the GDPR is EU law, it has unprecedented extra-territorial reach.

If your business processes the 'personal data' of individuals who are in the EU and either:

- offers goods or services to individuals in the EU
- monitors the behaviour of individuals in the EU

the GDPR will apply to you, even if you do not have an office in the EU. The individuals in the EU do not need to be EU citizens.

For example, the GDPR will apply if your website allows EU customers to order goods or services in a European language other than English or allows payment in Euros or if you use data processing techniques to analyse the personal preferences of individuals in the EU.

Another way in which the GDPR will apply to your business is if your business has an office in the EU.

In other words, if your business has a global presence – there is a high chance the GDPR will apply to you.

Importantly, your business could be fined up to 4 percent of its annual global turnover for the previous financial year or €20 million (whichever is higher) for non compliance with the GDPR. This is eye wateringly higher than the maximum fine of $2.1 million under the *Australian Privacy Act 1988*. Each EU Member State's supervisory authority will have wide-ranging corrective powers, for example, the power to issue reprimands to a business in breach of the GDPR.

People who have suffered damage (e.g. reputational damage or identity theft) due to a business' breach of the GDPR will also be able to seek compensation from that business.

Illustration by Tam Morris, 2017

...your business could be fined up to 4 percent of its annual global turnover for the previous financial year or €20 million (whichever is higher) for non compliance with the GDPR

3 Key aspects of the GDPR

The GDPR applies to both a 'controller' and a 'processor'. While some other jurisdictions, like Australia, do not make this distinction, in the EU a business is either:

- a 'controller' if the business decides how and why personal data is processed
- a 'processor' if the business processes personal data on behalf of a controller.

Consent: A controller must obtain an individual's consent to process their personal data. In particular, a controller must ask for consent using plain language and make it as easy for an individual to withdraw consent as it is to give it.

Sensitive information: There is a general prohibition on processing of sensitive information such as health information, sex life, sexual orientation, genetic data, religion, philosophical beliefs etc. Exceptions are if the individual has given express consent for a specified purpose or processing is necessary for exercising the controller or individual's rights and obligations in the context of employment, social security or social protection law.

Breach notification: A controller must notify the relevant supervisory authority of a data breach within 72 hours of finding out about it. This deadline is very demanding compared to other countries. Many countries in the APAC region do not have mandatory notification, and the requirement under the Australian regime (to come into force on 22 February 2018) is for businesses to report a data breach 'as soon as practicable' after becoming aware of it. A controller must keep an internal register of any data breaches. If a data breach is likely to cause a high risk to individuals' rights and freedoms, the controller must notify the individuals affected without undue delay and in plain language. A processor must notify the controller without undue delay after first becoming aware of the data breach. All businesses handling personal data need to be increasingly aware of mandatory notification requirements in light of the constant risk and the negative impact of data breaches. A case in point is Anthem Inc.'s $115 million settlement to end class action litigation over a data breach in 2015 where the personal data of 78.8 million members and employees was stolen.

Right to be forgotten: An individual may ask a controller to erase his/her personal data on certain grounds. For example, the data is no longer necessary for the purpose for which it was collected or an individual has withdrawn consent. If the controller has made the personal data public and is obliged to erase the personal data, it must inform other controllers that they should erase any copies of that personal data.

Data portability: If an individual has previously provided personal data to a controller, she/he is entitled to receive their personal data in a commonly used and machine-readable format and transmit that data to another controller.

Overseas transfers of personal data: The GDPR allows the transfer of personal data outside the EU to countries the EU Commission regards as providing an adequate level of data protection. For countries where the EU has not made such a decision, transfers are permitted in limited circumstances. For example, the controller has approved 'binding corporate rules' enabling transfers within a corporate group or entered into an agreement containing the model data protection clauses adopted by the EU Commission or a supervisory authority.

Data protection officers: A controller or processor must appoint its staff member or an external service provider as a data protection officer (**DPO**) if its core activities are:

- processing operations which require regular and systematic monitoring of individuals on a large scale
- processing sensitive information (e.g. health information) on a large scale.

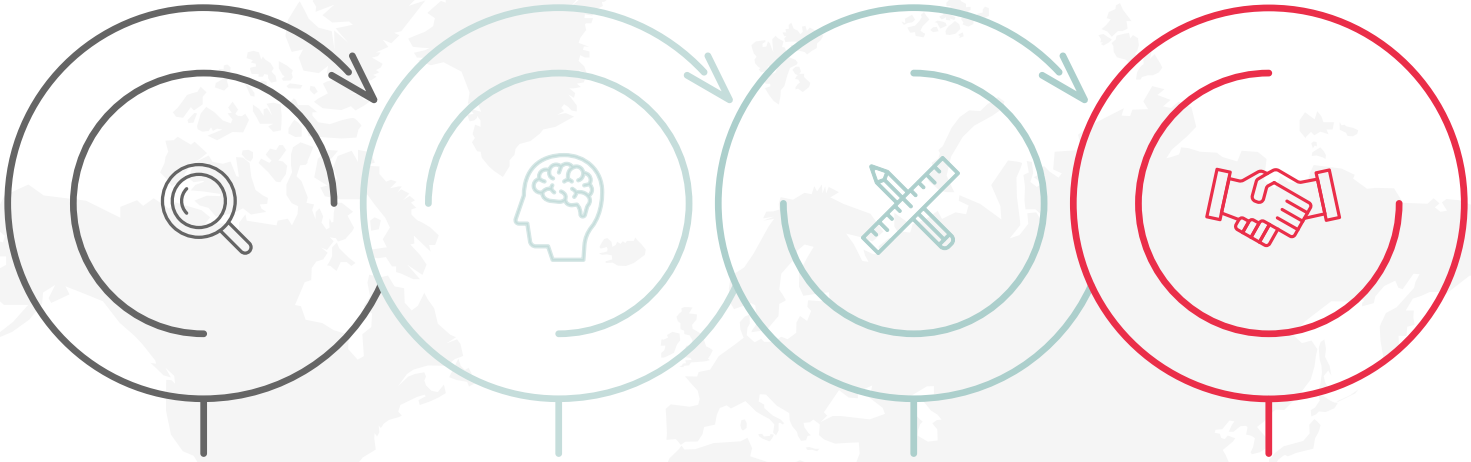
The DPO's duties are monitoring and advising on compliance with the GDPR and internal privacy policies and procedures, as well as cooperating with the supervisory authority.

Illustration by Tam Morris, 2017

COMMVAULT

Maddocks

4 How your business needs to prepare for the GDPR



Clarify

- Understand personal data flows in and out of your business?
- Determine if your business has customers in the EU or monitor the behaviour of people in the EU?
- Identify if your business has an office in the EU.
- How much control does your business have over the processing of the data?

Understand

- What are your GDPR obligations?
- Obtain expert advice on your legal obligations and IT solutions.

Review

- Ensure your current policies, documents, procedures and third party arrangements compliant with the GDPR?
- Amend any policies, documents, procedures, response plans and third party arrangements that are not compliant.

On board

- Get your staff on board.
- Employ or engage a DPO.
- Train staff members on the GDPR.

5 Overview of data protection obligations

While many APAC businesses will soon be required to comply with the GDPR, this does not replace the obligation to comply with relevant local privacy legislation which apply (see table below).

In an increasingly global and digital economy, APAC businesses need to remain astute and aware of both local and international privacy regimes which may apply to their operations. The GDPR, is one more (giant) ball to juggle in the increasingly complex landscape of data, privacy and security compliance.

Issued	GDPR	Australia	New Zealand	Singapore	Hong Kong
Maximum fines for breach	Greater of 4 percent of annual global turnover or €20 million.	AUD$2.1 million	Individuals may complain to Privacy Commissioner to facilitate a settlement. If no settlement is reached, the Human Rights Tribunal may award damages.	SGD$1 million	HK$50,000 (and a further penalty of HK$1,000 for each day that the offence continues).
Mandatory data breach notification?	Yes	Yes (when new laws commence on 22 February 2018).	No	No	No
Consent	Must be freely given, specific and informed. Ask for consent in plain language. Make it as easy to withdraw consent as it is to give it.	Must be freely given, specific, informed and current. Can be express or implied.	Must be freely given, specific, informed and current. Can be express or implied.	Must be freely given, specific, informed and current. Can be express or implied.	Must be freely given, specific, informed and current. Can be express or implied.

If you would like further advice about your business's privacy obligations, please contact Commvault or Maddocks.

Michael Bishop | Commvault
APAC Legal Director
61 2 8243 9815
mbishop@commvault.com

Brendan Tomlinson | Maddocks
Special Counsel
61 2 9291 6121
brendan.tomlinson@maddocks.com.au

Sonia Sharma | Maddocks
Senior Associate
61 2 9291 6143
sonia.sharma@maddocks.com.au

Emily Lau | Maddocks
Lawyer
61 2 9291 6141
emily.lau@maddocks.com.au

If you would like to read more about Australia's mandatory data breach laws, view our previous article maddocks.com.au/mandatory-data-breach-laws/